# LANDesk® System Manager 8.7

## Guia do usuário

LANDesk®

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

**Capa** ..... **1**
**Conteúdo** ..... **3**
**Visão geral** ..... **5**
Sobre LANDesk® System Manager ..... 5
**Introdução** ..... **9**
**Licenciamento** ..... **22**
Como adicionar licenças ..... 22
**O console** ..... **24**
Iniciar o console ..... 24
Uso do console ..... 24
Como especificar dispositivos-alvo ..... 29
Como filtrar a lista de exibição ..... 30
Utilização de grupos ..... 30
Utilização da guia Ações ..... 32
Colunas personalizadas ..... 35
Atributos personalizados ..... 36
Configurações de página ..... 37
Exibição do console de informações do servidor ..... 37
Gerenciamento de dispositivos Intel* AMT ..... 44
**Administração baseada em funções** ..... **51**
Sobre a administração baseada em funções ..... 51
Adição de usuários de produtos ..... 55
Criação de escopos ..... 57
Atribuição de direitos e escopo aos usuários ..... 58
**Descoberta de dispositivos** ..... **60**
Uso da descoberta de dispositivos ..... 60
Criação de configurações de descoberta ..... 62
Agendamento e execução da descoberta ..... 64
Como ver os dispositivos descobertos ..... 66
Como mover os dispositivos descobertos para a lista Meus dispositivos ..... 67
Descoberta de dispositivos Intel* AMT ..... 68
**Instalação e configuração de agentes de dispositivos** ..... **70**
Visão geral da instalação e configuração de agentes ..... 70
Configuração dos agentes ..... 72
Distribuição de agentes para dispositivos gerenciados ..... 75
Instalação de agentes ..... 77
Instalação de agentes com um pacote de instalação ..... 77
Instalação de agentes por recepção (pull) ..... 78
Instalação de agentes de servidores Linux ..... 81
**Monitoração do dispositivo** ..... **87**
Sobre a monitoração ..... 87
Configuração dos contadores de desempenho ..... 90
Monitoração do desempenho ..... 91
Monitoração de mudanças na configuração ..... 92
Monitoração de conectividade ..... 93
**Configuração de alertas** ..... **95**
Utilização de alertas ..... 95
Configuração de ações de alertas ..... 98

Configuração de conjunto de regras do alerta ..... 100
Distribuição do conjunto de regras ..... 101
Como ver os conjuntos de regras de alerta de um dispositivo ..... 102
Ver o log de alertas ..... 103
**Atualizações de software ..... 105**
**Scripts ..... 117**
Gerenciamento de scripts ..... 117
**Agendamento de tarefas ..... 121**
**Relatórios ..... 124**
Sobre relatórios ..... 124
Ver relatórios ..... 124
**Consultas ..... 126**
Utilização de consultas ..... 126
Consultas personalizadas ..... 129
Criação de consultas personalizadas ..... 129
Etapa 1: Criação de um critério de pesquisa (obrigatório) ..... 130
Etapa 2: Seleção dos atributos a serem mostrados (obrigatório) ..... 131
Etapa 3: Ordenação de resultados por atributos (opcional): ..... 132
Etapa 4: Execução da consulta ..... 132
Como ver os resultados da consulta ..... 133
Como ver os resultados de consulta da pesquisa ..... 133
Exportação de resultados de consultas para arquivos CSV ..... 133
Mudança dos cabeçalhos de colunas da consulta ..... 134
Exportação e importação de consultas ..... 134
**Gerenciamento de inventário ..... 136**
Gerenciar inventários ..... 136
Visão geral da análise de inventário ..... 136
Como ver os dados de inventário ..... 138
Opções de personalização de inventário ..... 140
Editar o arquivo LDAPPL3.TEMPLATE ..... 140
**Configuração de hardware ..... 144**
Suporte a Intel* AMT ..... 144
Configuração de dispositivos Intel* AMT ..... 145
Modificação no nome do usuário e senha para os dispositivos Intel* AMT ..... 149
Configuração de diretivas do System Defense ..... 150
Configuração da Presença do agente AMT Intel* ..... 152
Suporte IPMI ..... 154
Configuração IPMI BMC ..... 156
**Instalação e Manutenção do banco de dados núcleo ..... 164**
Instalação do banco de dados núcleo ..... 164
**Apêndice A: Requisitos do sistema e uso da porta ..... 165**
**Apêndice B: Ativação do servidor núcleo ..... 169**
**Apêndice C: Configurar serviços ..... 172**
Configuração das guias de serviços ..... 173
**Apêndice D: Segurança de agente e certificados confiáveis ..... 182**
**Dicas de resolução de problemas ..... 184**

# Visão geral

## Sobre LANDesk® System Manager

Bem-vindo ao LANDesk® System Manager 8.70, um aplicativo de gerenciamento independente que lhe permite manter a disponibilidade de seus servidores - inclusive os que executam o Windows, Linux, HP-UX e AIX. Ele pode também ser instalado e usado simultaneamente com o LANDeskManagement Suite, usando o mesmo banco de dados núcleo Management Suite para facilitar os relatórios de TI.

Criado com ênfase no baixo impacto de recurso, este produto tem vários agentes e serviços (por demanda) que só é executado quando são necessários, liberando assim memória e ciclos de CPU para outras tarefas. A LANDesk sabe que a disponibilidade de dispositivo é muito importante para a sua empresa, portanto o produto é projetado para a estabilidade, sendo executado em ambientes de 24 horas por dia, 7 dias por semana. Ele o deixa no controle do software que é executado nos seus dispositivos. Você pode instalar o agente completo, selecionar componentes específicos ou mudar dispositivos para sua lista de dispositivos sem instalar nenhum agente.

Para os diálogos e as janelas aparecerem corretamente na tela, o site do System Manager deve ser adicionado à lista permitida do bloqueador de popup do navegador.

### O que há de novo na versão 8.70

Os seguintes recursos foram adicionados ou receberam upgrade da versão anterior do System Manager:

**Gerenciamento de dispositivo sem agente:** Gerencie dispositivos na tela **Meus dispositivos** sem instalar um agente de gerenciamento neles, quando são habilitados com uma tecnologia de gerenciamento fora de banda como, Intel* AMT, IPMI ou DRAC.

**Grupos personalizados em Tarefas agendadas:** Você pode agrupar tarefas em grupos personalizados para execução simultânea.

**Modo principiante:** Você pode configurar para mostrar os títulos dos botões na barra de ferramentas e, assim, tornar mais fácil para os novos usuários saber as funções dos botões. Se preferir, você pode configurar também para não mostrar os títulos (as dicas de ferramenta continuarão a aparecer quando o ponteiro do mouse for colocado sobre o botão ou recurso).

**Configuração de hardware:** Esta nova ferramenta permite configurar opções para dispositivos com os recursos de Intel* AMT. Você pode gerar IDs para configurar dispositivos Intel AMT, ver os IDs gerados e mudar as opções de configuração para configurar os dispositvos Intel Intel AMT. É possível também definir diretivas de interruptor de circuito, o qual detecta e bloqueia atividades suspeitas de rede vinda dos dispositivos.

**Melhor suporte para a AMT (Active Management Technology - Tecnologia de gerenciamento ativo):** Este produto agora dá suporte à Tecnologia de gerenciamento ativo

(AMT) 2 Intel* (além da versão 1). A AMT versão 2 também suporta o gerenciamento sem agente e a descoberta automática dos dispositivos com Intel* AMT 2 devices.

## Recursos do produto

O System Manager lhe permite escolher seu nível de abrangência de gerenciamento, da simples coleta de informações à análise robusta de desempenho, segurança e controle de configuração. O System Manager contém o seguinte:

**Web console fácil de usar:** Execute o produto a qualquer hora e de qualquer local com o console baseado na web, projetado para fornecer uma abundância de dados em uma interface de fácil utilização. Execute-o da sua estação de trabalho primária ou de uma estação de trabalho na sala de servidores, sem ter de fazer nenhuma instalação. Vá até o URL do produto, http://*coreserver*/LDSM. Você "seleciona como alvo" dispositivos específicos para receberem ações como a distribuição de software, através da seleção e colocação na lista de **Dispositivos alvo**, semelhante ao modelo de cesta de compras em muitos aplicativos da web.

**Suporte expandido ao sistema operacional:** Gerencie o seu ambiente diverso de servidor a partir de um console integrado. Além de gerenciar servidores Windows 2000 e 2003, o System Manager fornece suporte para vários outros tipos de Linux e Unix:

- 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 – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (ES) 32 bits – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (WS) 32 bits – U3
- Red Hat Enterprise Linux v4 (WS) EM64t – U3
- SUSE* Linux Server 9 ES 32 bits SP2
- SUSE Linux Server 9 EM64t SP2
- SUSE Linux Professional 9.3
- SUSE Linux Professional 9.3 EM64t
- HP-UX 11.1
- Unix AIX

**Tela da tarefa agendada:** Veja toda a distribuição de agente agendada ou completada, descoberta,  atualização de software, e tarefas de script personalizadas de um local. Você pode reagendar a tarefa, modificá-la ou torná-la um evento reocorrente.

**Suporte a Intel* AMT:** O suporte para a Tecnologia de gerenciamento ativo (AMT) Intel* versões 1 e 2. A Intel AMT permite gerenciar remotamente dispositivos gerenciados em rede em qualquer estado de sistema através da comunicação fora de banda (OOB), até mesmo quando o SO não responder ou o dispositivo estiver desligado. Os únicos requisitos para o dispositivo são que ele deve estar conectado a uma rede corporativa e tenha alimentação de espera.

**Suporte IPMI:** O produto oferece suporte a servidores com o IPMI (Intelligent Platform Management Interface) ativado (versões 1.5 ou 2.0), permitindo recuperação remota de servidores fora de banda e a exibição de dados de gerenciamento autônomo, mesmo quando o SO ou o processador não estão em execução.

**Ferramenta de scripts:** Você pode executar tarefas personalizadas nos dispositivos criando scripts para o agendador local.

**Monitoração do desempenho:** Você pode monitorar em tempo real o desempenho dos servidores da empresa ou servidores blade gerenciados, utilizando uma ampla gama de atributos. É possível até fazer um acompanhamento desses atributos e ver os dados do desempenho histórico em relatórios abrangendo vários dias. Você pode monitorar dispositivos que têm o agente de monitoração instalado, e pode também monitorar servidores fora de banda com o IPMI ativado, mesmo que eles não tenham o agente instalado.

**Suporte a servidores blade:** O chassi de blade IBM e blades de servidor são suportados, inclusive os recursos de descoberta, detecção de chassis, inventário,  e gerenciamento de patches. As ferramentas do produto lhe permitem agrupar blades por função, chassi, gabinete ou outros critérios, o que resulta em uma coleta de dados mais eficaz.

**Relatórios:** Execute relatórios em qualquer dispositivo no banco de dados, e veja estatísticas de utilização, alocação de recursos e vários outros parâmetros. Este produto inclui vários relatório pré-formulados, prontos para serem utilizados. Esses relatórios são executados rapidamente através do acesso direto ao banco de dados para coletar informações e exibir os dados em gráficos de pizza e de barras bidimensionais e tridimensionais. É possível criar relatórios adicionais através da criação de consultas personalizadas.

**Monitoração / Alertas de funcionamento:** E fácil monitorar o funcionamento geral de um dispositivo. Você pode definir limites para medidas, como a utilização do espaço em disco e da CPU, e configurar como você deseja receber alertas no caso de um dos limites ser excedido. Você pode ver a tendência do estado de dispositivos selecionados e iniciar ações para resolver o problema antes que os usuários tenham um desempenho sofrível ou que haja necessidade de desligar o servidor para manutenção.

**Atualizações de software:** Você pode receber atualizações de software para System Manager e para hardware Intel*. Você pode distribuir manualmente as atualizações selecionadas, usando os recursos de distribuição de software.

**Administração com base em função:** Adicione usuários e configure seu acesso às ferramentas e a outros dispositivos com base em sua função administrativa. Com a administração baseada em funções, você atribui um escopo para determinar os dispositivos que um usuário pode visualizar e gerenciar, e direitos para determinar as tarefas que ele pode realizar.

**Inventário:** Com a ferramenta de análise de inventário, o produto compila uma grande quantidade de informações de hardware e software, e as armazena no banco de dados núcleo. Você pode exibir, imprimir e exportar os dados de inventário.

**Descoberta de dispositivos:** Saiba, com certeza, o que está na sua rede. A descoberta de dispositivos coleta informações básicas sobre todos os dispositivos no seu ambiente, possibilitando maior controle e permitindo uma distribuição mais rápida de agentes aos dispositivos alvo.

**Suporte ao Active System Console:** Suporte para o Active System Console, que fornece uma vista geral do funcionamento do sistema quando o agente do Active System Console é instalado no dispositivo. Você pode ver rapidamente se os elementos de um determinado hardware estão funcionando corretamente e se há problemas potenciais que podem precisar de resolução. Você pode também ver as estatísticas detalhadas de desempenho do sistema assim como uma lista de componentes do sistema, inclusive hardware, software, logs e informações sobre Intel* AMT e IPMI (se o dispositivo estiver habilitado para um deles).

**Executive dashboard:** Grupo de ferramentas (gráficos informativos, diagramas, mostradores e medidores) que capacitam os executivos a monitorar o funcionamento ou status da empresa.

**Ajuda:** Este produto inclui um Guia de introdução, e também tópicos de ajuda sensíveis ao contexto.

## 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. O servidor núcleo pode ser um novo servidor ou um servidor redirecionado para este fim.
- **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.
- **Meus dispositivos:** Dispositivos na rede que têm agentes de produto instalados. "dispositivos" são computadores, servidores, computadores laptop/móveis, chassis blade, etc. Um servidor núcleo pode gerenciar milhares de dispositivos.
- **Público:** Itens (grupos, pacotes de distribuição ou tarefas) que são visíveis a todos os usuários. Quando um usuário modifica um item Público, a modificação permance Pública. Os grupos Públicos são criados por usuários com direitos de Administrador.
- **Privado** ou **Usuário:** Itens que são criados pelo usuário conectado no momento. Esses grupos não são visíveis aos outros usuários. Os itens Privados ou Usuários aparecem nas árvores **Meus métodos de distribuição**, **Meus pacotes** e **Minhas tarefas**. Os usuários com direitos de Administrador podem ver grupos Privados e pacotes e tarefas de Usuários.
- **Comum:** Item visível a outros usuários. Quando um usuário assume a propriedade de um item Comum (ao modificá-lo), o item se ramifica em dois: o item Comum permanece e o item do usuário é salvo na pasta Usuários. A instância Usuário desse item não é mais visível aos outros usuários. O usuário pode marcar qualquer tarefa visível a ele como Comum, e assim compartilhá-la com outros usuários. Quando o usuário limpa a opção Comum das propriedades do item, a tarefa só é visível ao grupo de tarefas Usuário, dessa pessoa.

# Introdução


- Visão geral
- Execução do programa de instalação
- Ativação do servidor núcleo
- Adição de usuários
- Configuração de serviços e credenciais
- Execução do console
- Como descobrir dispositivos
- Agendamento e execução da descoberta
- Como ver os dispositivos descobertos
- Como mover os dispositivos para a lista Meus dispositivos
- Como agrupar dispositivos para ações
- Configuração de dispositivos para gerenciamento
- O que vem a seguir?


## 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 ou fazer upgrade para Management Suite ou 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**.
2. Digite o nome de usuário exclusivo e a senha fornecida quando adquiriu suas licenças.
3. 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.

# Licenciamento

O processo de licença ajuda a manter a sua organização em conformidade com os seus contratos de licenciamento de nós através da execução de um processo contínuo de autorização. Esta abordagem também permite usar vários servidores núcleo sob uma conta de um usuário específico. O processo do Licenciamento utiliza um banco de dados backend para criar e gerenciar contas de usuários. O processo de licenciamento é um processo de solicitação e resposta simples do servidor núcleo para o processo do backend, permitindo que o núcleo renove sua atividade por outro período.

Quando executar o produto (ou qualquer outro produto suplementar) após uma instalação, é possível ativar uma licença de avaliação por determinado período ou digitar um nome de usuário e senha para ativar uma licença adquirida das Vendas da LANDesk. Os mesmos nome de usuário e senha são utilizados para ativar todos os servidores núcleo para a conta existente.

O processo de ativação é essencialmente o mesmo para a avaliação e para a compra de produtos. Quando o dispositivo tem uma conexão com a Internet, o processo é um simples intercâmbio de informações. Quando o dispositivo não está conectado, deve ser executado o processo manual de enviar um arquivo por email para a LANDesk e posteriormente salvar um arquivo retornado por email no servidor núcleo. O processo de ativação funciona da seguinte maneira:

1. O usuário executa o utilitário Ativar núcleo
2. É criado um arquivo contendo as informações do servidor e do uso. Ele é assinado pela chave privada do núcleo e criptografada com a chave pública do LANDesk.
3. Se houver uma conexão com a Internet, o núcleo e os servidores da LANDesk se comunicam e o núcleo carrega o arquivo de ativação. O backend processa as informações e envia de volta as informações de ativação, as quais são gravadas diretamente no banco de dados.
4. Se não houver conexão com a internet, você pode enviar por email o arquivo que se encontra na pasta Arquivos de programas\LANDesk\Authorization Files para licensing@landesk.com.

# Como adicionar licenças

A funcionalidade disponível a você no console depende de uma chave de licença. Você pode adicionar uma nova chave de licença para acessar funcionalidade adicional ou atualizar o número de usuários. Durante a instalação é gerada uma licença de avaliação de 45 dias. Quando você adicionar uma licença válida usando o console, a licença temporária será excluída.

**Para adicionar uma chave de licença**

1. No painel de navegação esquerdo, clique em **Preferências**.
2. Clique na guia **Licença**.
3. Na parte inferior da tela, clique no link http:/www.landesk.com/contactus/.

Se o link acima não funcionar, pode ser porque o Nível de segurança do seu navegador não está configurado como Médio. Você deve mudar o Nível padrão de segurança da internet para Médio

no Internet Explorer (**Ferramentas > Opções da internet > Segurança > Internet > Nível padrão**).

# O console

## Iniciar o console

**Para iniciar o console**

1. No servidor núcleo, clique em **Iniciar | Todos os programas | LANDesk | LANDesk System Manager**.

   ou

   Em uma workstation remota, abra um navegador e digite o endereço do console. O endereço estará no formato http://*corename*/ldsm.

2. Digite um nome válido de usuário e uma senha.

   Se você estiver se conectando a um servidor núcleo remoto, siga as regras normais do Windows para login remoto (ou seja, se o usuário estiver no mesmo servidor núcleo, basta informar o nome do usuário; se o usuário for um usuário de domínio, digite o nome de domínio nome\usuário do usuário).
3. Clique em **OK**.

Se a lista de dispositivos e os botões não aparecerem quando o console for iniciado, pode ser que você precise ativar o servidor núcleo.

### Sobre a caixa de diálogo Login do System Manager

Use esse diálogo para iniciar o console e conectar-se a um servidor núcleo.

- **Nome do usuário:** identifica um usuário. Esse usuário pode ser um administrador ou outro tipo de usuário produto com acesso restrito (para mais informações, consulte Administração com base em funções). O usuário deve ser um membro do grupo LANDesk Management Suite no servidor núcleo. Se estiver se conectando a um servidor núcleo remoto, digite o nome de domínio e o nome do usuário.
- **Senha:** a senha do usuário.

## Uso do console

Você pode usar essas ferramentas para ver, configurar, gerenciar e proteger os dispositivos na sua rede—tudo isso de um único console. Você pode atualizar software ou configurações, diagnosticar problemas de hardware e software, e usar a administração baseada em funções para controlar o acesso de usuários a recursos e dispositivos. Além disso, se estiver também usando outros produtos LANDesk, poderá conectá-los diretamente do console.

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 direito no console mostra os diálogos e as telas que lhe permitem gerenciar dispositivos e usuários, ver relatórios, executar descobertas, criar e modificar consultas, etc. É possível redimensionar os painéis e colunas na lista **Meus dispositivos**. Quando não há nenhum agente instalado em um dispositivo, as colunas Nome e Endereço IP são as únicas que contêm informações. Em alguns casos, o sistema operacional também é exibido.

O System Manager fornece algumas funcionalidades de aplicativo Windows na conveniência e acessibilidade do seu navegador de web.

- Clique com o botão direito na lista **Meus dispositivos** para ver as opções disponíveis do dispositivo como, por exemplo, Pinge Alvo.
- Para selecionar várias entradas da lista, clique no primeiro item, pressione e segure a tecla **Shift** e, a seguir, clique no último item.
- Para selecionar várias entradas não consecutivas da lista, clique no primeiro item, pressione e segure a tecla **Ctrl** e, a seguir, clique em cada item.

Para que os diálogos e as janelas apareçam corretamente na tela, o site do System Manager deve ser adicionado à lista permitida do bloqueador de popup do navegador.

**Administração baseada em funções**
Como usuário, os dispositivos que você pode ver e gerenciar na lista **Meus dispositivos** e as ferramentas de gerenciamento que você pode usar são determinados pelos direitos de acesso e pelo escopo de dispositivos atribuídos a você pelo Administrador. Para ver mais informações, consulte "Uso da administração baseada em funções".

Esta seção fornece informações sobre:

- Lista Meus dispositivos
- Ícones de dispositivos
- Utilização dos menus de atalho
- Uso das ferramentas
- Como ver as propriedades de dispositivo

# Lista Meus dispositivos

A lista **Meus dispositivos** contém os grupos e subgrupos a seguir. Além disso, dependendo dos seus direitos de acesso e do escopo de dispositivos, você pode criar seus próprios grupos para facilitar o gerenciamento dos dispositivos.

## Todos os dispositivos

A lista **Todos os dispositivos** relaciona os dispositivos do usuário atualmente conectado, baseada em seu escopo, em uma lista sem subgrupos. Quando conectado a um determinado servidor núcleo, o administrador pode ver todo dispositivo gerenciado por esse servidor núcleo. Os usuários dos produtos, por outro lado, são restritos e podem ver apenas os dispositivos contidos no seu escopo atribuído (um escopo é baseado em uma consulta do banco de dados ou em um local de diretório).

Os dispositivos que estiverem executando os agentes do produto (Agente de gerenciamento padrão e Inventário) aparecem automaticamente na lista **Todos os dispositivos** quando são

analisados no banco de dados núcleo pelo analisador de inventário. Normalmente, essa análise é feita pela primeira vez durante a configuração inicial do dispositivo. Após um dispositivo ser analisado e colocado no banco de dados núcleo, ele se torna um dispositivo gerenciado—podendo então ser gerenciado pelo servidor núcleo. Para ver mais informações sobre a configuração de dispositivos, consulte "Configuração dos agentes do cliente".

Pelo fato de o grupo **Todos os dispositivos** ser preenchido automaticamente por meio de uma varredura de inventário, talvez não seja preciso descobrir dispositivos manualmente. Entretanto, para descobrir dispositivos que ainda não estão no banco de dados núcleo (ou para mover dispositivos não gerenciados para o grupo servidores), você pode usar a ferramenta Descobrir dispositivos para fazer uma varredura da rede e encontrar dispositivos. Para ver mais informações, consulte "Uso de descobertas".

O grupo **Todos os dispositivos** fornece as seguintes informações de cada dispositivo. Clique duas vezes em **Todos os dispositivos** para abrir a lista.

- **Nome:** O nome do dispositivo host, por exemplo, o nome do computador no Windows*.
- **Endereço IP:** O endereço IP do dispositivo.
- **Funcionamento:** O status de funcionamento e disponibilidade do dispositivo. Os estados podem ser: Normal, Aviso, ou Crítico.
- **Agente:** O agente atual em execução no dispositivo.
- **Tipo de dispositivo:** Mostra o tipo de hardware no computador (Intel AMT, IPMI, ASIC ou IPMI Avançado).
- **Sistema operacional:** O tipo de sistema operacional em execução no dispositivo.
- **Executando desde:** A data e o horário desde quando o computador começou a operação contínua (no fuso horário do banco de dados).

Quando você seleciona um dispositivo, as propriedades do dispositivo são mostradas no painel **Propriedades**, abaixo da lista de dispositivos. O painel **Propriedades** mostra muitos atributos importantes do dispositivo:

- **ID:** O número de identificação do dispositivo. Esse número é determinado pela seqüência em que o dispositivo foi adicionado à lista **Todos os dispositivos**.
- **Endereço IP:** O endereço IP do dispositivo.
- **Fabricante:** O fabricante do dispositivo.
- **Modelo:** O modelo do dispositivo.
- **Velocidade do processador:** A velocidade da CPU do dispositivo.
- **Tipo de processador:** O tipo da CPU do dispositivo.

Do console, você pode , ver um inventário detalhado, e definir o dispositivo como alvo de uma ação, por exemplo, alvo da execução de um relatório.

Clicar duas vezes em um dispositivo na lista **Todos os dispositivos** abre o Console de informações do servidor, que contém as informações de resumo do dispositivo, as configurações, as opções de controle remoto e as informações de conjunto de regras de alertas.

## Grupos públicos

A lista **Grupos públicos** mostra grupos de dispositivos que foram criados por um usuário com direitos de Administrador. Esses grupos são visíveis aos outros usuários.

Esta lista também mostra grupos de chassis de blades que são automaticamente criados quando um CMM (Chassis Management Module ou Módulo de gerenciamento de chassi) é adicionado à lista de dispositivos gerenciados. O grupo lista o CMM e cada servidor blade associado que você está gerenciando. Não é possível editar um grupo de chassis do mesmo modo que se edita um grupo que você tiver criado.

Grupos podem ser estáticos ou dinâmicos. Grupos dinâmicos contêm dispositivos que satisfazem critérios de filtro pré-definidos, por exemplo, velocidade do processador, SO do dispositivo ou um atributo personalizado, como o tipo do dispositivo. Grupos estáticos incluem uma lista fixa de dispositivos, outros grupos estáticos ou grupos dinâmicos.

## Grupos privados

A lista **Grupos privados** mostra grupos de dispositivos criados pelo usuário atualmente conectado. Grupos privados não são visíveis a outros usuários, portanto, não podem ser usados por outros usuários.

# Ícones de dispositivos

Os ícones de dispositivos são mostrados na lista **Todos os dispositivos** e mostram o estado de funcionamento atual de cada dispositivo. Você pode atualizar o estado de funcionamento dos dispositivos, um de cada vez, ao selecioná-los na lista **Meus dispositivos** e clicar no botão da barra de ferramentas **Atualizar**.

A tabela a seguir relaciona os possíveis ícones de status e dispositivo, bem como seus significados:

| Ícone | Descrição |
|---|---|
|  | Dispositivo com o estado Normal |
|  | Dispositivo com o estado Aviso |
|  | Dispositivo com o estado Crítico |
|  | Dispositivo com o estado Desconhecido |

## Utilização dos menus de atalho

Menus de atalho (contexto) estão disponíveis para todos os itens do console, inclusive grupos, dispositivos, consultas, tarefas agendadas, scripts, etc. Os menus de atalho proporcionam acesso rápido às tarefas comuns e às informações críticas de um item.

Para ver o menu de atalho de um item, clique nele com o botão direito. Por exemplo, ao clicar com o botão direito em um dispositivo gerenciado na lista **Meus dispositivos**, o seu menu de atalho geralmente mostrará as seguintes opções:

- **Remover do grupo:** Remove o item de um grupo definido pelo usuário.
- **Alvos:** Transfere o dispositivo selecionado para a lista Dispositivos alvo. **Nota:** se os dispositivos alvo não aparecerem na **Lista de alvos**, clique em **Atualizar** na guia **Dispositivos alvo**.
- **Fazer ping ao dispositivo:** Verifica se o dispositivo está ativo.
- **Fazer tracert para o dispositivo:** Envia um comando de rota de traço para ver um pacote de rede ser enviado e recebido e o número de saltos necessários para o pacote chegar ao destino.

A ajuda não cobre todos os menus de atalho de cada item do console, mas recomendamos que você clique com o botão direito em qualquer item para ver as opções disponíveis.

## Uso das ferramentas

As ferramentas estão disponíveis no painel esquerdo. Use as setas na parte superior do painel para ver todas as ferramentas.

Um administrador vê todas as ferramentas no painel de navegação esquerdo. Os outros usuários podem ver apenas as ferramentas (os recursos) permitidas pelos seus direitos atribuídos. Por exemplo, se um usuário não tem o direito Relatórios, a ferramenta Relatórios não será exibida no painel de navegação esquerdo.

A seguir, é apresentada uma lista completa das ferramentas:

- **Atualizações de software:** Download de pacotes de atualização aplicáveis
- **Scripts:** Cria e gerencia scripts.
- **Tarefas agendadas:** Mostra todas as tarefas (originadas na Configuração de agentes, Vulnerabilidades, Descoberta de dispositivo, ou Scripts) no Agendador.
- **Monitoração:** Monitora o desempenho em tempo real dos dispositivos gerenciados, utilizando uma ampla gama de atributos.
- **Alertas:** Configura alertas, definindo os limites e a resposta que o produto usará se um limite for excedido.
- **Configuração de agentes:** Permite fazer configurações de agentes IPMI (Baseboard Management Controller), Linux ou Windows.
- **Descoberta de dispositivos:** Localiza dispositivos na rede, que não foram analisados e cujos dados não se encontram no banco de dados núcleo.
- **Logs:** Mostra o log de Alerta, exibindo os alertas que você marcou como os que quer ver nos dispositivos gerenciados.
- **Relatórios:** Gerencia relatórios de serviço pré-definidos.

- **Consultas:** Cria e modifica consultas no banco de dados para isolar dispositivos específicos que satisfaçam critérios determinados.
- **Usuários:** Controla o acesso dos usuários a ferramentas e dispositivos de acordo com seus direitos e escopo.
- **Preferências:** Permite criar atributos de inventário personalizados e ver informações sobre o licenciamento.
- **Configuração de hardware:** Abre uma janela separada com as opções de configuração para dispositivos Intel* AMT.

Quando você clica no nome de uma ferramenta, a sua janela é aberta no painel direito.

## Exibição das propriedades de dispositivos

Na tela **Meus dispositivos**, você pode exibir rapidamente informações sobre um dispositivo, clicando no dispositivo na lista e selecionando **Propriedades** no painel inferior.

Veja outras informações mais detalhadas sobre o dispositivo em seus dados de inventário. Para ver os dados de inventário na tela **Todos os dispositivos**, clique no dispositivo e selecione a guia **Ver inventário** no painel inferior, para abrir a janela completa **Inventário**.

# Como especificar dispositivos-alvo

A lista **Dispositivos alvo** o habilita a completar numerosas tarefas em dispositivos selecionados como, por exemplo, distribuir agentes ou fazer análise para encontrar atualizações de software para um grupo selecionado de dispositivos.

O número recomendado de dispositivos que você deve adicionar à lista é 250 ou menos. Os dispositivos permanecerão na lista até ser atingido o limite de tempo de sua sessão do Console (após 20 minutos de inatividade).

Acrescente dispositivos à lista de **Dispositivos alvo** selecionando-os de qualquer lista de dispositivos. Se os dispositivos desejados não aparecerem na lista, use o botão **Localizar** na barra de ferramentas. Procure um dispositivo específico ou vários clientes usando os caracteres curinga % ou *. Clique no botão **Alvo** da barra de ferramentas para adicionar o dispositivo à lista de **Dispositivos alvo**. Se o botão não estiver visível, clique no botão **<<**.

Se forem encontrados vários dispositivos, selecione aqueles que você deseja adicionar à lista e clique em **Alvo**. Se a lista de dispositivos retornada contiver várias páginas, é necessário clicar em **Alvo** para cada página. Você não pode selecionar dispositivos em várias páginas e clicar nos botões apenas uma vez para todas as páginas. Clique na seta para baixo, na parte inferior da barra de ferramentas, do lado direito, para definir quantos dispositivos quer mostrar por página. É possível mostrar até 500 dispositivos por página. Para mudar o número de dispositivos mostrados na lista, consulte Configurações de página em **Preferências**.

Se houver um ou mais dispositivos na lista **Dispositivos alvo**, você pode executar tarefas como, por exemplo, distribuição de uma configuração de agente para cada dispositivo alvo ou mudar dispositivos não gerenciados para a lista **Meus dispositivos**.

**Para selecionar dispositivos**

1. Na lista **Meus dispositivos** ou na tela **Dispositivos descobertos**, clique no dispositivo que deseja selecionar como alvo para uma ação. Selecione múltiplos dispositivos usando os métodos padrão de seleções múltiplas (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.

No painel inferior, os dispositivos selecionados são mostrados na guia **Dispositivos alvo**. Quando eles são mostrados nessa guia, você pode abrir uma ferramenta (por exemplo, Distribuição de agente) e agendar uma tarefa, a qual pode ser aplicada aos dispositivos alvo. Se tiver selecionado como alvo dispositivos não gerenciados, você pode clicar na guia **Gerenciar** e mudá-los para a lista **Meus dispositivos**.

# Como filtrar a lista de exibição

A lista **Meus dispositivos** tem um ícone de filtro que você pode usar para determinar que dispositivos serão mostrados na lista. É possível filtrar somente por um dos critérios (por nome do dispositivo ou endereço IP) ou combinar os critérios para concentrar-se em um subconjunto de computadores.

**Para filtrar a lista de servidores**

1. Na lista **Meusdispositivos**, clique duas vezes em **Todos os dispositivos** ou navegue para um grupo.
2. Clique em **Filtro**  na barra de ferramentas.
3. Na lista suspensa, selecione **Nome do dispositivo** ou **Endereço de IP**.
4. Defina os parâmetros dos critérios especificados digitando na caixa de texto. Na caixa **Localizar** não são suportados os seguintes caracteres estendidos: < , > , " , ' , !.

   Se você fez um filtro por nome do dispositivo, digite o nome do host ou uma faixa de nomes de computadores. É possível usar caracteres curinga para encontrar nomes de computadores específicos (como *srv).

5. Clique em **Localizar**.

# Utilização de grupos

Você pode organizar os dispositivos em grupos para facilitar o gerenciamento. Você pode criar grupos para organizar dispositivos de acordo com sua função, localização geográfica, departamento, atributos de dispositivo ou qualquer outra categoria que atenda às suas necessidades. Por exemplo, você pode criar um grupo de servidores web para todos os servidores configurados como servidores web ou um grupo que inclua todos os dispositivos executando um SO específico. Clique com o botão direito em um grupo para abri-lo, excluí-lo, ou para definir como alvos todos os dispositivos nele contidos para ações como a  conjunto de regras de alertas e análise de inventário.

A tela principal **Meus dispositivos** contém os seguintes grupos:

- **Todos os dispositivos:** Relaciona todos os dispositivos que podem ser vistos pelo usuário atualmente conectado, com base em seu escopo, em uma lista sem subgrupos. Para o administrador, **Todos os dispositivos** relaciona todos os dispositivos que foram analisados ou movidos para o banco de dados núcleo. Os dispositivos que executam o agentes de gerenciamento padrão são exibidos automaticamente no grupo/pasta **Todos os dispositivos** quando são analisados e colocados no banco de dados núcleo pela análise de inventário. Os usuários, inclusive os administradores, não podem criar grupos em **Todos os dispositivos**.
- **Grupos públicos:** Enumera os grupos/dispositivos que um administrador tenha adicionado a partir do grupo **Todos os dispositivos**, e também os grupos de chassis de blades. O administrador (usuário com direitos de Administrador) pode ver todos os dispositivos desse grupo, ao passo que os outros usuários podem ver apenas os dispositivos permitidos pelo seu escopo. Apenas os administradores podem criar grupos em **Grupos públicos**.
- **Grupos privados:** Relaciona os grupos/dispositivos do usuário atualmente conectado, de acordo com o escopo desse usuário. O usuário pode criar subgrupos de dispositivos apenas em **Grupos privados**. Os usuários podem adicionar dispositivos a seu grupo **Grupos privados**, ou a qualquer um de seus subgrupos, movendo-os ou copiando-os dos **Grupos públicos** e **Todos os dispositivos**. Todos os usuários podem criar grupos em **Grupos privados**.

Para obter mais informações sobre dispositivos que você pode ver e gerenciar na tela de dispositivos, e sobre as ferramentas de gerenciamento que pode utilizar, consulte "Administração baseada em funções".

## Tipos de grupos

Você pode criar e gerenciar dois tipos de grupos:

- **Grupos estáticos**. Um *grupo estático* consiste em dispositivos que você adicionou manualmente ao grupo. Grupos estáticos só podem ser modificados através da adição ou remoção manual de dispositivos.
- **Grupos dinâmicos**. Um *grupo dinâmico* consiste em computadores que satisfazem um definição de um filtro ou consulta. Cad vez que o grupo é expandido, a consulta é resolvida e os resultados exibidos. Por exemplo, um grupo dinâmico pode conter todos os dispositivos atualmente em um estado de Aviso. Nesse caso, os computadores seriam colocados ou removidos do grupo de acordo com suas mudanças de estado.

**Para criar um grupo estático**

1. Na tela de dispositivo do console, clique com o botão direito no grupo-pai (como **Grupos privados**), em seguida, clique em **Adicionar grupo**.
2. Digite um nome para o novo grupo.
3. Selecione **Estático** e clique em **OK**.

Após ter criado um grupo estático, você pode mover ou copiar dispositivos para o grupo selecionando-os de uma lista e clicando em **Mover/copiar** na barra de ferramentas. Você pode

copiar dispositivos da lista **Todos os dispositivos** para um grupo ou mover/copiar dispositivos de outros grupos.

**Para criar um grupo dinâmico**

1. Na tela de dispositivo do console, clique com o botão direito no grupo-pai (como **Grupos privados**), em seguida, clique em **Adicionar grupo**.
2. Digite um nome para o novo grupo.
3. Selecione **Dinâmico** e clique em **OK**.

Após ter criado um grupo dinâmico, você deve criar um filtro para determinar que computadores serão exibidos neste grupo. Você pode especificar um novo filtro ou basear o filtro em uma consulta existente.

**Para criar um novo filtro**

1. Selecione o grupo dinâmico que você criou (isto causará a exibição do botão **Propriedades do grupo** no painel inferior).
2. Em **Propriedades do grupo**, selecione **Criar um novo filtro** e clique em **Novo filtro**.
3. Selecione os critérios do filtro que desejar e clique em **OK**.

**Para criar um filtro baseado em uma consulta existente.**

1. Selecione o grupo dinâmico que você criou (isto causará a exibição do botão **Propriedades do grupo** no painel inferior).
2. Em **Propriedades do grupo**, selecione **Criar um filtro baseado em uma consulta existente**
3. Selecione a consulta existente que desejar usar para filtrar o grupo e clique em **Novo filtro**.
4. Selecione os critérios adicionais de filtro que desejar e clique em **OK**

Se você basear um filtro em uma consulta existente e essa consulta for modificada mais tarde por você ou por outro usuário, o filtro baseado naquela consulta não mudará dinamicamente para refletir a consulta modificada.

# Utilização da guia Ações

Use a guia **Ações** para executar operações em dispositivos selecionados e direcionados (alvo). Você pode excluir dispositivos da lista de computadores gerenciados, ligá-los, desligá-los e reiniciá-los e monitorar conexões com dispositivos gerenciados.

- Excluir dispositivos
- Opções de alimentação
- Monitor de dispositivos

## Excluir dispositivos

A opção **Excluir dispositivos** permite excluir os servidores selecionados (ou alvo) da lista de computadores gerenciados. A função excluir pode excluir um ou vários dispositivos de qualquer grupo (de um grupo padrão ou de um grupo criado pelo usuário) no System Manager. Quando o dispositivo é excluído de um grupo, ele é completamente removido de todas as listas de dispositivos gerenciados/inventariados, inclusive do grupo padrão **Todos os dispositivos**.

Se você estiver excluindo um grande número de dispositivos, o tempo da operação pode esgotar. Se isso acontecer, divida-a em operações menores.

## Opções de ligar / desligar

**Opções de ligar/desligar** lhe permitem desligar, reiniciar, e, no caso de computadores IPMI gerenciados, ligar dispositivos remotos. No caso de servidores não-IPMI, o dispositivo deve ter o agente LANDesk distribuído para ele a fim de poder executar as funções de reinicialização e desligamento. Com computadores IPMI, são necessárias as credenciais IPMI corretas para executar os recursos de ligar, desligar e reinicializar. Se um computador IPMI tiver o agente LANDesk, então você pode executar os recursos de desligar e reinicializar sem as credenciais IPMI. Use o utilitário Configurar serviços para configurar a senha IPMI BMC a ser usada no gerenciamento de servidores IPMI.

**Para usar as opções de ligar/desligar**

1. Na lista **Meus dispositivos**, clique em um dispositivo ou em uma lista de dispositivosalvo.
2. No painel inferior, clique na guia **Ações**.
3. Clique em **Opções de ligar/desligar**.
4. Selecione executar a ação nos dispositivos na lista Dispositivos alvo ou somente nos dispositivos selecionados.
5. Selecione entre as opções a seguir:
    - Reinicialização
    - Desligar
    - Ligar (funciona nos dispositivos habilitados com IPMI Wake on LAN)

6. Clique em **Mostrar a janela de redireção de console** para abrir um contêiner ultra-slim com um lançador (o lançador é muito mais fácil de recompilar para EM64T que o controle TTY).

   Ao ligar ou reinicializar um servidor gerenciado IPMI, você pode abrir uma janela de redireção de console que mostra as informações de inicialização do servidor. Isso pode ser útil se quiser verificar se o servidor está reinicializando. Você também pode usar a janela do console para fazer pausa do processo de reinicialização e mudar as configurações do BIOS no servidor gerenciado.

   Para ver uma janela de redireção de console, o servidor deve ter a Redireção de console através de porta serial habilitada na configuração do BIOS. Os dados do console são enviados para a porta serial. Se houver um cabo conectando-se ao servidor ao console administrador, a redireção do console será feita pelo cabo. Caso contrário, o System Manager inicia uma conexão serial por LAN (SOL) para redirigir os dados da porta serial para a conexão LAN. A conexão SOL fica aberta enquanto a janela do console estiver aberta. Quando os dados do console terminarem de aparecer você deve fechar a janela.

   Quando a janela do console abre, aparece uma segunda janela de mensagem. Você pode fechar a janela de mensagem. Após a janela de redireção do console abrir, mas antes do console mostrar a seqüência de inicialização, pode aparecer caracteres aleatórios. Isso acontece porque o BMC do servidor está enviando mensagens de pulso, as quais são transmitidas na conexão com o console administrador. Os caracteres não aparecem quando o console mostra a tela de inicialização, mas podem reaparecer após o processo de incialização terminar.

## Monitor de dispositivos

Use o Monitor de dispositivos para verificar a conectividade dos dispositivos selecionados. Se um dispositivo perder sua conectividade com a rede, ele não poderá enviar um alerta para o servidor núcleo. O Monitor de dispositivos verifica se os dispositivos ainda são capazes de se comunicar na rede.

1. Na lista **Todos os dispositivos**, clique em um dispositivo ou em uma lista de dispositivosalvo.
2. No painel inferior, clique na guia **Ações** e, em seguida, clique em **Monitor de dispositivos**.
3. Para ver a lista de dispositivos sendo monitorados no momento, clique em **Mostrar dispositivos monitorados**.
4. Digite os minutos entre as varreduras de ping e o número de vezes que o produto tentará se comunicar com um dispositivo.
5. Selecione se deseja executar a ação nos dispositivos na Lista de dispositivos alvo ou em todos os dispositivos no grupo **Todos os dispositivos**.
6. Para parar a monitoração de todos os dispositivos, selecione **Nunca fazer ping de dispositivos**.
7. Clique em **Aplicar**.

Só é monitorado o último grupo de dispositivos alvo. Por exemplo, se você selecionar o dispositivo A e o dispositivo B, e aplicar a monitoração de dispositivos a eles, somente o dispositivo A e o dispositivo B receberão o ping do servidor núcleo. Se você então selecionar o dispositivo C e o dispositivo D como alvo e aplicar a monitoração de dispositivos a eles, somente

o dispositivo C e o dispositivo D serão monitorados, os dispositivos A e B não serão mais monitorados.

# Colunas personalizadas

Use **Colunas personalizadas** para modificar nomes e campos de colunas. Nome é o nome da coluna e um campo contém o(s) atributo(s) que pode(m) aparecer na coluna (se o atributo estiver presente). As mudança que você fizer nas colunas não serão vistas por outros usuários. As mudanças nas colunas personalizadas serão vistas na tela **Meus dispositivos**.

Este produto contém um conjunto de colunas padrão com sete colunas. Não é possível editar o conjunto padrão, mas você pode definir um conjunto de colunas personalizadas para usar como padrão.

Não é recomendável criar colunas personalizadas nas quais possa haver múltiplos nomes de campo. Por exemplo, se você criar um campo Computer.Software.Package.Name e o dispositivo tiver instalado múltiplos pacotes, o System Manager só mostrará um nome de pacote por linha, mesmo se os diferentes nomes de pacotes estiverem no mesmo dispositivo, dessa forma, fazendo com que a lista **Todos os dispositivos** e o dashboard tenham múltiplas entradas para o mesmo dispositivo.

**Para criar um conjunto de colunas personalizadas**

1. No painel de navegação esquerdo, clique em **Preferências**.
2. Clique na guia **Colunas personalizadas**.
3. Clique em **Novo**.
4. Digite um nome para o conjunto de colunas.
5. Na caixa do alto, selecione cada um dos cabeçalhos de colunas desejados e clique em **Adicionar**.

   A caixa mostra uma lista que representa todos os dados do inventário atualmente no banco de dados. Percorra essa lista a fim de selecionar um atributo a ser mostrado na lista de resultados da consulta. Lembre-se de selecionar atributos que ajudarão a identificar os clientes retornados na consulta. Se não conseguir encontrar atributos que deseja exibir, você pode adicioná-los no diálogo Atributos personalizados. Entretanto, esses atributos devem ser atribuídos a computadores para poderem aparecer na caixa de diálogo de consulta.

   **Nota:** Se você selecionar um atributo no banco de dados que tem um relacionamento 1:*, terá entradas duplicadas no dispositivo. Atributos com um relacionamento 1:1 (somente um atributo possível, como, por exemplo, Computer.System.Asset Tag), não mostrarão entradas duplicadas.

6. Para mudar a ordem das colunas, selecione um cabeçalho de coluna e clique em **Mover para cima** ou **Mover para baixo**.
7. Para remover uma coluna, selecione-o e clique em **Remover**.
8. Para mudar o cabeçalho da coluna, selecione-o na caixa inferior, clique em **Editar**, faça suas modificações e pressione **Enter**. Não são suportados os seguintes caracteres estendidos: < , > , ' , " , !.
9. Clique em **OK** para salvar o conjunto de colunas.

10. Para usar o conjunto de coluna personalizada quando aparecer a lista **Todos os dispositivos**, selecione-a e clique em **Definir como conjunto de coluna atual** na barra de ferramentas.

**Para editar um conjunto de colunas personalizadas**

1. No painel de navegação esquerdo, clique em **Preferências**.
2. Clique na guia **Colunas personalizadas**.
3. Selecione o conjunto de coluna personalizada e clique **Editar**.
4. Na caixa do alto, selecione um cabeçalho de coluna e clique em **Adicionar** para adicionar a coluna  (consulte as notas na etapa 5 acima).
5. Para remover uma coluna, selecione-a e clique em **Remover**.

6. Para mudar o cabeçalho da coluna, selecione-o na caixa inferior, clique em **Editar**, faça suas modificações e pressione **Enter**. Não são suportados os seguintes caracteres estendidos: < , > , ' , " , !.
7. Para mudar a ordem das colunas, selecione um cabeçalho de coluna e clique em **Mover para cima** ou **Mover para baixo**.
8. Clique em **OK** para salvar suas mudanças.

# Atributos personalizados

Atributos são características ou propriedades de um dispositivo.  Quanto mais atributos um dispositivo tiver no banco de dados, mais fácil se torna identificá-lo com exclusividade. Você só pode criar atributos personalizados se estiver usando o LANDesk® Server Manager com direito de Administrador. Se forem criados atributos personalizados e adicionados ao banco de dados núcleo, você pode atribuir valores a esses atributos em um dispositivo gerenciado. Se não tiverem sido adicionados atributos personalizados ao banco de dados núcleo, a opção **Designar atributos** não aparecerá na guia **Ações**..

## Para designar atributos personalizados a dispositivos

1. Na lista **Todos os dispositivos**, selecione um ou vários dispositivos.
2. No painel inferior, clique na guia **Ações**.
3. Selecione **Designar atributos** no painel esquerdo.
4. Cada Nome de atributo tem uma lista suspensa de valores. Selecione um valor na lista suspensa para o nome do atributo e repita conforme necessário. Clique em **Dispositivos selecionados**.
5. Clique em **Designar** e, a seguir, clique em **OK**.

Você também pode designar atributos personalizados a múltiplos dispositivos que selecionou como alvo. Se tiver dispositivos na lista Alvos, clique em **Dispositivos alvo** na etapa 4 acima.

# Configurações de página

Use **Configurações de página** para configurar as preferências de tela nas páginas mostrando dispositivos ou gráficos.

1. No painel de navegação esquerdo, clique em **Preferências**.
2. Clique na guia **Configurações de página**.
3. Na lista suspensa **Tipo de gráfico**, selecione o tipo de gráfico que quiser mostrar nos **Relatórios**.
4. No diálogo **Itens/página**, digite o número máximo de itens que quiser mostrar em cada página com paginação. O valor deve ser 500 itens ou menos.

## Modo principiante

Você pode exibir texto ao lado dos botões nas barras de ferramentas para ajudar os novos usuários a identificarem os recursos.  Se esta opção não for selecionada, apenas os ícones aparecerão nas barras de ferramentas. Os ícones continuarão a exibir texto se o ponteiro do mouse passar sobre eles.

1. Para exibir o texto ao lado dos botões nas barras de ferramentas, clique na caixa de seleção **Mostrar texto nas barras de ferramentas**.
2. Clique em **Atualizar**.

# Exibição do console de informações do servidor

Use o console de informações do Servidor para ver um resumo de informações gerais sobre um dispositivo, ver informações do sistema, como informações da CPU ou de ventiladores, monitorar os status de funcionamento e os limites de componentes-chave de um dispositivo, gerenciar vulnerabilidades, ligar, desligar ou reinicializar um dispositivo. O console de Informações do servidor tem as seguintes seções listadas ao lado esquerdo do painel de navegação.

- Informações do sistema
- Atualizações de software
- Monitoração
- Conjuntos de regras
- Opções de alimentação
- Configuração de hardware

A fim de ver o console de informações do servidor para um dispositivo, primeiro é necessário distribuir o agente de gerenciamento padrão naquele dispositivo (consulte Configuração de agentes). O dispositivo também deve ser reinicializado após a instalação do agente para que o console de informações do servidor funcione corretamente. Essa reinicialização é necessária quando você instalar o agente no servidor núcleo e nos dispositivos gerenciados.

**Para exibir o console de informações do servidor**

1. Na tela **Meus dispositivos**, clique duas vezes no nome do dispositivo.

   O console abre em uma nova janela de navegador e exibe a página **Resumo de funcionamento**, como padrão.

2. Clique nos botões do painel de navegação esquerdo para ver as informações do servidor e usar as ferramentas disponíveis.

# Informações do sistema

**Informações do sistema** contém dados do resumo sobre o funcionamento do dispositivo assim como informações sobre hardware e software, logs do sistema e outros dados como informações de recursos e da rede.

## Resumo do funcionamento

A página **Resumo do funcionamento** fornece uma visão geral rápida do funcionamento do sistema para este dispositivo. Você pode ver rapidamente se os elementos de um determinado hardware estão funcionando corretamente e se há problemas potenciais que podem precisar de resolução.

Quando um dos elementos do funcionamento estiver em um estado de aviso ou crítico, o botão correspondente mostra um ícone amarelo (aviso) ou vermelho (crítico) indicando a existência de um problema. Clique no botão para ver a descrição do evento que causou o alerta de aviso ou crítico.

## Resumo do sistema

Use a página **Resumo do sistema** para ver importantes informações sobre o dispositivo selecionado. As informações relacionadas na página podem incluir o seguinte, dependendo do tipo de hardware e software configurados no dispositivo.

- **Funcionamento:** O estado de funcionamento geral do dispositivo conforme definido pelas condições e parâmetros por você configurados.
- **Tipo:** O tipo do dispositivo, como, por exemplo, de impressão, de aplicativos ou de banco de dados.
- **Fabricante:** O fabricante do dispositivo.
- **Modelo:** O modelo do dispositivo.
- **Versão do BIOS:** A versão do BIOS do dispositivo.
- **Sistema operacional:** O sistema operacional do dispositivo.
- **Versão do SO:** O número da versão do sistema operacional.
- **CPU:** O fabricante, modelo e velocidade do processador do dispositivo.
- **Analisador de vulnerabilidades:** A versão do analisador de vulnerabilidade.
- **Controle remoto:** A versão do agente do controle remoto.
- **Distribuição de software:** A versão do agente da distribuição de software.
- **Varredura de inventário:** A versão do analisador de inventário.

- **tipo do IPMI, versão do IPMI:** O tipo e número da versão do IPMI que o dispositivo está usando.
- **Versão do SDR:** A versão SDR (Sensor Data Record) no BMC do dispositivo.
- **Versão do BMC:** A versão do BMC (Baseboard Management Controller) do dispositivo.
- **Kernel:** O número da versão do kernel instalado para os dispositivos Linux.
- **Monitoração:** O número da versão do agente de monitoração do dispositivo.
- **Uso da CPU:** Porcentagem em uso do processador.
- **Memória física utilizada*:** A porcentagem do total de memória física utilizada no dispositivo.
- **Memória virtual utilizada*:** A porcentagem do total de memória virtual utilizada no dispositivo.
- **Última inicialização*:** A data e o horário em que o dispositivo foi reinicializado pela última vez (de acordo com o fuso horário do banco de dados).
- **Unidade:** As unidades no dispositivo com o tamanho total da unidade e porcentagem de espaço utilizado.

Essas informações são obtidas no registro do Windows ou dos arquivos de configuração no Linux.

*Essa informação aparece quando o agente tiver sido instalado no dispositivo.

## Hardware

Use a página **Hardware** para ver os detalhes sobre a configuração de hardware do dispositivo. Os itens na lista **Hardware** são agrupados nas seguintes categorias. Observe que nem todas as categorias aparecem para todos os dispositivos. Por exemplo, se o dispositivo não tiver sensores de ventilador e temperatura, a categoria **Resfriamento** não aparecem nesta lista.

- **CPU:** Processadores e cache
- **Armazenamento:** Unidades lógicas, unidades físicas, mídias removíveis e adaptadores de armazenamento
- **Memória:** Informações sobre o uso e módulos de memória
- **Chassis:** O chassi do servidor; mostra se a caixa está aberta ou fechada
- **Dispositivos de entrada:** Teclado, mouse e outros dispositivos
- **Motherboard:** Motherboard, slots de expansão e BIOS
- **Resfriamento:** Sensores de ventilador e temperatura
- **Alimentação:** Fontes de alimentação e voltagem

**Configuração dos limites de alerta para itens de hardware**

Alguns itens na lista **Hardware** representam dados dos sensores no dispositivo, como os sensores de temperatura. Se um dispositivo gerenciado tiver componentes com sensores suportados, é possível mudar a leitura do sensor que disparou o alerta. Por exemplo, um sensor de temperatura de CPU pode ter leituras baixas e altas de temperatura que disparam os alertas de aviso e críticos. Os limites são normalmente baseados nas definições recomendadas do fabricante, mas você pode mudar as configurações altas e baixas usando a caixa de diálogo **Limites**.

1. No console de informações do servidor, clique em **Informações do sistema**.

2. Expanda a pasta **Hardware** e procure o elemento de hardware desejado (por exemplo, **Resfriamento| Temperaturas**).
3. Na lista dos sensores, clique duas vezes no sensor ao qual quiser configurar limites.
4. Digite os valores nos quadros de texto de limites menores e/ou maiores ou arraste as barras para a esquerda ou para a direita para mudar os valores.
5. Clique em **Atualizar** para salvar suas mudanças.
6. Para voltar para os valores originais para os limites, clique em **Restaurar padrões**.

## Logs

A página Logs mostra os logs dos sistemas locais, o SEL (System Events Log) para dispositivos IPMI e um log de alerta.

Logs locais, como logs de Aplicativos, de Segurança e de Systema não têm botões para limpar o log do console, mas podem ser vistos e limpos com o Gerenciamento de computador do Windows.

Se o BIOS desse dispositivo tiver a habilidade de limpar o logo do SMBIOS, clique no botão **Limpar log** para remover todas as entradas do log. Esse botão não está disponível se o BIOS não suportar essa ação.

## Software

A página **Software** mostra as informações de resumo sobre os processos, serviços e pacotes neste dispositivo, assim como uma lista de variáveis atuais de ambiente.

- **Processos:** Mostra os processos que estão sendo executados; selecione um processo e clique em **Eliminar processo** para terminá-lo.
- **Serviços:** Mostra os serviços disponíveis no dispositivo e seu status; selecione um serviço e clique em **Parar**, **Iniciar** ou **Reiniciar** para fazer as mudanças
- **Pacotes:** Relaciona os pacotes instalados com números de versões e nome do fornecedor
- **Ambiente:** Relaciona as variáveis de ambiente definidas no momento para o dispositivo

## Outros

A página **Outro** mostra as informações sobre os recursos e um resumo do hardware e conexões da rede.

- **Informações de recursos:** Mostra e edita informações sobre o gerenciamento de recursos, como por exemplo local e número de etiqueta patrimonial; é também possível mostrar as informações do sistema como número de série, fabricante e tipo de chassi
- **Informações da rede:** Mostra uma lista do hardware de rede instalado, estatísticas da atividade na rede, um resumo de configuração (inclusive endereço IP, endereço padrão do gateway e informações sobre WINS, DHCP e DNS) e uma lista das conexões atuais da rede (unidades mapeadas)

# Atualizações de software

Use a página **Atualizações de software** para analisar as vulnerabilidades detectadas no dispositivo selecionado.

**Para verificar as vulnerabilidades detectadas**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em uma nova janela do navegador.

2. No painel de navegação esquerdo, clique em **Atualizações de software**.

**Descrições de colunas**

- **ID:** Identifica a vulnerabilidade com um código alfanumérico exclusivo, definido pelo fornecedor.
- **Gravidade:** Indica o nível de gravidade da vulnerabilidade. Os níveis possíveis de gravidade são: Service Pack, Crítica, Alta, Média, Baixa, Não aplicável (N/A) e Desconhecida.
- **Título:** Descreve a natureza ou alvo da vulnerabilidade em um breve texto.
- **Idioma:** Indica o idioma do SO afetado pela vulnerabilidade.
- **Data de publicação:** Indica a data em que a vulnerabilidade foi publicada pelo fornecedor.
- **Instalação silenciosa:** Indica se o arquivo do patch associado à vulnerabilidade será instalado silenciosamente (sem interação com o usuário). Algumas vulnerabilidades podem ter mais de um patch. Se algum dos patches da vulnerabilidade não puder ser instalado silenciosamente, o atributo da vulnerabilidade **Instalação silenciosa** mostrará **Não**.
- **Reparável:** Indica se a vulnerabilidade pode ser consertada com a distribuição e instalação do arquivo de correção. Os possíveis valores são os seguintes: Sim, Não e Alguns (para uma vulnerabilidade que inclua várias regras de detecção e nem todas as vulnerabilidades detectadas podem ser reparadas).

# Monitoração

Use a **Monitoração** para ver contadores e gráficos, e para definir limites para componentes de dispositivos. Para mais informações sobre esse recurso, consulte a seção Monitoração do dispositivo.

**Para selecionar um contador de desempenho a monitorar**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em uma nova janela do navegador.

2. No painel de navegação esquerdo, clique em **Monitoração**.
3. Clique na guia **Configurações do contador de desempenho**.
4. Na coluna **Objetos**, selecione o objeto que deseja monitorar.
5. Na coluna **Instâncias**, selecione a instância do objeto que deseja monitorar, se aplicável.
6. Na coluna **Contadores**, selecione o contador específico que deseja monitorar.

7. Especifique a freqüência de sondagem (polling) e o número de dias em que o histórico deverá ser mantido.
8. Na caixa de texto **Alertar após o contador estar fora do intervalo**, especifique o número de vezes que o contador poderá ultrapassar o limite antes de ser gerado um alerta.
9. Especifique os limites superior e/ou inferior.
10. Clique em **Aplicar**.

**Para ver um gráfico do desempenho de um contador monitorado**

1. Clique na guia **Contadores de desempenho ativos**.
2. Selecione um contador na lista.
3. Na lista **Contadores**, selecione o contador do qual deseja ver um gráfico do desempenho.
4. Selecione **Visualizar dados em tempo real** para ver um gráfico do desempenho atual ou selecione **Visualizar dados do histórico** para ver um gráfico mostrando o desempenho durante o período que você especificou (Manter histórico) ao selecionar o contador.

No gráfico de desempenho, o eixo horizontal representa o tempo decorrido. O eixo vertical representa as unidades sendo medidas, como bytes por segundo (ao monitorar transferências de arquivos, por exemplo), Porcentagem (ao monitorar a porcentagem de CPU em uso) ou bytes disponíveis (ao monitorar o espaço em discos rígidos).

## Conjuntos de regras

Use a página **Conjuntos de regras** para ver uma lista de configurações de alertas e conjuntos de regras de monitoração designadas a um dispositivo selecionado, e para ver os detalhes de cada alerta.

**Para ver os conjuntos de regras de alerta**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console se abre em uma nova janela do navegador.
2. No painel de navegação esquerdo, clique em **Conjuntos de regras**.
3. Clique na guia **Conjuntos de regras de alerta**.

O texto a seguir descreve os detalhes fornecidos sobre cada alerta. Para mais informações sobre a modificação desses detalhes, consulte Uso de alertas.

- **Quando o estado atingir:** Quando o estado do alerta atingir o estado exibido, será gerado um alerta.
- **Afeta o funcionamento:** Se o estado de alerta atingir o limite especificado, o estado afeta o funcionamento geral do dispositivo. A seleção de um alerta que afeta o funcionamento é determinada no diálogo de Conjuntos de regras de alerta.
- **Nome do conjunto de regras:** O nome do conjunto de regras do alerta, como definido no diálogo Conjuntos de regras do alerta.
- **Tipo de alerta:** O tipo de alerta a ser gerado, por exemplo, um email, uma interceptação SNMP ou a execução de um programa.
- **Configuração de ação:** A ação que ocorre quando o alerta é gerado, conforme definida no diálogo Conjunto de regras da ação.
- **Nome do manipulador:** O manipulador associado com o alerta, por exemplo, um manipulador de email.

- **Instância:** Indica a origem específica do alerta.

**Para exibir os conjuntos de regras de monitoração**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em uma nova janela do navegador.
2. No painel de navegação esquerdo, clique em **Conjuntos de regras**.
3. Clique na guia **Conjuntos de regras de monitoração**.

O texto a seguir descreve os detalhes fornecidos sobre cada conjunto de alerta de monitoração. Para mais informações sobre a modificação desses detalhes, consulte Sobre a monitoração.

- **Nome:** O nome da configuração do conjunto de regras, como definido na página Monitoração.
- **Nome do conjunto de regras:** Se o conjunto de regras é ou não padrão.
- **Ativado:** O conjunto de regras foi ou não ativado para executar no dispositivo.
- **Aviso de limite:** O limite no qual, se excedido, o dispositivo enviará uma mensagem de advertência ao núcleo.
- **Limite crítico:** O limite no qual, se excedido, o dispositivo enviará uma mensagem crítica ao núcleo.
- **Verificar a cada:** A freqüência na qual o item é monitorado.

## Opções de ligar / desligar

**Opções de ligar/desligar** permitem desligar, reiniciar, e, no caso de dispositivos IPMI e Intel AMT gerenciados, ligar dispositivos remotos. No caso de dispositivos não-IPMI, o servidor deve ter o agente LANDesk distribuído para ele a fim de ele poder executar as funções de reinicialização e desligamento.

Com dispositivos IPMI e Intel AMT, você deve ter configurado as credenciais corretas para executar os recursos de ligar, desligar e reinicializar. Se dispositivos IPMI ou Intel AMT tiverem o agente LANDesk você pode executar os recursos de desligamento e reinicialização sem as credenciais IPMI ou Intel AMT. Para configurar as credenciais BMC nos dispositivos IPMI ou as credenciais do dispositivo Intel AMT, use o utilitário Configurar serviços (consulte Configuração de serviços e credenciais).

**Para utilizar as opções de ligar/desligar no dispositivo selecionado**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console se abre em uma nova janela do navegador.
2. No painel de navegação esquerdo, clique em **Opções de ligar/desligar**.
3. Selecione entre as opções a seguir:

   -  Reinicialização
   -  Desligar
   -  Ligar

## Configuração de hardware

A ferramenta **Configuração de hardware** o habilita a definir opções para dispositivos com capacidade IPMI ou Intel* AMT. Essa ferramenta e quaisquer opções só são mostradas nos dispositivos com hardware correspondente (por exemplo, opções IPMI mostradas somente se o dispositivo for reconhecido como IPMI).

É possível gerar IDs para configurar dispositivos Intel AMT, mostrar os IDs gerados e mudar as opções de configuração relacionadas para configurar dispositivos Intel AMT. Também é possível definir diretivas do disjuntor, que detecta e bloqueia atividades suspeitas da rede para os dispositivos e habilitar a monitoração Presença do agente e assegurar que os agentes de gerenciamento nos seus dispositivos estejam funcionando continuamente. (Para mais informações, consulte Suporte Intel AMT.)

Para os dispositivos IPMI, você pode personalizar as opções de configuração como temporizador de alimentação e configurações do usuário BMC. É também possível configurar o uso de um canal LAN ou SOL (serial over LAN) para manter comunicações fora da banda com um dispositivo IPMI. (Para mais informações, consulte Configuração BMC IPMI.)

Para os dispositivos com o Dell* DRAC (Remote Access Controller), é possível mostrar os logs Dell DRAC e editar os nomes de usuários para acesso ao OpenManage Server Administrator. (Para mais informações, consulte Gerenciamento dos dispositivos Dell DRAC.)

# Gerenciamento de dispositivos Intel* AMT

Quando um dispositivo Intel* AMT é descoberto e adicionado ao banco de dados para ser gerenciado, ele pode ser gerenciado de forma limitada mesmo se ele não tiver um agente LANDesk instalado. (Consulte Descoberta de dispositivos Intel* AMT se precisar de mais informações sobre a descoberta e transferência de dispositivos para o banco de dados núcleo.)

A seguinte tabela contém as opções de gerenciamento disponíveis para um dispositivo que tiver somente Intel AMT em vez de Intel AMT e um agente de gerenciamento System Manager instalado.

| | Somente Intel AMT | Intel AMT e agente | Somente agente |
|---|---|---|---|
| Inventário | resumo | X | X |
| Log de eventos | X | X | X |
| Gerenciador de inicialização remota | X | X | |
| Desativar rede do SO | | X | |

| | Somente Intel AMT | Intel AMT e agente | Somente agente |
|---|---|---|---|
| Ativar rede do SO | | X | |
| Forçar vulscan na reinicialização | | X | |
| Histórico do inventário | | X | X |
| Controle remoto | | X | X |
| Bate-papo | | X | X |
| Transferência de arquivos | | X | X |
| Execução remota | | X | X |
| Ativar | | X | X |
| Desligar | | X | X |
| Reinicialização | | X | X |
| Varreduras de inventário | | X | X |
| Tarefas agendadas e diretivas | limitado | X | X |
| Agrupar opções | | X | X |
| Executar relatório de inventário | | X | X |
| Alertas de Intel AMT | | X | X |

**Para ver o resumo de inventário da Intel AMT para um dispositivo**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.

2. No console de informações do servidor, clique em **Opções Intel AMT**.
3. Clique em **Resumo de inventário**.

O resumo mostra o GUID do dispositivo, produto e fabricante, número de série e BIOS, processador e resumos de memória e o número da versão do Intel AMT. Se alguma informação estiver faltando você pode atualizar os dados clicando em **Atualizar inventário**.

## Acesso a dispositivos configurados para modo Empresa

Quando um dispositivo Intel AMT é configurado para o modo Empresa, o servidor núcleo instala um certificado no dispositivo para proteger a comunicação. Se o dispositivo for ser gerenciado por outro servidor núcleo, ele deve ser desconfigurado e reconfigurado pelo novo servidor núcleo. Se isso não for feito, o acesso à Intel AMT do dispositivo não responderá pois o novo servidor núcleo não tem certificado correspondente. Da mesma forma, se outro computador tentar acessar a funcionalidade Intel AMT no dispositivo, ele não terá sucesso pois não tem certificado correspondente. (Consulte Suporte a Intel* AMT para ver as informações sobre a configuração de modos.)

## Log de evento de Intel AMT

O System Manager fornece uma janela para o log de evento gerados pelos dispositivos Intel AMT. As configurações determinam que eventos são capturados no log. Você pode ver a hora/data do evento, a origem do evento (Coluna Entidade), uma descrição e a gravidade que é determinada pelas configurações da Intel AMT (Crítico ou Não-crítico). Os dados do log também podem ser exportado em formato de valor separado por vírgula (CSV).

**Para ver o log de evento da Intel AMT**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. No console de informações do servidor, clique em **Informações do sistema**.
3. Expanda **Logs** e clique em **Log Intel AMT**.
4. Para exportar o log para um arquivo de formato CSV, clique no botão **Exportar** na barra de ferramentas e especifique um local onde salvar o arquivo.
5. Para limpar todos os dados no log, clique no botão **Purgar log** na barra de ferramentas.
6. Para atualizar as entradas de log, clique no botão **Atualizar** na barra de ferramentas.

## Opções de energia do Intel AMT

System Manager contém opções para ligar e desligar dispositivos Intel AMT. Essas opções podem ser usadas mesmo quando o sistema operacional do dispositivo não estiver respondendo, desde que o dispositivo esteja conectado à rede e tenha alimentação de espera.

Quando o System Manager inicia os comandos de opção de energia, não é possível, em alguns casos, verificar se os comandos são suportados no hardware recebendo o comando. Alguns dispositivos com o Intel AMT podem não suportar todos os recursos de opção de energia (por exemplo, um dispositivo pode suportar a reinicialização IDE-R do CD mas não de um disquete). Consulte a documentação do fabricante de hardware se uma opção de energia não estiver funcionando com um dispositivo em particular. É também possível checar atualizações de

firmware ou BIOS da Intel para o dispositivo se as opções de energia não funcionarem conforme esperado.

Ligue ou desligue a alimentação do dispositivo, ou reinicialize e especifique a forma pela qual quer que dispositivo seja reinicializado. As opções são explicadas na tabela abaixo.

| | |
|---|---|
| Desligar | Desliga a alimentação do dispositivo |
| Ligar | Liga a alimentação no dispositivo. |
| Reinicialização | Desliga e liga a alimentação no dispositivo. |
| Inicialização normal | Inicia o dispositivo com o uso da seqüência de inicialização que tiver sido definida no mesmo |
| Inicializa de um disco rígido local | Força uma inicialização do disco rígido do dispositivo independente do modo de inicialização padrão no dispositivo |
| Inicializa de uma unidade de CD/DVD | Força uma inicialização do CD ou do DVD do dispositivo independente do modo de inicialização padrão no dispositivo |
| Inicialização do PXE: | Ao ser iniciado, o dispositivo habilitado com PXE procura um servidor de PXE na rede, se encontrar, a sessão é iniciada no dispositivo |
| Inicialização de IDE-R | Reinicializa o dispositivo com o uso da opção de redireção de IDE selecionada (veja adiante) |
| Entre na configuração do BIOS | Quando o dispositivo é iniciado, ele permite ao usuário entrar na configuração do BIOS |
| Mostra a janela de redireção do console | Quando o dispositivo é inicializado, ele o faz em modo serial pela LAN a fim de mostrar a janela de redireção do console |
| Redireção de IDE: Reinicializa do disquete | Quando o dispositivo é inicializado, ele o faz de uma unidade de disquete ou de uma imagem especificada (os arquivos de imagem em disquete |

| | |
|---|---|
| | devem estar no formato .img; veja a nota adiante) |
| Redireção de IDE: Reinicializa do CD/DVD | Quando o dispositivo é inicializado, ele o faz de uma unidade de CD ou de uma imagem especificada (os arquivos de imagem em CD devem estar no formato .iso; veja a nota adiante) |
| Redireção de IDE: Reinicializa de um arquivo de imagem especificado | Na inicialização do dispositivo, ele começa a partir do arquivo de imagem especificado (veja a seguir) |

**Para usar as opções de alimentação Intel AMT**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. No console de informações do servidor, clique em **Opções de energia**.
3. Selecionar um comando de alimentação Se selecionar **Reinicializar**, selecione uma opção de incialização.
4. Clique em **Enviar** para iniciar o comando.

## Notas sobre o uso das opções de redireção de IDE

Para usar as opções de redireção de IDE, um disquete de inicialização ou disquete com arquivo de imagem e um CD/DVD de incialização ou CD/DVD com arquivo de imagem devem ser especificados. Os arquivos de imagem em disquete devem estar no formato .img e os arquivos de imagem em CD devem estar em formato .iso. Alguns BIOS podem exigir que a imagem de CD esteja localizada em disco rígido.

Normalmente, a Intel AMT lembra das últimas configurações IDE-R, mas o System Manager limpa as configurações após 45 segundos, portanto, em inicializações subseqüentes ela não reinicia o recurso IDE-R. A sessão de IDE-R em um dispositivo Intel AMT dura 6 horas ou até o console do System Manager ser desligado. As operações IDE-R ainda em andamento após 6 horas são terminadas.

## Como forçar a análise de vulnerabilidade e desabilitar o acesso à rede em computadores Intel AMT

Quando um dispositivo configurado com Intel AMT tem o agente do LANDesk instalado, este contém a funcionalidade que pode ajudar a resolver problemas relativos a sofware fraudulento ou outros problemas que o impeçam de acessar o dispositivo.

O serviço amtmon.exe é instalado com o agente do LANDesk. Quando esse dispositivo está sendo executado em um dispositivo, você pode forçar uma análise de vulnerabilidade na próxima reinicialização para tentar identificar software fraudulento que possam estar no dispositivo. Se a comunicação com o dispositivo não funcionar, desative a conexão de rede do dispositivo mesmo se o SO não estiver funcionando, o que pode ter sido provocado pelo software fraudulento SO

através do consumo de todos os ciclos da CPU. Ao desativar a conexão de rede o dispositivo é impedido de enviar pacores indesejados pela rede.

Quando um agente do LANDesk é instalado em um dispositivo Intel AMT, as opções a seguir estão disponíveis na página **Opções Intel AMT**:

- **Conexão de rede do sistema operacional:** Clique em **Desativar** para desabilitar a pilha de rede do SO para interromper o acesso à rede; clique em **Ativar** para habilitar o acesso à rede do SO, se tiver sido desativado.
- **Análise de vulnerabilidades após a reinicialização:** Força o analisador de vulnerabilidades a executar na próxima vez em que o dispositivo reinicializar.

Quando um dispositivo não responde ou pode conter um software fraudulento, o uso recomendado é primeiro, executar uma análise de vulnerabilidade na próxima reinicialização para tentar identificar o problema. Se o problema continuar e o computador estiver infetando/atacando a rede, ou se for impossível acessar o dispositivo, há a opção de desativar o adaptador NIC do so.

**Para forçar a análise de vulnerabilidade após uma reinicialização**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. Na janela de console do dispositivo, clique em **Opções Intel AMT**.
3. Clique em **Opções de configuração**, em seguida clique em **Analisar**. Aparece uma mensagem no dispositivo indicando que a análise será executada na próxima vez que o dispositivo reinicializar.
4. Para desligar ou reiniciar o dispositivo, use os recursos do Gerenciador de inicialização remota Intel AMT, acima.

**Para desativar ou ativar a conexão de rede em um dispositivo que não responde**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. Na janela de console do dispositivo, clique em **Opções Intel AMT**.
3. Para desativar a placa da rede do dispositivo para interromper as comunicações com outros dispositivos na rede, clique em **Desativar**. Quando a conexão de rede é desativada, aparece uma mensagem no dispositivo indicando que a placa de rede foi desativada.
4. Se um dispositivo estiver pronto para reconectar à rede, clique em **Habilitar**. Quando a conexão estiver restaurada, aparece uma mensagem no dispositivo indicando que a placa de rede está ativada outra vez.

## Abrir a tela de configuração da Intel AMT

O System Manager inclui um link que permite abrir a Tela de configuração da Intel AMT. Esta é uma interface fornecida pela Intel para ver o status do dispositivo, informações sobre o hardware, o log de eventos Intel AMT, configurações de inicialização remota e configurações da rede. Ela também permite a adição e edição das contas de usuário Intel AMT para o dispositivo. A janela que aparece nesta tela é separada do console do System Manager e qualquer dúvida que tenha a respeito do uso desta interface deve ser dirigida ao suporte técnico do fabricante do dispositivo.

**Para abrir a tela de configuração da Intel AMT**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. Na janela de console do dispositivo, clique em **Opções Intel AMT**.
3. Clique no **Console Intel AMT**, em seguida clique em **Iniciar o console da web Intel AMT**.

# Administração baseada em funções

## Sobre a administração baseada em funções

Use a administração baseada em funções para configurar o acesso de usuário à ferramenta do produto e a outros dispositivos com base em suas funções administrativas no sistema. 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.

Administradores (usuários com direito de Administrador) podem acessar as ferramentas de administração baseada em funções clicando em **Usuários** no painel de navegação esquerdo.

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 funções de acordo com as responsabilidades dos usuários, com as tarefas administrativas que deseja que eles possam executar e com os dispositivos que deseja que eles possam ver, acessar e gerenciar. O acesso aos dispositivos pode ser restrito a uma localização geográfica, como um país, uma região, um Estado, uma cidade ou, até mesmo, um único escritório ou departamento. Ou, pode ser restrito a uma plataforma específica, a um tipo de processador ou a algum outro atributo de hardware ou software. Pela administração com base em funções, você tem controle total sobre quantas funções diferentes serão criadas, quais usuários poderão atuar nessas funções e sobre o tamanho do escopo do acesso aos dispositivos.

### Exemplos de funções administrativas

A tabela a seguir lista algumas das possíveis funções administrativas que podem ser implementadas, as tarefas comuns que cada usuário realizaria e os direitos de que esse usuário precisaria para atuar com eficiência na função.

| Função | Tarefas | Direitos necessários |
|---|---|---|
| !CompanyName! | Configurar servidores núcleo, gerenciar usuários, configurar alertas, integrar outros produtos da empresa, etc. (Naturalmente, os administradores com direitos totais podem realizar qualquer tarefa de gerenciamento). | Administrador (todos os direitos implícitos) |
| Gerenciador de recursos | Descobrir dispositivos, configurar dispositivos, executar o analisador de inventário, ativar o acompanhamento de histórico de inventário, etc. | Descoberta de dispositivos, distribuição de software e gerenciamento de |

| Função | Tarefas | Direitos necessários |
|---|---|---|
| | | consultas públicas |
| Gerenciador de relatórios | Executar relatórios pré-formatados, imprimir relatórios, etc. | Relatórios (necessário para todos os relatórios) |

Estas funções são apenas exemplos. A administração baseada em funções é suficientemente flexível para permitir a criação de tantas funções personalizadas quanto necessárias. É possível atribuir os mesmos direitos a diferentes usuários, mas restringir seu acesso a um conjunto limitado de dispositivos com um escopo reduzido. Até mesmo um administrador pode ter seu escopo limitado, tornando-o, essencialmente, um administrador de uma região geográfica específica ou de um tipo de dispositivo gerenciado. A forma como a administração com base em funções será aproveitada depende dos recursos de rede e pessoal, além das suas necessidades específicas.

Para implementar e fiscalizar a administração com base em funções, basta designar usuários atuais do Windows ou criar e adicionar novos usuários do Windows como usuários do produto, adicionar usuários ao grupo de usuário do Management Suite e, em seguida, atribuir os direitos (aos recursos do produto) e o escopo (aos dispositivos gerenciados) necessários. Siga os procedimentos abaixo:

## Compreensão dos direitos

Os direitos dão acesso a ferramentas e recursos específicos. Os usuários devem ter os direitos necessários para realizar tarefas correspondentes. Por exemplo, para controlar dispositivos remotamente no seu escopo, o usuário deve ter o direito de Controle remoto. Se tiver vários produtos de gerenciamento LANDesk instalados, os direitos podem ser atribuídos a usuários de qualquer console e eles terão efeito em todos os consoles.

Quando não se atribui um direito a um usuário, as ferramentas associadas ao direito não ficarão visíveis para esse usuário no console do produto. Por exemplo, se um usuário não receber o direito de relatórios, os itens de relatórios não aparecem no painel de navegação esquerdo. A tabela abaixo mostra que direitos são requeridos para abrir a ferramenta para o usuário.

| Ferramenta | Direitos necessários para abrir no painel de navegação esquerdo |
|---|---|
| Meus dispositivos | Web console básico |
| Configuração de agentes | Distribuição de software administrador |
| Alertas | Alertas e monitoração |
| Descoberta de dispositivos | Descoberta de dispositivos |

| Ferramenta | Direitos necessários para abrir no painel de navegação esquerdo |
|---|---|
| Monitoração | Alertas e monitoração |
| Consultas | Console básico de web, gerenciamento de Consultas públicas, Relatórios |
| Relatórios | Relatórios, Conformidade de patch, Gerenciamento de patch |
| Tarefas agendadas | descoberta de dispositivo |
| Scripts: | gerenciamento de patch |
| Usuários | !CompanyName! |
| Atualizações de software | Gerenciamento de patch |
| Preferências | Web console básico |
| Configuração de hardware | !CompanyName! |

Veja as descrições abaixo para saber mais sobre cada direito do produto e sobre como eles podem ser usados para criar funções administrativas.

**O escopo controla o acesso aos dispositivos**
Ao utilizar os recursos permitidos por esses direitos, os usuários sempre estarão limitados pelo seu escopo (os dispositivos que poderão ver e manipular).

## !CompanyName!

O direito de administrador fornece acesso total a todas as ferramentas do produto (entretanto, o uso dessas ferramentas continua limitado aos dispositivos que integram o escopo do administrador).

Esse é o direito padrão para um usuário recém-adicionado, a menos que as configurações do Usuário modelo padrão tenham sido modificadas.

O direito de Administrador dá aos usuários a habilidade de:

- Ver e acessar a ferramenta **Usuários** no painel de navegação da esquerda
- Ver o Licenciamento de produtos em **Preferências** no painel de navegação esquerdo.
- Realizar todas as tarefas do produto permitidas pelos outros direitos mostrados abaixo

**Não é recomendada a exclusão do usuário Administrador. S**e você for o último administrador a conectar-se em um console LDSM e entrar no Gerenciamento de computador do Windows e remover o usuário Administrador do grupo Management Suite, pode haver problemas ao tentar entrar no console outra vez. Você continuará conectado como Administrador pelos próximos 20 minutos (que é o limite padrão da sessão), mas quando iniciar uma ação ou atualizar o navegador do console (tecla F5) onde estiver conectado como Administrador, os direitos exclusivos ao Administrador não estarão mais acessíveis. Recomenda-se não apagar o último usuário Administrador em nenhuma hipótese.

**Nota sobre direitos e ferramentas**
O direito de Administrador está exclusivamente associado à ferramenta **Usuários**. Se o usuário não tiver direito de Administrador, esta ferramenta não aparecerá no console.

Todas as ferramentas no console do produto estão associadas ao direito correspondente (como descrito abaixo).

## Descoberta de dispositivos

O direito Descoberta de dispositivos permite aos usuários:

- Encontrar dispositivos na rede que não tenham submetido uma análise de inventário ao banco de dados núcleo do produto de uma das várias maneiras possíveis, como uma análise de rede, uma descoberta de agentes padrão de gerenciamento e descoberta IPMI
- Agendar descobertas periódicas
- Mover dispositivos de Descobertos para Gerenciados

## Gerenciamento de consultas públicas

O direito Gerenciamento de consultas públicas permite aos usuários:

- Criar consultas disponíveis a todos os usuários
- Criar ou excluir consultas públicas
- Modificar/editar consultas públicas existentes

## Relatórios

O direito Relatórios permite aos usuários:

- Ver e acessar a ferramenta **Relatórios** no painel de navegação esquerdo
- Executar relatórios pré-formatados

## Gerenciamento de patch:

O direito de gerenciamento de patch é específico ao recurso de análise de vulnerabilidades. Se precisar de mais informações, consulte "Uso da ferramenta de atualizações de software".

### Web console básico

O direito Web console básico de web dá aos usuários a habilidade de usar os recursos associados a esse direito. Os recursos são mostrados abaixo, junto às exceções no recurso.

- **Meus dispositivos** (o direito não permite a atualização de grupos públicos ou a exclusão de dispositivos na guia **Ações**)
- Mudar preferências (mas não os atributos personalizados)

### Alertas e monitoração

O direito Alertas e monitoração permite aos usuários:

- Monitorar o desempenho de vários componentes do sistema e do SO como, unidades, processadores, memória, processos, bytes/seg transferidos pelo servidor de web do sistema, etc.
- Controlar o funcionamento exato de todos os dispositivos gerenciados
- Personalizar alertas a serem enviados por nível de gravidade (Crítico, Aviso, Informativo, OK, Desconhecido) ou o limite (por exemplo, se o uso do disco rígido exceder 90% da capacidade)
- Escolher a ação a ser executada se um alerta exceder um limite (adicionando informações ao log, enviando email de aviso, executando um programa no núcleo ou em um dispositivo individual ou enviando uma interceptação de SNMP para um console de gerenciamento de SNMP na rede)

## Adição de usuários de produtos

Os usuários do produto podem fazer logon no console do produto e realizar determinadas tarefas em dispositivos específicos da rede.

Na verdade, os usuários do produto não são criados no console. Em vez disso, os usuários aparecem na guia **Usuários** (no painel de navegação esquerdo, clique em **Usuários**) após terem sido adicionados ao grupo LANDesk Management Suite do ambiente de usuários do Windows 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**:

- **Usuário modelo padrão:** Esse usuário é basicamente um modelo de propriedades de usuário (direitos e escopo) usado para configurar novos usuários quando estes são incluídos no grupo LANDesk Management Suite. Em outras palavras, quando um usuário é adicionado a esse grupo no ambiente Windows, 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 todos os computadores padrão for selecionado, qualquer novo usuário colocado no grupo LANDesk Management Suite será adicionado ao grupo **Usuários** com direitos para todas as ferramentas de produto e acesso a todos os dispositivos.

  Você pode mudar as configurações de propriedade para o Usuário modelo padrão clicando com o botão direito nele e em **Editar direitos**. 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, primeiro modifique 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.

- **Administrador padrão:** Esse é o usuário administrativo que estava conectado ao servidor quando o núcleo deste produto foi instalado.

Quando você adiciona um usuário ao grupo LANDesk Management Suite no Windows, ele é automaticamente lido no grupo **Todos os usuários** da janela **Usuários**, herdando os mesmos direitos e o escopo do Modelo padrão de usuário atual. São mostrados o nome, o escopo e os direitos do usuário.

Se você remover um usuário do grupo LANDesk Management Suite no ambiente de usuários do Windows, ele não será mais um usuário ativo da LANDESK e poderá ser apagado do grupo **Usuários**. A conta do usuário permanece no servidor, podendo ser adicionada novamente ao grupo LANDesk Management Suite a qualquer momento. Além disso, os subgrupos do usuário em **Dispositivos do usuário**, **Consultas do usuário**, **Relatórios do usuário** e **Scripts do usuário** 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.

Para atualizar a lista **Usuários**, de modo a exibir usuários recentemente adicionados, clique em **Usuários** e clique no botão **Atualizar** no seu navegador.

**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**, em seguida, 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 ainda não houver contas de usuários no Windows, será necessário 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 Grupos 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.
7. Adicione os usuários ao grupo LANDesk Management Suite para que eles apareçam no grupo Usuários no console.

Agora, você pode atribuir os direitos e o escopo dos usuários do produto.

# Criação de escopos

Um escopo define os dispositivos que podem ser exibidos e gerenciados por um usuário do produto. Se tiver vários produtos de gerenciamento LANDesk instalados, os escopos podem ser atribuídos a usuários de qualquer console e eles terão efeito em todos os consoles.

Um escopo pode ter o tamanho que você quiser, pode abranger todos os dispositivos gerenciados analisados em um banco de dados núcleo, ou, possivelmente, apenas um único dispositivo ou nenhum dispositivo. Essa flexibilidade, aliada ao acesso modular à ferramenta, é o que torna a administração baseada em funções um recurso de gerenciamento tão versátil.

## Escopos padrão

A administração baseada em funções contém dois escopos padrão. Esses dois escopos pré-definidos podem ser úteis ao configurar as propriedades do modelo padrão de usuário.

- **(Padrão) Escopo sem computadores:** Exclui todos os dispositivos no banco de dados.
- **(Padrão) Escopo de todos os computadores:** Inclui todos os dispositivos no banco de dados.

Não é possível editar ou remover os escopos padrão.

## Escopos personalizados

Você pode criar os seguintes tipos de escopos personalizados e atribuí-los a usuários:

- **Baseado em consulta:** Controla o acesso apenas aos dispositivos que correspondam a uma consulta personalizada. É possível selecionar uma consulta existente ou criar novas consultas na caixa de diálogo **Consultar**, para definir um escopo. Para obter mais informações sobre a criação de consultas, consulte "Criação de consultas no banco de dados".

- **Baseado em grupo:**Controla o acesso a apenas aqueles dispositivos localizados no grupo selecionado. Você pode selecionar grupos do diálogo **Propriedades de escopo de grupo** para definir um escopo.

É possível atribuir mais de um escopo a qualquer usuário. Quando escopos múltiplos são atribuídos a um usuário, o escopo cumulativo efetivo (isto é, a gama completa de dispositivos que podem ser acessados e gerenciados como resultado da combinação de escopos atribuídos) é um composto simples.

Você pode personalizar o escopo efetivo de um usuário através da adição ou remoção de escopos a qualquer momento. Todos os tipos de escopo podem ser usados em conjunto.

**Para criar um escopo:**

1. No painel esquerdo de navegação, clique em **Usuários**.
2. Na guia **Escopo**, clique no botão **Novo escopo de consulta** ou **Novo escopo de grupo** na barra de ferramentas.
3. Digite o do novo escopo.
4. Se você selecionou baseado em consulta, escolha uma consulta existente ou clique em **Definir** para criar uma nova consulta. Clique em **OK**.
5. Se você selecionou baseado em grupo, escolha um grupo e clique em **OK**.
6. Clique em **OK** para salvar o escopo e fechar a caixa de diálogo.

# Atribuição de direitos e escopo aos usuários

- Sobre o diálogo Direitos/escopo do usuário
- Sobre o diálogo Configurações do controle remoto

Após adicionar usuários do produto, aprender sobre direitos e como eles controlam o acesso a recursos e ferramentas, e aprender a criar escopos de dispositivos para permitir ou restringir o acesso a dispositivos gerenciados, o próximo passo no estabelecimento da administração baseada em funções é atribuir os direitos apropriados e um escopo a cada usuário.

Os direitos e o escopo de um usuário podem ser modificados a qualquer momento.

Se os direitos ou o escopo de um usuário forem alterados, essas mudanças terão efeito apenas na próxima vez que esse usuário acessar o console.

**Para atribuir direitos e escopo a um usuário:**

1. No painel esquerdo de navegação, clique em **Usuários**.

2. Expanda a lista de usuários para ver todos os usuários que são membros atuais do grupo LANDesk Management Suite no ambiente Windows NT do servidor núcleo.

   Esta lista mostra os nomes dos usuário e os direitos atribuídos (se aparecer um tique ao lado, isso indica que o direito está habilitado ou ativo).

3. Clique com o botão direito em **Editar**.
4. No diálogo **Direitos/Escopos do usuário**, marque ou desmarque os direitos como desejado.
5. Clique na guia **Escopo** e selecione um escopo da lista de **Escopos atribuídos**.
6. Clique em **Aplicar**.

Os novos direitos são exibidos próximos ao nome do usuário na lista, entrando em vigor na próxima vez que o usuário se conectar com o servidor núcleo.

**Para excluir um escopo**

1. No painel esquerdo de navegação, clique em **Usuário**.
2. Na guia **Escopo**, clique no escopo que quiser excluir e clique em **Excluir**. Clique em **OK**.

Tenha cautela ao apagar escopos. Os usuários atribuídos a eles poderão acessar direitos previamente proibidos pelo escopo.

## Sobre o diálogo Direitos / escopos do usuário

Use esse diálogo para ver e modificar os direitos e o escopo atribuídos a um usuário. Abra o diálogo selecionando um usuário e clicando em **Editar direitos**.

**Guia Direitos:** mostra os direitos atribuídos ao usuário.

- **LANDesk Administrador**
- **Descoberta de dispositivos**
- **Gerenciamento de consultas públicas**
- **Relatórios**
- **Gerenciamento de patch:**
- **Web console básico**
- **Alertas e monitoração**

**Guia Escopos:** mostra os escopos atribuídos ao usuário.

- **Escopos atribuídos:** identifica os escopos atuais do usuário.
- **Adicionar:** abre a caixa de diálogo **Adicionar escopo** que permite a seleção de um escopo para adicionar ao usuário.
- **Remover:** Exclui o escopo selecionado.
- **Cancelar:** fecha a caixa de diálogo sem salvar as modificações.

# Descoberta de dispositivos

## Uso da descoberta de dispositivos

A descoberta de dispositivos encontra dispositivos na sua rede que não têm os agentes do núcleo de descoberta instalados e que não enviaram uma análise de inventário para o mesmo banco de dados núcleo. A descoberta de dispositivos encontra dispositivos na rede de várias maneiras.

- **Varredura de rede:** Procura computadores fazendo uma varredura de ping ICMP. Essa é a pesquisa mais completa, porém a mais lenta (se a impressão digital IP for usada). Você pode limitar a pesquisa a determinadas faixas de IP e sub-redes. Como padrão, essa opção usa o NetBIOS para coletar informações sobre o dispositivo. Você também pode selecionar Impressão digital IP, que fornece o tipo de SO na maioria dos casos. A opção de análise de rede também tem uma opção **Usar SNMP**, onde você pode configurar a análise para SNMP para dispositivos SNMP como, por exemplo, algumas impressoras.
- **Descobrimento do CBA:** Procura o agente padrão de gerenciamento (antes denominado agente de base comum, [CBA] no Management Suite) nos computadores. Esta opção descobre os computadores gerenciados pelo Server Manager, System Manager, etc. Você pode selecionar a opção PDS2 para descobrir dispositivos usando o agente PDS2 antigo do LANDesk. 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 os servidores com o IPMI - Intelligent Platform Management Interface ativado, o que permite que você o BMC (baseboard management controller), independentemente de o servidor estar ligado ou desligado ou do estado no qual o SO se encontra.
- **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 os servidores com o Intel Active Management Technology (versão 1) ativado, o que lhe dará acesso a recursos limitados de gerenciamento, independente de o servidor estar ligado ou desligado ou do estado no qual o SO se encontrar-.

A descoberta de dispositivos tenta descobrir informações básicas sobre cada dispositivo. Nem todas as informações abaixo estão disponíveis para todos os dispositivos.

- **Nome do nó:** O nome do dispositivo descoberto, se disponível.
- **Endereço IP:** O endereço IP descoberto.
- **Máscara da sub-rede:** A máscara de sub-rede descoberta.
- **Categoria:** O grupo da descoberta de dispositivos ao qual o dispositivo pertence.
- **Nome do SO:** A descrição do sistema operacional descoberto, se disponível.

Quando a descoberta de dispositivo localiza um dispositivo pela primeira vez, ele verifica no banco de dados núcleo se o endereço IP e o nome do dispositivo já estão no banco de dados na lista **Meus dispositivos**. Um dispositivo na lista **Não gerenciados** será redescoberto e, possivelmente, fornecerá mais dados. Se houver uma correspondência, a descoberta de dispositivos ignora o dispositivo. Se não houver uma correspondência, a descoberta de

dispositivos adiciona o dispositivo à tabela de dispositivos **Não gerenciado**. Os dispositivos na tabela **Não gerenciados** não usam uma licença System Manager. Um dispositivo é considerado gerenciado quando envia uma varredura de inventário ao banco de dados núcleo. Após mover um dispositivo para o grupo **Todos os dispositivos**, o dispositivo não aparece mais na lista de **Dispositivos descobertos**.

Os dispositivos IPMI devem ter um BMC (baseboard management controller) configurado, para serem descobertos como dispositivos IPMI e usar completa funcionalidade IPMI. Se o BMC não estiver configurado, o dispositivo pode ser descoberto como computador. Você poderá, então, acrescentar o dispositivo à lista de dispositivos gerenciados e executar o recurso Configuração de hardware para configurar a senha BMC. A funcionalidade do IPMI do dispositivo será, então, reconhecida por este produto. Observe que o endereço IP do BMC não é, necessariamente, o mesmo que o endereço do IP do SO, assim sendo pode não levar um push de agente direto ao endereço IP do BMC. Pode ser necessária uma redescoberta de IPs padrão para que um agente padrão faça uma instalação por envio (push) ao IP do BMC. O IP do BMC deve ser capaz de instalar um agente por envio IP (push).

Os dispositivos habilitados com Intel* AMT (versão 1) devem ser configurados com nome de usuário e senha Intel AMT para serem reconhecidos e descobertos como dispositivos Intel AMT. Após serem descobertos, você pode rodar o recurso de Configuração de hardware para definir o Intel AMT e disponibilizar o dispositivo no modo Pequena empresa ou no modo seguro Empresa.

Para automatizar a descoberta de dispositivos, você pode agendá-la para que ocorra periodicamente. Por exemplo, você poderia dividir sua rede em três sub-redes e agendar uma varredura de ping para uma das sub-redes a cada noite. Em todas a descobertas, o servidor núcleo é que faz a descoberta.

Para descobrir e gerenciar dispositivos na sua rede, realize as seguinte tarefas:

- Criar configurações de descoberta
- Agendar e executar a descoberta
- Como ver dispositivos descobertos
- Como mover os dispositivos descobertos para a lista **Meus dispositivos**

## Uso da descoberta de dispositivos não gerenciados com firewall

Em geral, a descoberta de dispositivos não gerenciados não descobre dispositivos que usam firewall como, por exemplo, a Windows Firewall, a não ser que você configure manualmente a firewall. É necessário abrir as portas a seguir. Para mudar essas configurações, acesse a Windows Firewall através do Painel de controle do Windows.

**Servidores gerenciados:**

- Compartilhamento de arquivos e impressoras: TCP 139, 445; UDP 137,138 (Por envio não funciona sem isto)
- Distribuição de software: TCP 9595 (Por envio não funciona sem este)
- Avançada - ICMP:  “Permitir requisição de eco de entrada” (Não pode ser descoberto se este não estiver habilitado.)

**Servidor núcleo:**

- Inventário: 5007
- Controle remoto: 9535

# Criação de configurações de descoberta

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. Para ver mais informações, consulte Configuração de análise 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. Para uma visão geral do IPMI, consulte Suporte ao IPMI.
- **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.

**Para editar ou excluir uma configuração**

- Na guia **Configurações de descoberta**, clique na configuração que desejar e clique em **Editar** ou **Excluir**.

## Configuração de análises SNMP

As descobertas de análise de rede podem usar SNMP. Dependendo da sua configuração SNMP da rede, pode ser necessário digitar informações adicionais de SNMP na configuração de descoberta. Se for clicada a opção **Configurar** próxima da opção **SNMP** aparecerá o diálogo **Configuração SNMP**, que tem as seguintes opções:

- **Novas tentativas:** Número de vezes de tentativas de descoberta do dispositivo para a conexão SNMP.
- **Aguardar pela resposta em segundos:** Tempo que a descoberta do dispositivo deve aguardar para uma resposta SNMP.
- **Porta:** A porta onde a descoberta do dispositivo deve enviar as consultas SNMP.
- **Nome de comunidade:** Nome da comunidade que a descoberta do dispositivo deve usar.
- **Configurar SNMP V3:** A descoberta do dispositivo também suporta SNMP V3. Clique neste botão para configurar as opções SNMP V3 no diálogo **Configuração de SNMP V3**.

O diálogo **Configuração SNMP V3** tem as seguintes opções:

- **Nome de usuário:** O nome de usuário que a descoberta do dispositivo deve usar para autenticar-se com o serviço SNMP remoto.
- **Senha:** A senha para o serviço SNMP remoto.
- **Tipo de autenticação:** O tipo de autenticação usado pelo SNMP. Pode ser **MD5**, **SHA** ou **Nenhum**.
- Tipo de **privacidade:** Método de criptografia usado pelo serviço SNMP. Pode ser **DES**, **AES128** ou **Nenhum**.
- Senha de **privacidade:** Senha a ser usada com o tipo especificado de privacidade. Não estará disponível se você selecionar o tipo de privacidade**Nenhum**.

# Agendamento e execução da descoberta

Use o botão **Agendar** na guia **Configuração de descoberta** para abrir a caixa de diálogo **Tarefas agendadas**. Use este diálogo para determinar quando as configurações devem ser executadas. É possível agendar uma configuração de descoberta para ser executada imediatamente, no futuro, ser agendada como uma ação recorrente ou para ser executada somente uma vez.

As tarefas de descoberta podem ser reagendadas ou excluídas na guia **Tarefas de descoberta**. Após agendar uma descoberta, consulte a guia **Tarefas de descoberta**para ver o status da descoberta. Também é possível acessar o status da tarefa de descoberta na ferramenta **Tarefas agendadas**. Uma vez completada uma tarefa de descoberta, novos dispositivos que não estejam no banco de dados do núcleo serão adicionados às categorias de dispositivos descobertos.

A caixa de diálogo **Tarefa agendada** contém as seguintes opções.

- **Mostrar nas tarefas comuns:** Permite a outros usuários verem a tarefa. Quando outro usuário edita ou executa a tarefa, ele se torna o proprietário daquela instância da tarefa.
- **Proprietário:** O proprietário da tarefa.
- **Deixar sem agendar:** (padrão) Deixa a tarefa na lista Tarefas para agendamento 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:
    - **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.
    - **Hora:** A hora em que você deseja que a tarefa inicie.
    - **Repetir a cada:** Se desejar que a tarefa seja repetida, selecione a freqüência da 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 descoberta**

1. No painel de navegação à esquerda, clique em **Descoberta de dispositivos**.
2. Na guia **Configurações da descoberta**, selecione a configuração desejada e clique em **Agendar**. Configure o agendamento da descoberta. Ao terminar, clique em **Salvar**.
3. Monitore o progresso da descoberta na guia **Tarefas de descoberta**.
4. Após a descoberta ser completada, veja os resultados da descoberta no painel superior em **Dispositivos descobertos**. Se você clicar duas vezes na tarefa de descoberta, a quantidade e a porcentagem de dispositivos será zero porque esses números referem-se aos dispositivos alvo e as tarefas de descoberta não têm alvos.

A guia **Tarefas de descoberta** mostra o status da tarefa de descoberta. O status inclui o seguinte:

- O nome da configuração de descoberta.
- O status da tarefa. O status pode ser: Trabalhando, 100% concluído, 0% concluído ou Com falha.
- A última vez que a tarefa foi executada.
- O tipo de execução da tarefa.

**Para excluir ou reagendar uma descoberta**

Se deseja excluir uma tarefa da lista, independente da tarefa ter sido executada ou não, clique na tarefa e clique em **Excluir**. Se a tarefa ainda não tiver sido executada, ou se for uma tarefa recorrente, apagá-la fará com que ela não seja mais executada.

Também é possível reagendar uma tarefa de descoberta na lista para ser executada novamente ou em outro horário, clicando na tarefa, clicando em **Editar**, escolhendo **Agendar**, e reconfigurando a agenda. Para executar mais uma vez a tarefa imediatamente, selecione a tarefa e clique em **Iniciar agora**.

**Para ver o status da tarefa de descoberta**

1. No painel de navegação à esquerda, clique em **Dispositivos descobertos**.
2. Clique na guia **Tarefas de descoberta** ou clique em **Atualizar** na barra de ferramentas do painel.

# Como ver os dispositivos descobertos

Veja todos os dispositivos descobertos no painel superior em **Descoberta de dispositivos**. Esse painel mostra os resultados de todas as descobertas que você tiver executado. Quando você executa uma nova descoberta, os dispositivos encontrados são adicionado essa lista.

Quando a descoberta de dispositivo localiza um dispositivo, ela tenta identificar o tipo, de modo que possa adicioná-lo a uma destas categorias:

- **Chassis:** Contém módulos de gerenciamento (CMMs) de chassis de servidores blade.
- **Computadores:** Contém computadores. Sistemas Linux podem ser rotulados com sistemas Unix na coluna **Nome do SO**.
- **Infra-estrutura:** Contém roteadores e outros hardwares de rede.
- **Intel AMT:** Contém dispositivos com suporte para a Tecnologia Intel* Active Management.
- **IPMI:** Contém dispositivos com o IPMI ativado.
- **Outro:** Contém dispositivos não identificados.
- **Impressoras:** Contém impressoras.

Essas seis categorias ajudam a manter a lista da **Descoberta de dispositivosy** organizada de forma que você possa localizar com mais facilidade os dispositivos nos quais tem interesse. Você pode ordenar as listas de dispositivos por qualquer cabeçalho de coluna clicando em um dos cabeçalhos. Às vezes, a Descoberta de dispositivos pode não classificar os dispositivos corretamente. É possível transferir com facilidade dispositivos identificados incorretamente para o grupo correto clicando no dispositivo que quiser mover e clicando em **Mover**, selecionando a Categoria correta e, em seguida, clicando em **OK**.

De vez em quando, o servidor núcleo é relacionado duas vezes. Isso ocorre porque o mesmo computador é encontrado através de diferentes mecanismos de descoberta (por exemplo, CBA, IPMI, CMM, PDS1 e PDS2) e as informações do computador são acrescentadas ao banco de dados sob aquele mecanismo.

Assim que você distribui agentes para um dispositivo descoberto e o dispositivo envia uma análise de inventário para o núcleo, o dispositivo é removido da lista de dispositivos descobertos.

## Como filtrar a lista de dispositivos

Localize dispositivos que correspondam a critérios de busca que você especificar usando o campo **Filtrar por** na barra de ferramenta. É possível filtrar por Nome do nó, Endereço IP, Máscara de sub-rede, Categoria ou Nome de SO. Quando você usa um filtro, os dispositivos são ordenados alfabeticamente pelo atributo que você filtrou.

**Para filtrar a lista de dispositivos**

1. No painel de navegação esquerdo, clique em **Descoberta de dispositivos**.
2. Na árvore **Não gerenciados**, clique no grupo que deseja filtrar.
3. Em **Filtrar por**, clique no atributo pelo qual deseja filtrar. (Se **Filtrar por** não estiver visível, clique em **>>** para expandi-lo.)
4. Na caixa ao lado do atributo, digite o texto pelo qual deseja filtrar.
5. Clique em **Localizar**.

## Adicionar categorias

É possível criar categorias de dispositivos para agrupar os dispositivos não gerenciados. Se você transferir um dispositivo para outra categoria, ele aparecerá naquele grupo outra vez se a descoberta de dispositivos detectar o dispositivo mais tarde. Ao transferir dispositivos, que você sabe que não serão gerenciados com o Web console, para outros grupos, é possível ver mais facilmente novos dispositivos no grupo **Computadores**.

Se você excluir um grupo que contém dispositivos, a descoberta de dispositivos transferirá os dispositivos para o grupo **Outros**.

**Para adicionar uma categoria de dispositivos**

1. Na tela **Descoberta de dispositivos**, clique em **Adicionar categoria**.
2. Digite um nome para o grupo na caixa **Nome da categoria**, em seguida clique em **OK**.
3. Para apagar uma categoria adicionada, selecione-a, clique em **Excluir categoria** e clique em **OK** para confirmar essa ação.

# Como mover os dispositivos descobertos para a lista Meus dispositivos

Após descobrir dispositivos você pode mudá-los para a lista **Meus dispositivos**. No processo de mudar os dispositivos as respectivas informações são adicionadas ao banco de dados. Quando as informações estiverem no banco de dados, você pode distribuir o agente de configuração de dispositivos, executar consultas e relatórios e realizar muitas outras tarefas de gerenciamento.

Para dispositivos que podem ser gerenciados fora de banda (aqueles com funcionalidade IPMI, Intel AMT ou DRAC) você também tem a opção de gerenciar os dispositivos sem distribuir agente. Quando isso é feito, as informações do dispositivo são salvas no banco de dados e o BMC do dispositivo é configurado de forma que você pode usar os recursos de gerenciamento permitidos pelo hardware de gerenciamento fora de banda.

**Para mover os dispositivos descobertos para a lista Meus dispositivos**

1. Na tela **Descoberta de dispositivos**, clique no dispositivo que quiser mudar para a lista **Meus dispositivos**. Selecione múltiplos dispositivos utilizando as combinações SHIFT+clique ou CTRL+ clique.
2. Clique no botão **Alvo**. Os dispositivos selecionados são mostrados na guia **Lista alvo**.
3. Clique na guia **Gerenciar**.
4. Selecione **Mover dispositivos alvo**.
5. Se os dispositivos podem ser gerenciados fora de banda e você não quer distribuir um agente de gerenciamento, selecione **Gerenciar dispositivos sem agente habilitados fora de banda**.
6. Clique em **Mover**.

Os dispositivos são removidos da lista de dispositivos não gerenciados e aparecem na lista **Meus dispositivos**.

Se selecionar a opção fora de banda, você pode ver o status do processo de mudança clicando na guia **Status da mudança** no painel inferior. Os erros de configuração são aqui registrados. Para mover um dispositivo habilitado com IPMI para a lista **Meus dispositivos**, é necessário fornecer as credenciais apropriadas de BMC no utilitário Configurar serviços a fim de permitir ao servidor núcleo autenticar-se no dispositivo.

Quando você move um módulo de gerenciamento de chassi (CMM) para a lista **Meus dispositivos**, ele é exibido na lista **Todos os servidores** e também como grupo na lista **Todos os dispositivos**. Os detalhes do grupo mostram o CMM e uma lista da baias disponíveis no chassi com o nome dos servidores blade nas baias. Os servidores blade são detectados e gerenciados como servidores individuais.

# Descoberta de dispositivos Intel* AMT

O System Manager inclui a opção de descobrir dispositivos configurados com o Intel® AMT (Intel* Active Management Technology), versão 1. Os dispositivos podem ser descobertos como Intel AMT somente após você ter acessado a Tela de configuração AMT no dispositivo e mudado a senha padrão do fabricante para uma senha protegida. (Consulte a documentação do fabricante para ver as informações sobre o acesso à Tela de configuração Intel AMT.) Se não fizer isso, os dispositivos serão descobertos, mas não serão identificados como Intel AMT e você não poderá ver as mesmas informações de resumo de inventário.

---

Os dispositivos com o Intel AMT versão 2 não são descobertos com o uso deste este processo. Após os IDs de configuração terem sido inseridos na Tela de configuração Intel AMT com o endereço IP do servidor núcleo, o dispositivo é descoberto automaticamente. Consulte Configuração dos dispositivos Intel AMT para mais detalhes sobre como trabalhar com a versão 2.

---

**Para descobrir dispositivos Intel AMT**

1. No painel de navegação à esquerda, clique em **Descoberta de dispositivos**.
2. Clique em **Nova** para criar uma nova configuração e digite um nome para a mesma. Ou, clique em uma configuração já existente e clique em **Editar**, para modificá-la.
3. Cheque a **Descoberta de dispositivos Intel AMT**.
4. Insira os endereços IP iniciais e finais para analisar uma faixa de endereços, e insira uma máscara de sub-rede.
5. Clique em **Adicionar**, em seguida clique em **OK**.
6. Selecione a configuração e clique em **Agendar**. Defina as opções de agendamento ou clique em **Iniciar agora**, em seguida clique em **Salvar**.
7. Para ver o progresso da análise, clique na guia **Descoberta de tarefas**.

Os dispositivos configurados com Intel AMT são mostrados em uma pasta chamada **Intel AMT**. Nesta pasta, você pode selecionar o dispositivo e movê-lo para a lista de dispositivos gerenciados.

Para adicionar o dispositivo ao banco de dados núcleo a fim de gerenciá-lo, é necessário antes configurar o nome do usuário/senha para o dispositivo de forma a coincidir com o nome de usuário/senha no utilitário Configuração serviços, o que permite ao System Manager autenticar no dispositivo. Quando você salva a configuração da senha no utiltiário Configuração de

serviços, ela armazena as informações no banco de dados núcleo para o System Manager poder autenticar em dispositivos Intel AMT.

Se tiver dispositivos Intel AMT com credenciais diferentes, será necessário ter certeza de que essas credenciais coincidam com as do utilitário Configuração de serviços para poder gerenciá-los.

Quando um dispositivo Intel AMT é descoberto e transferido para a lista **Meus dispositivos**, ele é automaticamente configurado com o modo que você selecionou através do utilitário Configuração de serviços. O modo Pequenas empresas fornece gerenciamento básico sem serviços de infra-estrutura e não é protegido, enquanto que o modo Empresa é destinado a empresas de grande porte e fornece segurança com base em serviços de rede como DHCP, DNS e um serviço de autoridade de certificado TLS.

Se o seu núcleo estiver usando um servidor proxy, este servidor deve suportar a Autenticação Digest Access a fim de descobrir os dispositivos Intel AMT.

**Para configurar a senha da tecnologia Intel AMT**

1. Clique em **Iniciar | Todos os programas | LANDesk | Configuração de serviços**. Clique na guia **Configuração Intel AMT**.
2. Digite o nome de 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) para gerenciar os dispositivos Intel AMT.
3. Para mudar o nome de usuário e a senha, preencha a seção **Nova senha Intel AMT**.
4. Selecione o modo (**Pequenas empresas** ou **Empresa**) que quiser usar para configurar dispositivos quando adicioná-los ao banco de dados para gerenciá-los.
5. Clique em **OK**. Essa mudança será feita quando a configuração do cliente for executada.

**Para mover dispositivos Intel AMT descobertos para a lista de dispositivos gerenciados**

1. Clique em um ou mais nomes de dispositivos na lista de dispositivos não gerenciados.
2. Clique no botão **Alvo** na barra de ferramentas.
3. Clique no botão **Gerenciar** no painel inferior, selecione **Mover dispositivos alvo**, em seguida clique em **Mover**.

   Se todos os dispositivos que quiser gerenciar estiverem visíveis na lista, selecione-os, clique no botão **Gerenciar** no painel inferior, selecione **Mover dispositivos selecionados**, em seguida clique em **Mover**.

O dispositivo é removido da lista de dispositivos não gerenciados e aparece na lista **Todos os dispositivos**. Observe que quando você transfere dispositivos para a lista **Meus dispositivos**, a configuração de Intel AMT é executada em um processo separado no background. Você pode continuar a descoberta ou as tarefas de gerenciamento durante esse processo.

Para ver mais informações sobre o gerenciamento de dispositivos Intel AMT, consulte Gerenciamento de dispositivos Intel* AMT e Suporte Intel* AMT.

# Instalação e configuração de agentes de dispositivos

## Visão geral da instalação e configuração de agentes

Para ter a capacidade total de gerenciamento dos dispositivos usando o console, é necessário instalar os agentes neles. Você pode decidir instalar a configuração de agente padrão (a qual instala todos os agentes do produto) ou personalizar a sua própria configuração de agente para instalá-la em seus dispositivos. A instalação de System Manager não instala agentes no núcleo automaticamente; é necessário instalar também os agentes no núcleo, e depois reinicializar o núcleo manualmente. A configuração de agente deve incluir o agente de monitoração para receber alertas de estado de funcionamento.

Você pode instalar os agentes de gerenciamento usando um dos seguintes métodos:

- Distribuindo agentes. Selecione os dispositivos alvo na lista **Meus dispositivos**, em seguida agende uma tarefa de configuração de agentes para instalar os agentes remotamente nos dispositivos.
- Instalando agentes com um pacote de instalação. Crie um pacote de auto-extração para a instalação no dispositivo. Execute esse pacote localmente no dispositivo para instalar os agentes. Isso deve ser feito conectado com privilégios administrativos.
- Executando uma instalação 'Pull' dos agentes. Crie um mapeamento para o compartilhamento ldlogon do núcleo (//*nome do servidor*/ldlogon) e execute o SERVERCONFIG.EXE.
- Manualmente em um dispositivo com uma unidade USB portátil (consulte Instalação de agentes com um pacote de instalação)

O capítulo Descoberta de dispositivo no *Guia do Usuário* é outro recurso para a instalação e configuração de agente .

**Nota:** Para tornar padrão a configuração de dispositivo, selecione a configuração na página **Configuração de agente** e clique em **Definir como padrão**. Uma configuração apenas BMC IPMI não pode ser padrão. As configurações padrão não podem ser excluídas.

Para os sistemas Windows, as seguintes configurações de porta requerem a configuração manual da firewall para obter-se a funcionalidade plena do produto. Para mudar estas configurações, acesse a Windows Firewall através do Painel de controle do Windows.

**Servidores gerenciados:**

- Compartilhamento de arquivos e impressoras: TCP 139, 445; UDP 137,138 (A opção por envio não funciona sem estes dados)
- Distribuição de software: TCP 9595 (Sem este valor não funciona por envio)
- Avançada: ICMP - “Permitir requisição de eco de entrada” (Não pode ser descoberto se este não estiver habilitado.)

**Servidor núcleo:**

- Inventário: 5007
- Controle remoto: 9535

Para fazê-lo, clique em **Iniciar** | **Painel de controle** | **Segurança**.

## Atualização de agentes

Você pode enviar configurações de agentes para seus dispositivos, mesmo se o agente da gerenciamento padrão e o agente do controle remoto ainda não estiverem presentes. Consulte Configuração de serviços e credenciais no *Guia do Usuário* se precisar das informações sobre a configuração de credenciais.

Uma vez instalado um pacote de agentes, uma nova instalação removerá a instalação anterior e instalará a nova configuração. Você pode desinstalar um agente através da criação de um novo pacote de agentes que não inclua o agente a ser removido.

## Desinstalação de agentes

Se você precisar desinstalar agentes de servidores, siga este procedimento.

**Aviso:** Como padrão, o Uninstallwinclient.exe reinicializa o dispositivo após a desinstalação dos agentes a menos que você use o argumento **/noreboot** na linha de comando. A reinicialização é necessária para completar a desinstalação. Se a reinicialização começar, o servidor reinicializará sem aviso e todos os aplicativos serão forçados a fechar. O argumento /noreboot permite ao servidor continuar funcionando sem a reinicilização.

**Para desinstalar agentes de um servidor**

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

   ```
   uninstallwinclient.exe /noreboot
   ```

A desinstalação será executada silenciosamente e removerá todos os agentes.

Você pode selecionar também **Iniciar** > **Executar** >***nome do núcleo*\ldmain\uninstallwinclient.exe /noreboot**.

**Para desinstalar agentes de um servidor Linux**

1. Copie o arquivo linuxuninstall.tar.gz para o diretório temporário no dispositivo Linux. Este pode ser encontrado na pasta compartilhada ManagementSuite do servidor núcleo.

   O dispositivo Linux pode não ter o Samba instalado ou configurado, se esse for o caso você não poderá copiá-lo diretamente; você pode usar pscp do núcleo, copiá-lo na pasta ldlogon ou copiá-lo para uma mídia removível.
2. No comando do shell (no computador Linux), descompacte este arquivo usando tar e as opções x, z e f.

   ```
   tar -xzf linuxuninstall.tar.gz
   ```
3. Após o arquivo ter sido descompactado, execute o script linuxuninstall de um prompt do shell, do diretório atual:

   ```
   ./linuxuninstall.sh
   ```

# Configuração dos agentes

Para ter a capacidade total de gerenciamento dos dispositivos usando o console, é necessário instalar os agentes neles. A instalação do System Manager não instala agentes no núcleo automaticamente; é necessário instalar também os agentes no núcleo, e depois reinicializar o núcleo manualmente. Independentemente de usar uma das configurações padrão de agente ou criar uma configuração de agente no console, você pode instalá-la nos dispositivos Windows ou Linux, em uma dessas três maneiras:

- Crie uma configuração de agente, selecione dispositivos como alvo na lista **Meus dispositivos**, em seguida, agende uma tarefa de configuração de agente para instalar os agentes remotamente nos dispositivos.
- Crie um pacote de auto-extração para instalação. Execute esse pacote localmente no dispositivo para instalar os agentes. Isso deve ser feito conectado com privilégios administrativos. Para ver mais informações, consulte "Instalação de agentes com um pacote de instalação".
- No Windows, faça um mapeamento para o compartilhamento ldlogon do núcleo (*myserver*\ldlogon) e execute o SERVERCONFIG.EXE.

**Para criar uma configuração de agentes**

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

   Digite um nome que descreva as configuração em que está trabalhando. O nome pode ser o nome de uma configuração existente ou um novo nome.

4. Selecione a plataforma para a configuração.

5. Selecione o tipo de instalação da configuração (usuário selecionado ou IPMI somente BMC). Selecione **IPMI somente BMC** em **Configuração** e configure o controlador de gerenciamento de placa básica (BMC) nos dispositivos habilitados com IPMI (consulte a nota na etapa 9 abaixo).

   A configuração IPMI somente BMC define o controlador de gerenciamento de placa básica para acesso fora de banda, executa uma análise completa de inventário e remove a si mesma. Uma configuração apenas BMC IPMI não pode ser padrão. Quando você cria uma configuração IPMI somente BMC, note que a maioria das opções de edição descritas nas etapas seguintes não estão disponíveis.

6. Selecione a configuração que acabou de criar e clique em **Editar**.

   Nas guias, algumas opções estão desativadas porque não são configuráveis para esta opção.
7. Na guia **Agente**, selecione os agentes que desejar distribuir.

   - **Todos:** Instala todos os agentes no dispositivo selecionado.
   - **Agente de gerenciamento padrão:** Forma a base das comunicações entre dispositivos e o servidor núcleo. Este é um agente requerido (exceto para as configurações somente BMC). A maioria dos processos de agentes são por demanda.
   - **Atualizações de software:** Instala o analisador de atualização de software Com este agente, é possível definir a forma como o agente funciona. Este não é um agente por demanda.
   - **Monitoração:** Instala o agente de monitoração no servidor selecionado. O agente de monitoração permite muitos tipos de monitoração, inclusive a monitoração direta ASIC, IPMI em banda, IPMI fora de banda e CIM. Este não é um agente por demanda.
   - **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. Este agente é suportado somente nos dispositivos com motherboards Intel.

8. Nas caixas de tipo de sistema de **Configuração**, selecione o tipo. Se esta parte estiver acinzentada, é porque você já selecionou o tipo.

9. Selecione a opção de **Reinicialização**.

   A reinicialização manual significa que os dispositivos não reinicializarão após a instalação. Não é necessário reinicializar um dispositivo após a configuração dos agentes. É necessário reinicializar manualmente o dispositivo.

   A reinicialização, se necessária, faz a reinicialização para as atualizações de agente quando os arquivos de atualização estão bloqueados.

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 usados 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:** A hora em que o inventário será executado. É possível selecionar a freqüência e especificar que seja executada sempre na inicialização. É possível executar o analisador manualmente a partir do servidor gerenciado; você poderá iniciá-lo em Iniciar | Programas | LANDesk Gerenciamento | Análise de inventário No Linux, é necessário estar conectado como raiz e executar o seguinte da linha de comando:
  `/usr/LANDesk/ldms/ldiscan -ntt`

  - **Sempre executar na inicialização:** Executa a Varredura de inventário nos dispositivos selecionados. Se estiver criando uma configuração HP-UX, este botão estará desativado porque o analisador HP-UX está definido para execução como tarefa cron, que se repete diária, semanal e mensalmente. Isso não pode ser modificado.
  - **Hora inicial:** Especifica um intervalo em que analisador pode ser executado. 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.
  - **Repetir a cada:** Digite um número que representa o incremento (por exemplo, 1, 2 ou 3) e a medida (minutos, horas ou dias).
  - **Restrições:** Limita os dias disponíveis e as horas em que o analisador pode ser executado. Clique em **Hora do dia**, **Dia da semana** ou **Dia do mês** e digite os parâmetros inclusivos. Por exemplo, digite 10 para o **Dia do mês** e 1:00 hr e 3:00 hr para a **Hora do dia** a fim de permitir que o analisador de inventário seja executado no 10º dia de cada mês entre 1:00 hr e 3:00 hr.

11. Na guia **Atualizações de software**, defina os dias e as horas em que quiser que o Analisador de atualizações de software seja executado. O analisador é executado automaticamente sem precisar de uma tarefa agendada.
    - **Sempre executar na inicialização:** Executa a Análise de inventário nos dispositivos selecionados.
    - **Hora inicial:** Especifica um intervalo em que analisador pode ser executado. Se um dispositivo conectar durante o intervalo de horas que você especificar, a análise de atualizações de software de inventário será executada automaticamente. Se o dispositivo já estiver conectado, quando o momento chegar, a análise de inventário iniciará automaticamente. Essa opção é útil se você quiser intercalar disparos de análises nos dispositivos de forma que elas sejam enviadas de um só vez.
    - **Repetir a cada:** Digite um número que representa o incremento (por exemplo, 1, 2 ou 3) e a medida (minutos, horas ou dias).

- **Restrições:** Limita os dias disponíveis e as horas em que o analisador de atualizações de software pode ser executado. Clique em **Hora do dia**, **Dia da semana** ou **Dia do mês** e digite os parâmetros inclusivos. Por exemplo, digite 10 para o **Dia do mês** e 1:00 hr e 3:00 hr para a **Hora do dia** a fim de permitir que o analisador de inventário seja executado no 10º dia de cada mês entre 1:00 hr e 3:00 hr.

12. 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.
13. Clique em **Salvar as alterações** para salvar as informações no banco de dados. Clique em **Salvar como arquivo** para salvar a configuração como um pacote distribuível.

**Nota:** Você pode tornar padrão a configuração de agente dispositivo selecionando a configuração na página **Configurações de agente** e clicando em **Definir como padrão**. As configurações padrão não podem ser excluídas.

**Para agendar uma tarefa de configuração de agente**

1. No painel de navegação esquerdo, clique em **Configuração do agente**.
2. Clique em configuração do agente e clique em **Agendar tarefa**.
3. Edite a lista de dispositivos alvo e o agendamento de tarefas.
4. Clique em **Salvar**.

Ao clicar em **Agendar tarefa**, é criada uma tarefa (ela não tem dispositivos alvo e é não agendada). Se cancelar esta tarefa de configuração de agente sem salvá-la, lembre-se de que ela foi criada e aparecerá na lista **Tarefas** com status de Não agendada. Ela pode ser apagada na lista **Minhas tarefas**.

Após a tarefa de configuração do agente ser completada, é necessário reinicializar o dispositivo para ver os detalhes sobre ele no console (consulte Ver o Console de informações do servidor). Esta reinicialização é necessária quando você instala o agente no servidor núcleo e nos dispositivos gerenciados. O processo de configuração do agente permite escolher quando reinicializar para que a reinicialização não interfira com o uso do servidor.

# Distribuição de agentes para dispositivos gerenciados

Após ter descoberto dispositivos, você pode distribuir agentes para eles. Só é possível distribuir agentes para os dispositivos Windows, Linux e HP-UX. É necessário ter o direito de Administrador para distribuir agentes para dispositivos Windows, e o privilégio raiz para configurar dispositivos Linux e HP-UX.

Você pode distribuir agentes para dispositivos não gerenciados de uma das seguintes formas:

- Distribuições com instalação por envio usando uma tarefa de descoberta e uma conta administrativa de domínio que você configurou para o Serviço do planejador, o qual processa as tarefas de descoberta. A conta administrativa de domínio dá ao Serviço do planejador os direitos necessários para instalar os agentes de servidores. Isto funciona para servidores da família do Windows NT.
- Distribuições baseadas em envio usando o agente de gerenciamento padrão. Se os servidores tiverem o agente de gerenciamento Padrão, que é usado por vários dos produtos LANDesk  Software, você pode distribuí-los sem requerer uma conta administrativa no domínio.

Ao fazer a distribuição para os dispositivos descobertos, use a opção **Filtrar por** na árvore **Não gerenciados**. Você pode filtrar pelo endereço IP para isolar dispositivos específicos.

Para os sistemas Windows, as definições de porta a seguir requerem configuração manual da firewall para obter funcionalidade completa do produto. Para mudar essas configurações, acesse a Windows Firewall através do Painel de controle do Windows.

**Servidores gerenciados:**

- Compartilhamento de arquivos e impressoras: TCP 139, 445; UDP 137,138 (Por envio não funciona sem isto)
- Distribuição de software: TCP 9594, 9595 (Por envio não funciona sem isto)
- Avançada - ICMP: “Permitir requisição de eco de entrada” (Não pode ser descoberto se este não estiver habilitado.)

**Servidor núcleo:**

- Inventário: 5007
- Controle remoto: 9535

## Configuração das credenciais de autenticação nos dispositivos

Os dispositivos não gerenciados com o agente de gerenciametno padrão instalados não requerem credenciais de autenticação para a distribuição de agentes. Para instalar agentes em servidor do SO Windows que não têm o agente de gerenciamento padrão, é necessário especificar as credenciais que o Serviço do agendador no dispositivo do console deve utilizar para obter os direitos necessários.

Para instalar os agentes em dispositivos não gerenciados, o serviço do agendador precisa poder conectar-se aos dispositivos com uma conta administrativa. A conta padrão que o serviço do planejador utiliza é LocalSystem. As credenciais LocalSystem geralmente funcionam com dispositivos que não estão em um domínio.

Se os dispositivos estão em um domínio, é necessário especificar um conta de administrador de domínio. Se estiver configurando dispositivos não gerenciados em vários domínios, você deve configurá-los um domínio de cada vez, já que o serviço do planejador se autentica com um conjunto de credenciais, e cada domínio requer uma conta administrativa de domínio diferente.

O servidor núcleo inclui o utilitário Configurar serviços, que você pode utilizar para personalizar opções de inventário. Esse utilitário só pode ser executado no servidor núcleo.

**Para configurar as credenciais de login do serviço do planejador**

1. Abra o utilitário Configurar serviços, no servidor núcleo clicando em **Iniciar | Arquivos de programas | LANDesk | Configurar serviços**.
2. Clique na guia **Planejador**.
3. Clique no botão **Alterar login**.
4. Digite as credenciais que você deseja que o serviço utilize nos clientes, normalmente uma conta administrativa de domínio.

# Instalação de agentes

Após criar uma configuração de agente no console, você precisa instalá-la nos dispositivos. A instalação do System Manager não instala agentes no núcleo automaticamente; é necessário instalar também os agentes no núcleo, e depois reinicializar o núcleo manualmente.

Os pacotes de agente de cliente são um arquivo executável auto-extraível. Como padrão eles são armazenados na pasta \Arquivos de programas\LANDesk\ManagementSuite\ldlogon no servidor núcleo. Quando o executável é executado, os agentes de cliente são instalados silenciosamente sem necessidade de interação do usuário. Não necessário um navegador no dispositivo alvo para a instalação do agente.

## Instalação de agentes

Você pode atualizar os agentes através da criação de uma nova configuração de cliente e de sua distribuição do console, ou através da instalação manual dos agentes nos dispositivos não gerenciados.

Após ter instalado um pacote de agentes de cliente, a instalação de outros pacotes de agentes de cliente removerá todos os agentes instalados e instalará os agentes especificamente selecionados. Você pode desinstalar um agente através da criação de um novo pacote de agente de cliente que não inclua o agente a ser removido.

## Desinstalação de agentes

Se precisar desinstalar agentes usando dispositivos, consulte "Visão geral de instalação e configuração de agentes".

# Instalação de agentes com um pacote de instalação

Uma das maneiras pelas quais você pode instalar agentes de instalação é com um pacote de auto-extração de agentes de dispositivo. Isto lhe permite copiar o arquivo para um CD ou unidade USB para instalar os agentes manualmente. Para criar esses pacotes, clique em **Salvar como arquivo** na parte inferior do diálogo **Configuração**.

1. Clique em **Configuração de agentes**, em seguida clique duas vezes no nome de uma configuração.

2. No diálogo **Configuração de agente**, clique em **Salvar como arquivo**, em seguida clique em **Fechar**.

Clicar em **Salvar como arquivo** cria um pacote de auto-extração executável, cujo nome de arquivo é igual ao nome da configuração especificada. Pode levar alguns minutos para o pacote estar disponível na pasta \Arquivos de programas\LANDesk\ManagementSuite\ldlogon\ConfigPackages do servidor núcleo.

Quando o executável é executado, os agentes são instalados, sem necessidade de haver interação do usuário. Você deve estar conectado com direitos administrativos.

Se seus usuários não puderem conectar com privilégios administrativos para instalar o pacote, você pode distribuir os pacotes através de email, download na Web, scripts de login ou de um compartilhamento.

# Instalação de agentes por recepção (pull)

Esta seção contém detalhes sobre a distribuição de agentes a partir da linha de comandos. Você pode controlar que componentes são instalados nos dispositivos usando os parâmetros da linha de comandos do SERVERCONFIG.EXE. É possível iniciar o SERVERCONFIG.EXE no modo standalone. Ele é localizado no compartilhamento *http:\\servidor_núcleo\LDLogon*, acessível de qualquer servidor Windows.

O SERVERCONFIG.EXE utiliza o SERVERCONFIG.INI para a configuração de dispositivos.

## O SERVERCONFIG.EXE

O SERVERCONFIG.EXE configura servidores da família Windows NT para o gerenciamento usando o processo a seguir:

1. O SERVERCONFIG determina se o computador já foi configurado anteriormente com um agente de gerenciamento. Se tiver sido, o SERVERCONFIG remove todos os componentes e reinstala os componentes selecionados.
2. O SERVERCONFIG carrega o arquivo de inicialização correto (SERVERCONFIG.INI) e executa as instruções nele contidas.

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

| Parâmetro | Descrição |
|---|---|
| /I= | Componentes a incluir (incluindo as aspas):<br><br>"Common Base Agent"<br><br>"Analisador de inventário"<br><br>"Alertas"<br><br>"Analisador de vulnerabilidades" |

| Parâmetro | Descrição |
|---|---|
| | "Monitor de servidor"<br><br>Você pode combinar todos esses na mesma linha. Por exemplo:<br><br>`SERVERCONFIG.EXE /I="Alerting" /I="Vulnerability Scanner"` |
| /L ou /Log= | Caminho para arquivos de log CFG_YES e CFG_NO que registram quais servidores foram ou não configurados. |
| /LOGON | Executa comandos [LOGON] com prefixos. |
| /N ou /NOUI | Não exibe a interface do usuário. |
| /NOREBOOT | Não reinicializa o servidor quando concluído (padrão). |
| /REBOOT | Força a reinicialização após execução |
| /X= | Componentes a excluir. Por exemplo:<br><br>`SERVERCONFIG.EXE /X=SD` |
| /CONFIG=<br><br>/[CONFIG]= | Especifica um arquivo de configuração de servidor a ser usado em vez do arquivo SERVERCONFIG.INI padrão.<br><br>Por exemplo, se você tiver criado um arquivo de configuração chamado NTTEST.INI, use esta sintaxe:<br><br>`SERVERCONFIG.EXE /CONFIG=TEST.INI`<br><br>Os arquivos .INI personalizados devem estar no mesmo diretório que o SERVERCONFIG.EXE e é necessário verificar se o parâmetro /config usa o nome de arquivo sem o prefixo NT. |
| /? ou /H | Exibir menu de ajuda |

## Criação de uma configuração de agentes

Use **Configuração do agente** para criar e atualizar configurações de agentes de servidores (por exemplo, que agentes são instalados em servidores gerenciados). Você pode criar diferentes configurações para as necessidades específicas de um grupo. Por exemplo, você pode criar uma configuração para servidores Web e outra para servidores de aplicativos.

Para instalar por envio uma configuração em um servidor, você precisa:

- **Criar a configuração de agentes**: Definir configurações específicas para seus servidores.
- **Agendar a configuração dos agentes**: Instalar por envio a configuração nos servidores, ou, de um servidor, executar o SERVERCONFIG.EXE no compartilhamento LDLogon do servidor núcleo.

**Para criar uma configuração de agentes**

1. No console, clique em **Configuração de agentes**.
2. Clique no botão da barra de ferramentas **Nova**.
3. Digite o **Nome da configuração** e selecione o sistema operacional, em seguida clique em **OK**.
4. Clique no nome da nova configuração, em seguida clique em **Editar**.
5. Selecione os agentes que deseja distribuir.
6. Use as guias no topo do diálogo para navegar para as opções relacionadas aos componentes que você selecionou. Personalize as opções que selecionou conforme necessário.
7. Clique em **Salvar as alterações**, em seguida feche o diálogo.
8. Se desejar que essa configuração seja a configuração padrão, clique em **Definir como padrão**.

## Para instalar por pull uma configuração de agente Linux

**Para instalação por recepção (pull) uma configuração de agentes Linux**

1. Crie um diretório temporário no dispositivo 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 script 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 relacionados no arquivo <*nome da configuração*>.ini no diretório temporário. Para identificar esses arquivos, faça uma busca no arquivo .INI por "ARQUIVO*xx*", onde *xx* é um número. A maioria das entradas encontradas foram copiadas no cliente na etapa 1, mas há arquivos .XML que precisam ser copiados. Os nomes de arquivos não devem ser modificados, mas há exceções:
        - alertrules\<*qualquer texto*>.ruleset.xml deve ser renomeado como internal.ruleset.xml
        - monitorrules\<*qualquer texto*>.ruleset.monitor.xml deve ser renomeado como masterconfig.ruleset.monitor.xml
2. Se o dispositivo tiver IPMI e BMC (com a Monitoração incluída durante a instalação), digite o seguinte em uma 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" (por envio), use o caminho completo usado abaixo:

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

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

Nota: Lembre-se de que se você fizer envio ou recepção (push or pull) em um agente para um dispositivo Linux, em seguida executar

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

para limpá-lo e depois fizer o push ou pull novamente, o arquivo com o GUID será o único arquivo no dispositivo após a operação ter sido completada.

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

## Criação de pacotes standalone de configuração de agentes

Normalmente o utilitário de configuração do agente, o SERVERCONFIG.EXE, configura os agentes em dispositivos gerenciados. Se você desejar, é possível fazer a janela de **Configuração de agentes** criar um único arquivo executável de auto-extração que instala a configuração de agentes no servidor em que for executado. Isto é útil quando você deseja instalar agentes a partir de um CD ou unidade USB portátil.

## Instalando por envio configurações de agentes em dispositivos

**Para fazer envio de uma configuração de agente**

1. No console, selecione os dispositivos para os quais você deseja distribuir os agentes, em seguida clique em **Alvo**.
2. No painel de navegação esquerdo, clique em **Configuração do agente**.
3. Clique com o botão direito na configuração de agentes que deseja instalar por envio, em seguida clique em **Agendar tarefa.**
4. Clique em **Dispositivos alvo** na caixa de diálogo Propriedades da **Tarefa agendada**, em seguida clique em **Adicionar lista de alvos**.
5. Clique em **Agendar tarefa**.
6. Especifique o horário de distribuição do agente, em seguida clique em **Salvar**.

# 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. Para instalar um agente em um servidor Linux, é necessário ter privilégios de raiz.

A instalação padrão do Linux (Red Hat 3 e 4, e SUSE) inclui os RPMs requeridos pelo agente de gerenciamento padrão para Linux. Se selecionar o agente de monitoração em **Configuração de agentes**, você precisará de um RPM adicional e sysstat. Para ver uma lista completa dos RPMs que o produto requer, consulte o *System ManagerGuia de distribuição*.

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 **Planejador**, para reiniciar o serviço. Isto ativará as alterações.

## Distribuição de agentes Linux

Após ter configurado seus servidores Linux e adicionado as credenciais Linux ao servidor núcleo, é necessário adicionar servidores à lista **Meus dispositivos** para poder 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 dispositivo**.

**Para descobrir seus servidores Linux**

1. Em **Descobrir 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. Em **Descoberta de dispositivo**, selecione os servidores que quer gerenciar e clique em **Alvo** para adicionar os dispositivos selecionados à Lista de alvos. Clique na guia **Gerenciar** na parte de baixo 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. Em **Configuração de agentes**, clique em **Nova**.
2. Digite um nome para a configuração, clique em **HP-UX**ou **Linux Server Edition**, selecione o tipo de instalação (servidor ou desktop) 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. 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.
7. Clique em **Salvar as alterações**.

Para distribuir a sua configuração de agente, selecione-a em **Configurações de agente** e clique em **Agendar tarefa**. Configure a tarefa e monitore o andamento da tarefa em **Tarefas de configuração.**

**Nota:** Não aparecerá nenhuma informação de funcionamento em um dispositivo 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 dispositivo Linux (por exemplo, /tmp/ldcfg) e copie o seguinte nesse diretório:
   - Todos os arquivos do diretório LDLOGON\unix\linux.
   - O script de shell nomeado após a configuração (<*nome da configuração*>.sh).
   - O arquivo *.0 nomeado após a configuração. O * representa oito caracteres (0-9, a-f).
   - Todos os arquivos são mostrados no arquivo <*nome da configuração*>.ini. Para identificar esses arquivos, faça uma busca no arquivo .INI com o critério "FILE*xx"*, onde *xx* é um número. A maioria do que encontrar já deve ter sido copiado no cliente na Etapa 1, mas você encontrará arquivos .XML que devem ser copiados. Os nomes de arquivo devem ser deixados intactos, com as seguintes opções:
     - 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 dispositivo tiver IPMI e BMC (com a Monitoração inclusa na instalação), digite o seguinte na linha de comando:

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

3. Como raiz, execute o script de shell para a configuração usando o caminho completo abaixo :

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

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

**Nota:** Se você fizer envio ou recepção de um agente do dispositivo Linux, execute

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

para limpá-lo e, em seguida, faça o envio ou a recepção outra vez, o arquivo com o GUID é o único deixado no dispositivo após a operação terminar.

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

## Parâmetros de linha de comandos da análise de inventário

A análise de inventário, ldiscan, tem vários parâmetros da linha de comandos que especificam como ela deve ser executada. Consulte "ldiscan -h" ou "man ldiscan" para ver uma descrição detalhada de cada uma. Cada opção pode ser precedida por '-' ou '/'.

| Parâmetro | Descrição |
|---|---|
| -d=Dir | Inicia a análise de software no diretório Dir, em vez de na raiz. Por padrão, a análise é iniciada no diretório raiz. |
| -f | Força uma análise de software. Se você não especificar -f, a varredura analisará o software de acordo com o intervalo especificado (o padrão é todos os dias) no console em **Configurar \| Serviços \| Inventário \| Configurações da varredura**. |
| -f- | Desabilita a análise de software. |
| -i=ConfName | Especifica o nome do arquivo de configuração. O padrão é /etc/ldappl.conf. |
| -ntt=address:port | Digite o nome de host ou endereço IP do servidor núcleo. A porta é opcional. |
| -o=File | Grava os dados de inventário no arquivo de saída especificado. |

| Parâmetro | Descrição |
|---|---|
| -s=Server | Especifica a instalação do servidor núcleo. Este comando é opcional e só existe para compatibilidade retroativa. |
| -stdout | Grava informações de inventário na saída padrão. |
| -v | Habilita mensagens de status detalhadas durante a análise. |
| -h ou -? | Mostra a tela de ajuda. |

## Exemplos

Para obter dados de saída em um arquivo de texto, digite:

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

Para enviar dados ao servidor núcleo, digite:

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

## Arquivos do analisador de inventário Linux

| Arquivo | Descrição |
|---|---|
| ldiscan | O executável que é executado com parâmetros da linha de comandos para indicar a ação a ser realizada. Todos os usuários que executarão o analisador precisam ter direitos suficientes para executar o arquivo.<br><br>Há uma versão diferente desse arquivo para cada plataforma suportada acima. |
| /etc/ldiscan.conf | Esse arquivo encontra-se em /etc e contém as seguintes informações:<br><br>• ID exclusivo atribuído ao inventário<br>• Última análise de hardware<br>• Última análise de software<br><br>Todos os usuários que executam o analisador necessitam de atributos de leitura e gravação para esse arquivo. O ID exclusivo em /etc/ldiscan.conf é o número exclusivo atribuído a um computador na primeira vez que a varredura de inventário é executada. Esse número é usado para identificar o computador. Se for alterado, o servidor núcleo o tratará como um computador |

| Arquivo | Descrição |
|---|---|
| | diferente, o que pode resultar em uma entrada duplicada no banco de dados.<br><br>**Aviso:** Não mude o número exclusivo do ID nem remova o arquivo ldiscan.conf depois de criado. |
| /etc/ldappl.conf | Esse arquivo é o local no qual você personaliza a lista de executáveis que a varredura de inventário reportará ao executar uma análise de software. O arquivo contém alguns exemplos e não é necessário adicionar entradas para os pacotes de software que usar. Os critérios de busca são baseados no nome e tamanho do arquivo. Embora esse arquivo geralmente esteja em /etc, o analisador pode usar um arquivo alternativo, usando o parâmetro da linha de comando -i=. |
| ldiscan.8 | Página Man do ldiscan. |

## Integração com o console

Assim que um computador Linux for analisado no banco de dados núcleo, será possível:

- Consultar qualquer atributo apresentado pela varredura de inventário Linux no banco de dados núcleo.
- Usar recursos de relatório para gerar relatórios que incluam informações coletadas pelo analisador Linux. Por exemplo, Linux aparecerá em um tipo de SO no Relatório de resumo de sistemas operacionais.
- Ver informações de inventário de computadores Linux.

**Consultas de "Tempo de atividade do sistema" ordenam-se alfabeticamente, retornando resultados inesperados**
Se você deseja realizar uma consulta para descobrir quantos computadores estão em execução além de um determinado número de dias (por exemplo, 10 dias), faça uma consulta com "System Start" e não "System Uptime". As consultas realizadas com System Uptime podem apresentar resultados inesperados, pois o tempo de ativação do sistema é simplesmente uma seqüência de caracteres formada como "x dias, y horas, z minutos e j segundos". A ordenação é feita em ordem alfabética e não em intervalos de tempo.

**O caminho para os arquivos de configuração referenciados em ldappl.conf não aparece no console**
As entradas ConfFile no arquivo ldappl.conf precisam incluir o caminho.

# Monitoração do dispositivo

## Sobre a monitoração

O System Manager oferece vários métodos de monitoração do funcionamento de um dispositivo. Os recursos de monitoração coletam dados de várias fontes para ajudá-lo a manter controle de muitos conjuntos de dados nos seus dispositivos como, por exemplo:

- Níveis de utilização
- Eventos do SO
- Processos e Serviços
- Histórico do desempenho
- Sensores de hardware (ventiladores, voltagens, temperaturas, etc.)

Este capítulo inclui as informações sobre os diferentes recursos que monitoram seus dispositivos gerenciados:

- Instalação de um agente de monitoração nos dispositivos e criação de conjuntos de regras de monitoração que podem ser distribuídos para os dispositivos
- Configuração de contadores de desempenho nos dispositivos e monitoração dos dados de desempenho
- Monitoração das mudanças de configuração com alertas quando ocorrem mudanças
- Ping de dispositivos regularmente para monitorar sua conectividade, usando o recurso **Monitor de dispositivo**

Alertas é um recurso relacionado que utiliza o agente de monitoração para iniciar ações de alerta como, por exemplo, enviar email ou mensagens de pager, reinicializar ou desligar um dispositivo ou adicionar informações ao log de alertas. Você pode gerar alertas de qualquer um dos eventos de dispositivos que podem ser monitorados. Consulte "Uso de alertas" para ver mais informações.

**Notas**

- As comunicações como o agente de monitoração são feitas através de HTTP em TCP/IP no formato de solicitações GET, POST ou XML. As respostas a solicitações são feitas em documentos de tabela XML ou HTML.
- Para executar e armazenar uma consulta sobre o status de funcionamento de dispositivos (Computer.Health.State), é preciso estar alerta para o fato de que o estado no banco de dados é representado por um número. Os números correspondem aos seguintes estados: 4=Crítico, 3=Advertência, 2=Normal, 1=Informativo, nulo ou 0=desconhecido.
- A monitoração de hardware depende das capacidades do hardware instalado em um dispositivo, assim como da correta configuração do hardware. Por exemplo, se um disco rígido com capacidades de monitoração S.M.A.R.T. for instalado em um dispositivo mas a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não suportar unidades S.M.A.R.T., os dados de monitoração não estarão disponíveis.

- Se estiver fazendo um relatório de um computador específico que parece ter parado, você pode usar o restartmon.exe na pasta LDCLIENT para reiniciar o coletor e todo os provedores de monitoração. Esse utilitário é para computadores onde foi instalada a opção de relatório e essa função parou. Use esse utilitário para reiniciar o coletor e os provedores sem ter que reinicializar o dispositivo.

## Distribuição do agente de monitoração para dispositivos

O System Manager fornece um resumo imediato da condição de um dispositivo quando o agente de monitoração é instalado no dispositivo. O agente de monitoração é um dos seis agentes que podem ser instalados em dispositivos gerenciados. Ele checa o hardware e a configuração do dispositivo, regular e periodicamente e reporta as mudanças nas condições do dispositivo. Isso é mostrado pelo ícone de status na lista **Meus dispositivos** e os detalhes são dispostos em entradas de log (mostrados no resumo **Informações do sistema** do dispositivo) e em gráficos (mostrados na página de resumo **Monitoração** do dispositivo).

Por exemplo, um dispositivo monitorado que tem um disco rígido cujo espaço está se esgotando pode mostrar um ícone de status de advertência quando o disco atingir 90% da capacidade total, mudando para um ícone de status crítico quando o disco atingir 95% da capacidade total. Você também pode receber alertas para o mesmo status de disco rígido se o dispositivo tiver um conjunto de regras de alerta com regras para alerta de espaço de disco.

Os conjuntos de regras de monitoração padrão podem ser distribuídos para os dispositivos. Ou, se preferir, crie um conjunto de regras personalizado com apenas os itens relativos aos funcionamentos de dispositivo com os quais está preocupado.

## Criação de um conjunto de regras de monitoração

Você pode escolher o que é monitorado em um dispositivo criando um conjunto de regras de monitoração, que define o que o agente de monitoração deve checar no dispositivo. É possível distribuir um conjunto de regras a um dispositivo ou a um grupo de dispositivos alvo. Por exemplo, você pode definir um conjunto de regras para servidores dedicados ao armazenamento e usar um conjunto de regras diferente para servidores de web.

O conjunto de regras padrão de monitoração contém 16 itens. Ao criar um conjunto de regras, você pode desligar ou ligar qualquer desses itens, especificar a freqüência na qual quer que eles sejam verificados e definir limites de desempenho para determinados itens. É possível também selecionar serviços em execução nos dispositivos, os quais quer monitorar.

O processo geral para a criação e distribuição de um conjunto de regras de alerta é o seguinte:

1. Selecione os dispositivos para os quais quer distribuir o conjunto de regras e clique em **Alvo** para adicioná-los à lista **Dispositivos alvo**.
2. Criação ou edição de um conjunto de regras de monitoração. Observe que é necessário checar o quadro para ativar a monitoração em cada evento que você quiser monitorar no conjunto de regras. Nem todos estão configurados para a monitoração padrão. Alguns eventos, como por exemplos serviços, também requerem a seleção de cada serviço que quiser monitorar. (Veja detalhes a seguir.)

3. Distribuição do conjunto de regras aos dispositivos alvo. Dispositivos adicionais podem também ser alvos antes da distribuição do conjunto de regras, se necessário. (Veja detalhes a seguir.)

**Para criar um conjunto de regras de monitoração**

1. No painel de navegação esquerdo, clique em **Monitoração**.
2. Clique em **Nova**, digite um nome e descrição para a configuração e clique em **OK**.
3. Selecione a configuração na coluna à esquerda.
4. Na lista de itens, clique em um item que deseja mudar e clique em **Editar**.
5. Para desativar a monitoração de um item, limpe a caixa de seleção e clique em **Atualizar**.
6. Para mudar a freqüência em que o item é monitorado, selecione **Segundos** ou **Minutos** e especifique um número na caixa de texto.
7. Se aplicável, defina as porcentagens para os status advertência e crítico.
8. Para monitoração de **Serviços**, selecione o SO na lista suspensa. Selecione um ou mais serviços para monitorar (use CTRL + clique para selecionar mais de um serviço) e clique em **>>** para adicioná-los à lista à direita.
9. Para cada item que modificar, clique em **Atualizar** para aplicar as mudanças na configuração. Se modificar um item e depois decidir que não quer a modificação, clique em **Reverter** para restaurar as configurações originais.

Quando editar serviços em uma configuração de monitoração a partir do servidor núcleo, a lista **Serviços disponíveis** mostra os serviços conhecidos do banco de dados de inventário. Não aparece nenhum serviço no quadro de lista **Serviços disponíveis** até que um agente LANDesk tenha sido distribuído a um ou mais dispositivos e uma análise de inventário seja retornada ao núcleo. Por exemplo, para selecionar serviços Linux na lista, é necessário primeiro ter distribuído um agente ao dispositivo Linux.

**Para distribuir um conjunto de regras de monitoração**

1. No painel esquerdo de navegação, clique em **Meus dispositivos**, em seguida, clique no grupo **Todos os dispositivos**.
2. Selecione os dispositivos para os quais quer distribuir o conjunto de regras de alerta, em seguida, clique em **Alvo** para colocar os dispositivos na lista **Dispositivos alvo**.
3. No painel de navegação esquerdo, clique em **Monitoração**, em seguida clique na guia **Distribuir conjunto de regras**.
4. Na caixa **Conjuntos de regras de monitoração**, selecione o conjunto de regras que desejar distribuir.
5. Clique no link para ver a lista de **Dispositivos alvo**. Para remover um dispositivo da lista, clique o botão direito no servidor e clique em **Remover**. (Para acrescentar dispositivos, é necessário adicioná-los à lista de alvos conforme descrito na etapa 2.)
6. Clique em **Distribuir** para distribuir conjunto de regras selecionado aos dispositivos alvo.

Como parte do processo de distribuição, é criada uma página em XML contendo os conjuntos de regras distribuídos e os dispositivos para os quais os conjuntos de regras foram distribuídos. O relatório é salvo no servidor núcleo no diretório LDLOGON e é nomeado com um número seqüencial atribuído pelo banco de dados. Se quiser ver essa página XML separadamente da distribuição de um conjunto de regras, clique no botão **Gerar XML** e clique no link para ver o arquivo XML. A geração de um conjunto de regras também permite que ele seja mostrado na lista de conjuntos de regras disponíveis nas definições da **Configuração de agente**.

## Como desativar o serviço ModemView

ModemView é o serviço/driver que monitora as chamadas de modem (recebidas e enviadas) e gera um alerta se detectar uma chamada. Esse serviço utiliza aproximadamente 10 Mb de memória, pois usa MFC. Recomenda-se que esse serviço esteja desativado, especialmente se não houver um modem no dispositivo.

**Para desativar o serviço ModemView**

1. No dispositivo (diretamente ou via controle remoto) clique em **Iniciar** > **Painel de controle** > **Ferramentas administrativas** > **Serviços**.
2. Clique duas vezes em **LANDesk Message Handler Service** (Serviço de manipulação de mensagem LANDesk).
3. Em **Tipo de inicialização**, selecione **Manual** e clique em **OK**.

Clique também na opção **Parar**, em **Status de serviço**.

# Configuração dos contadores de desempenho

O System Manager permite selecionar itens de desempenho (contadores) que você deseja monitorar em um dispositivo gerenciado. É possível monitorar muitos tipos diferentes de itens, inclusive componentes de hardware (como unidades, processadores e memória) ou monitorar componentes do SO (como processos) ou componentes de aplicativos (como bytes por segundo transferidos pelo servidor de Web do sistema). Quando um contador de desempenho é selecionado, você especifica a freqüência da sondagem do item e também especifica os limites de desempenho e o número de violações a serem permitidas antes de ser gerado uma alerta.

Após um contador de desempenho ser selecionado, você pode monitorar o desempenho na página **Monitoração**, através de um gráfico em tempo real ou de dados históricos. Consulte "Monitoração de desempenho", para ver mais detalhes.

**Para selecionar um contador de desempenho a monitorar**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em outra janela do navegador.
2. No painel de navegação esquerdo, clique em **Monitoração**.
3. Clique na guia **Configurações do contador de desempenho**.
4. Na coluna **Objetos**, selecione o objeto que deseja monitorar.
5. Na coluna **Instâncias**, selecione a instância do objeto que deseja monitorar, se aplicável.
6. Na coluna **Contadores**, selecione o contador específico que quer monitorar.

   Se o contador desejado não aparece na lista, clique em **Recarregar contadores** para atualizar a lista com novos objetos, instâncias ou contadores.

7. Especifique a freqüência de sondagem (polling) (**Verificar a cada*n* segundos**) e o número de dias em que o histórico deverá ser mantido.

8. Na caixa de texto **Alertar após o contador estar fora do intervalo**, especifique o número de vezes que o contador poderá ultrapassar o limite antes de ser gerado um alerta.
9. Especifique os limites superior e/ou inferior.
10. Clique em **Aplicar**.

**Notas**

- Os arquivos dos logs de desempenho podem tornar-se grandes demais, rapidamente. A sondagem de um único contador em intervalos de dois segundos adiciona diariamente 2,5 MB de informações ao log de desempenho.
- Um alerta de advertência é gerado quando um contador de desempenho vai abaixo do limite mais baixo em um dispositivo Windows ou Linux. Quando um contador de desempenho excede o limite mais alto em um dispositivo Linux, é gerado um alerta de advertência. Quando um contador de desempenho excede o limite mais alto em um dispositivo Windows, é gerado um alerta crítico.
- Na configuração dos limites, lembre-se de que serão gerados alertas independentemente de ser alcançado um limite mais alto ou mais baixo. No caso de espaço em disco, por exemplo, você talvez queira ser alertado somente se o dispositivo estiver sendo executado muito baixo. Nesse caso, é aconselhável configurar o limite maior a um número alto o suficiente para que você não receba um alerta se uma quantidade grande do espaço em disco tornar-se disponível no dispositivo.
- Mudar o número em **Alertar após o contador estar fora do intervalo** lhe permite colocar o foco em um problema quando ele é persistente ou quando ele é um evento isolado. Por exemplo, se você estiver monitorando os bytes enviados de um servidor Web, o System Manager pode alertá-lo quando a quantidade de bytes/seg. estiver consistentemente alta. Ou você pode especificar um número baixo, como 1 ou 2, para ser alertado sempre que o número de conexões anônimas de FTP exceder um certo número de usuários.

# Monitoração do desempenho

A página **Monitoração** permite monitorar o desempenho de vários objetos do sistema. É possível monitorar componentes de hardware específicos, como unidades, processadores e memória, ou monitorar componentes do SO, como processos ou bytes por segundo transferidos pelo servidor Web do sistema. A página **Monitoração** inclui um gráfico que mostra os dados em tempo real ou os dados históricos de contadores.

Para monitorar um contador de desempenho, primeiramente selecione o contador. Isto o adicionará à lista de contadores monitorados. Quando você faz isso, você também especifica a freqüência da sondagem do item e especifica os limites de desempenho e o número de violações a serem permitidas antes de ser gerado uma alerta. Consulte "Configuração dos contadores de desempenho" para ver os detalhes sobre a seleção de contadores.

**Para ver um gráfico do desempenho de um contador monitorado**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em outra janela do navegador.
2. No painel de navegação esquerdo, clique em **Monitoração.**
3. Clique na guia **Contadores de desempenho ativos**, se necessário.

4. Na lista suspensa **Contadores**, selecione o contador do qual deseja ver um gráfico do desempenho.
5. Selecione **Visualizar dados em tempo real** para ver um gráfico do desempenho em tempo real.

   ou

   Selecione **Visualizar dados do histórico** para ver um gráfico mostrando o desempenho durante o período que você especificou (Manter histórico) ao selecionar o contador.

No gráfico de desempenho, o eixo horizontal representa o tempo decorrido. O eixo vertical representa as unidades sendo medidas, como bytes por segundo (ao monitorar transferências de arquivos, por exemplo), Porcentagem (ao monitorar a porcentagem de CPU em uso) ou bytes disponíveis (ao monitorar o espaço em discos rígidos). A altura da linha não é uma unidade fixa. A altura da linha muda com relação aos valores extremos dos dados; para um contador o eixo vertical pode representar 1 a 100, e para outro ele pode representar 1 a 500.000. Quando a variação de dados é de grande amplitude, mudanças mínimas podem ser exibidas como uma aparente linha horizontal.

**Notas**

- A seleção de outro contador atualiza o gráfico e redefine as unidades de medida.
- Clique em **Atualizar**  para limpar o gráfico e reiniciá-lo.
- Se receber um alerta gerado por um contador na lista, clique com o botão direito do mouse no contador e clique em **Reconhecer** para limpar o alerta.

**Para parar a monitoração de um contador de desempenho**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em outra janela do navegador.
2. No painel de navegação esquerdo, clique em **Monitoração**.
3. Clique na guia **Contadores de desempenho ativos**, se necessário.
4. Em **Contadores de desempenhos monitorados**, clique com o botão direito do mouse no contador e clique em **Excluir**.

# Monitoração de mudanças na configuração

O produto pode gerar alertas se houver mudanças na configuração de software ou hardware de um dispositivo e o agente de monitoração estiver instalado no dispositivo. Tais mudanças podem afetar o desempenho e a estabilidade do dispositivo ou causar problemas em uma instalação padrão. Através da monitoração de peças vitais do dispositivo, este produto pode reduzir o custo total de propriedade (TCO).

As seguintes mudanças de configuração de dispositivo causarão a geração de alertas:

- **Aplicativo instalado ou desinstalado:** Você pode ver quais usuários instalaram ou removeram aplicativos. Isto pode ser útil no acompanhamento de licenças e da produtividade de funcionários. Os aplicativos que estiverem registrados na área do Windows Adicionar/remover programas no Painel de controle são monitorados. Outros aplicativos são ignorados. O nome do aplicativo que é usado pelo Adicionar/remover programas da Windows é o nome do aplicativo que aparecerá no log de notificação ou na janela pop-up do alerta.
- **Memória adicionada ou removida:** Este produto detecta e monitora o tamanho e o tipo da memória instalada. Se a configuração mudar, é gerado um alerta.
- **Unidade de disco adicionada ou removida:** Este produto detecta e monitora o tipo e o tamanho das unidade instaladas nos dispositivos. Se a configuração mudar, é gerado um alerta.
- **Processador(es) adicionado(s), removido(s) ou modificado(s):** Este produto detecta e monitora o número, o tipo e a velocidade do(s) processadore(s). Se a configuração mudar, é gerado um alerta.
- **Placa de rede adicionada ou removida:** Este produto detecta e monitora o número e o tipo de placas de interface de rede nos dispositivos e gera alertas quando a configuração muda.

Para ver um registro de alerta das mudanças de configuração, consulte o log de alerta no console de informações do servidor. Consulte "Ver o log de alertas" para ver os detalhes.

# Monitoração de conectividade

Na maioria dos casos, os dispositivos podem alertá-lo quando ocorrem situações críticas, por exemplo, quando o espaço no disco rígido está acabando ou o ventilador parou de funcionar. Entretanto, em algumas situações, o dispositivo pode entrar off-line antes de enviar um alerta. Por exemplo, um switch ou um roteador podem interromper o tráfego de rede, ou pode haver falta de energia no dispositivo.

Nessas situações, este produto pode verificar os dispositivos periodicamente para determinar se eles estão disponíveis na rede. Se o dispositivo não responder ao ping, o seu status de funcionamento muda para Crítico  na próxima vez que você atualizar a lista **Meus dispositivos**.

Você deve configurar o monitor de dispositivos para fazer ping nos dispositivos selecionados ou em todos os dispositivos no grupo **Todos os dispositivos**.

**Para configurar o monitor de dispositivo**

1. Na lista **Meus dispositivos**, selecione os dispositivos que você deseja monitorar. Selecione-os em **Todos os dispositivos** ou em um grupo público ou privado.
2. Clique em **Alvo**.
3. No painel inferior, clique em **Ações** e, em seguida, em **Monitor de dispositivos**.
4. Para ver a lista de dispositivos sendo monitorados no momento, clique em **Mostrar dispositivos monitorados**.
5. Digite os minutos entre as varreduras de ping e o número de vezes que o produto tentará se comunicar com um dispositivo.
6. Selecione se deseja executar a ação nos dispositivos na Lista de dispositivos alvo ou em todos os dispositivos no grupo **Todos os dispositivos**.

7. Para parar a monitoração de todos os dispositivos, selecione **Nunca fazer ping de dispositivos**.
8. Clique em **Aplicar**.

Só é monitorado o último grupo de dispositivos alvo. Por exemplo, se você selecionar o dispositivo A e o dispositivo B, e aplicar a monitoração de dispositivos a eles, somente o dispositivo A e o dispositivo B receberão o ping do servidor núcleo. Se você então selecionar o dispositivo C e o dispositivo D como alvo e aplicar a monitoração de dispositivos a eles, somente o dispositivo C e o dispositivo D serão monitorados, os dispositivos A e B não serão mais monitorados.

# Configuração de alertas

## Utilização de alertas

Quando ocorre um problema ou outro evento em um dispositivo (por exemplo, o dispositivo está com pouco espaço no disco), 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 ao console e podem ser configurados para executar ações específicas. Leia este capítulo para ver como funcionam os alertas.


- Como ver os alertas?
- Que tipos de problemas de dispositivo podem gerar alertas?
- Configuração de níveis de severidade para eventos
- Processo para configuração do conjunto de regras personalizado de alertas
- Exemplo: Configuração de um conjunto de regras de alerta para um problema de espaço em disco


### Como ver os alertas?

Este produto pode notificá-lo sobre problemas ou outros eventos de computador ao:

- Adicionar informações ao log
- Enviar um aviso por email ou enviar uma mensagem para um pager
- Executar um programa no núcleo ou em um dispositivo individual
- Enviar uma interceptação SNMP para um console de gerenciamento de SNMP na rede
- Reinicializar ou desligar um dispositivo

Lembre-se de que certos agentes designados a grupos de máquinas podem gerar simultaneamente um grande número de respostas. Por exemplo, você pode configurar o alerta “Alteração da configuração do computador” e associá-lo a uma ação de email. Se um patch de distribuição de software for aplicado nessas máquinas com essa configuração de alerta, esta ação iria gerar um número de emails do servidor núcleo igual ao número de máquinas nas quais o patch foi aplicado, potencialmente “inundando” seu servidor de email. Neste caso, uma opção para lidar com esse alerta seria simplesmente gravá-lo no log do núcleo, em vez de enviar um email.

### Que tipos de problemas de dispositivo podem gerar alertas?

Este produto tem uma lista extensa de eventos que podem gerar alertas. Alguns são problemas que precisam atenção imediata; outros são mudanças de configuração que podem ou não ser um problema, mas que fornecem informações úteis a um administrador de sistema. (Consulte "Monitoração das mudanças de configuração", para ver as informações relacionadas.) Os alertas só podem ser gerados quando os dispositivos estão equipados com o hardware apropriado. Por exemplo, os alertas gerados por leituras de sensor só são aplicáveis a dispositivos equipados com os sensores corretos.

Os tipos de eventos que você pode, potencialmente, monitorar, estão relacionados abaixo:

- **Mudanças de hardware:** Um componente como, por exemplo, processador, memória, unidade ou placa que foi adicionada ou removida.
- **Aplicativos adicionados ou removidos:** Um aplicativo foi instalado ou desinstalado de um dispositivo.
- **Evento de serviço:** Um serviço foi iniciado ou parado no dispositivo.
- **Desempenho:** Um limite de desempenho foi passado, por exemplo, a capacidade de uma unidade, memória disponível, etc.
- **Evento IPMI:** Um evento detectável que ocorreu em dispositivos IPMI, o que inclui mudança em controladoras, sensores, logs, etc.
- **Uso do modem:** O modem do sistema foi utilizado ou foi adicionado ou removido um modem.
- **Segurança física:** Ocorreu uma intrusão no chassi, ciclagem de alimentação ou outra mudança física.
- **Instalação do pacote**: Foi instalado um pacote no computador de destino.
- **Atividade do controle remoto:** Ocorreu uma atividade de sessão de controle remoto, o que inclui iniciar, parar ou falhas.

A monitoração de hardware que gera os alertas depende das capacidades do hardware instalado em um dispositivo, assim como da correta configuração do hardware. Por exemplo, se um disco rígido com capacidades de monitoração S.M.A.R.T. for instalado em um dispositivo mas a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não suportar unidades S.M.A.R.T., os alertas não serão gerados a partir da monitoração da unidade S.M.A.R.T.

## Configuração de níveis de severidade para eventos

Problemas ou eventos podem ser associados a alguns ou a todos os níveis de gravidade mostrados.

- **Informativo:** Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas. Esse nível de gravidade não afeta o funcionamento do dispositivo.
- **OK:** Indica que o status é um nível aceitável.
- **Aviso:** Fornece algum tipo de advertência antecipada de um problema antes deste atingir um ponto crítico.
- **Crítico:** Indica que o problema precisa de atenção imediata.
- **Desconhecido:** Não é possível determinar o status de alerta ou o agente de monitoração não foi instalado no dispositivo.

Dependendo da natureza de um evento ou problema de servidor, alguns níveis de severidade não se aplicam e não são incluídos. Por exemplo, no caso do Evento de detecção de intrusão, o gabinete do dispositivo está aberto ou fechado. Se estiver aberto, isso pode iniciar uma ação de alerta com severidade de advertência. Outros eventos, como Espaço em disco e Memória virtual, contêm três níveis de gravidade (OK, Advertência e Crítico).

Você pode escolher o nível de severidade ou limite que dispara alguns alertas. Por exemplo, você pode selecionar diferentes ações como resultado de um status de Advertência ou Crítico de um alerta. O status desconhecido não pode ser selecionado como um disparador de alerta, ele só indica que o status não pode ser determinado.

## Processo para configuração do conjunto de regras personalizado de alertas

É possível configurar um conjunto de regras de alerta para distribuir para um dispositivo individual ou para um grupo de dispositivos de destino. Cada dispositivo gerenciado deve ter o componente de monitoração do produto instalado para poder enviar alertas ao servidor núcleo. (Consulte "Configuração de agentes" para mais informações.)

Quando o componente de monitoração é instalado em um dispositivo gerenciado, é incluído um conjunto de regras de alertas padrão para fornecer informações de status de condição ao  ao 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)

Além do conjunto padrão de regras, você pode configurar e distribuir conjuntos personalizados de regras. Você pode incluir ações de alerta personalizadas para responder a um evento em particular. Por exemplo, se um ventilador parar, ele pode disparar um alerta e enviar um email para o grupo de suporte do hardware.

O processo geral para a criação e distribuição de um conjunto de regras de alerta é o seguinte:

1. Selecione os dispositivos para os quais quer distribuir o conjunto de regras e clique em **Alvo** para adicioná-los à lista **Dispositivos alvo**.
2. Crie os conjuntos de regras de ação de alerta que você irá usar. Esses conjuntos de regras de ação definem os tipos de ações que podem ser iniciados pelos alertas. (Consulte "Configurar ações de alerta" para ver mais informações.)
3. Crie o seu conjunto de regras personalizado de alerta. Ao fazê-lo, poderá selecionar as ações definidas anteriormente. (Consulte "Configuração de um conjunto de regras de alerta" para ver mais informações.)
4. Distribuição do conjunto de regras aos dispositivos alvo. Dispositivos adicionais podem também ser alvos antes da distribuição do conjunto de regras. (Consulte "Distribuição dos conjuntos de regras" para ver mais informações.)

Segue um exemplo simples deste processo.

## Exemplo: Configuração de um conjunto de regras de alerta para um problema de espaço em disco

1. No painel esquerdo de navegação, clique em **Meus dispositivos**, em seguida clique duas vezes no grupo **Todos os dispositivos**.
2. Selecione os dispositivos para os quais quer definir o alerta, em seguida, clique em **Alvo** para colocar os dispositivos na lista **Dispositivos alvo**.
3. Clique em **Alertas**, em seguida clique na guia **Conjuntos de regras de acões**.

4. Na lista suspensa **Ações**, selecione a ação que você deseja configurar (por exemplo,**Enviar mensagem de email/pager**). Clique em **Nova**, digite um nome no campo **Nome**, em seguida clique em **OK**.
5. De volta na página **Conjunto de regras de ação**, selecione o conjunto de regras que você acabou de nomear e clique em **Editar ações**. Especifique os dados conforme forem necessários, nos quadros de texto. Ao terminar, clique em **Salvar**.
6. Clique na guia **Conjuntos de regras de alerta**.
7. Clique em **Novo**, digite algo do tipo "Problema de espaço em disco" no campo **Nome**, digite uma descrição no campo **Descrição** e clique em **OK**.
8. Clique no conjunto de regras de alerta que acabou de nomear e clique em **Editar conjunto de regras**.
9. Clique no botão **Nova**.
10. Na lista suspensa **Tipo de alerta**, clique em **Espaço em disco**.
11. Verifique cada status para o qual quiser gerar alerta: **OK**, **Aviso** ou **Crítico**. (Se quiser a mesma ação para múltiplos status, selecione mais de uma. Se quiser uma ação para cada status, crie uma configuração separada para cada status de forma que você possa disparar diferentes ações para diferentes níveis de status.)
12. Na lista **Ação**, selecione a ação que você deseja que ocorra se as condições especificadas nas etapas 6 e 7 forem satisfeitas. Se a ação não estiver na lista, crie uma usando a página **Conjuntos de regras de ações**. (Se não tiver criado um conjunto de regras de ações de alerta, ele não estará na lista.)
13. Na lista suspensa **Ação de alertas**, selecione a configuração que desejar.
14. Selecione **Afeta o funcionamento do dispositivo** se quiser que o alerta seja aplicado à condição do servidor quando ele for mostrado no na lista **Todos os dispositivos**. Se o nível de gravidade do alerta for apenas **Informativo**, o alerta não afetará o funcionamento do dispositivo.
15. Clique em **Adicionar**.
16. Repita as etapas de 6 a 12 para adicionar outros alertas ao conjunto de regras.
17. Ao concluir, clique em **Fechar**.
18. Se quiser mudar qualquer tipo de alerta no conjunto de regras, selecione o tipo de alerta e clique em **Editar**, faça as modificações, clique em **Atualizar**, em seguida clique em **Fechar**.
19. Quando o conjunto de regras de alerta for definido, aplique o conjunto de regras aos dispositivos alvo: clique em **Distribuição do conjunto de regras**, selecione o conjunto de regras e clique em **Distribuir**.

# Configuração de ações de alertas

Use a página **Conjunto de regras de ação** para fornecer informações adicionais sobre como você deseja que as ações se comportem quando forem selecionadas. Ao ser excedido um limite é gerado um alerta. O alerta pode ter uma ação associada a ele, por exemplo, enviar um email. Cada ação tem suas próprias configurações e deve ser configurada individualmente.

**Para criar um conjunto de regras de ação**

1. No painel de navegação esquerdo, clique em **Alertas**, em seguida clique na guia **Conjunto de regras de ação**.
2. Na lista suspensa **Ações**, selecione a ação que você deseja configurar. Cada ação tem sua própria lista de configurações únicas.
3. Clique em **Nova**, digite um nome no campo **Nome**, em seguida clique em **OK**.

4. De volta na página **Conjunto de regras de ação**, selecione o conjunto de regras que você acabou de nomear e clique em **Editar ações**.
5. Se você selecionou **Executar programa no núcleo** ou **Executar programa no cliente**, digite ou cole o caminho para o programa que deseja executar no alerta, em seguida clique em **Salvar**. Quando você selecionar a ação **Executar programa**, note que os programas podem não aparecer como esperado no desktop. Quando o programa é executado, ele é iniciado em Windows e, assim, ele não é mostrado da forma como um aplicativo normal aparece. Os programas que são executados dessa forma não devem conter interface de usuário que requer interação. Para determinar definitivamente se o programa foi executado, verifique os processos no Gerenciador de tarefas do Windows.

   Se você selecionou **Enviar email/mensagem de pager**, digite o endereço de email completo da pessoa para quem quer enviar o email no campo **Para**; digite um endereço de email válido no campo **De**; digite um assunto no campo **Assunto**; digite uma mensagem no campo **Corpo**; selecione o dia ou horário em que deseja que a mensagem seja enviada; e digite o local de um servidor SMTP no campo **Servidor SMTP**. Clique na caixa **Ajuda** para aprender a enviar mensagens para múltiplos destinatários e a usar variáveis nas mensagens. Quando terminar, clique em **Salvar**.

   Se tiver selecionado **Enviar uma interceptação SNMP**, digite o nome do host, selecione uma versão, digite a string da comunidade na caixa **String de comunidade**, em seguida clique em **Salvar**.

**Notas**

- Lembre-se de que certos alertas designados a grupos de máquinas podem gerar simultaneamente um grande número de respostas. Por exemplo, você pode configurar o alerta “Alteração da configuração do computador” e associá-lo a uma ação de email. Se um patch de distribuição de software for aplicado nessas máquinas com essa configuração de alerta, esta ação iria gerar um número de emails do servidor núcleo igual ao número de máquinas nas quais o patch foi aplicado, potencialmente “inundando” seu servidor de email. Neste caso, uma opção para lidar com esse alerta seria simplesmente gravá-lo no log do núcleo, em vez de enviar um email.
- Algumas ações de alerta não afetam o funcionamento do dispositivo. Isso inclui ações como, por exemplo, Executar programa no cliente, Desligar/Reiniciar e qualquer alerta informativo apenas. Entretanto, se algumas dessas ações forem combinadas com outras ações de alerta que afetam o funcionamento do dispositivo, então qualquer alerta gerado afetará o funcionamento do dispositivo e aparecerá no log de alerta.
- O campo **De** no email deve conter um endereço válido de email a fim do alerta do SMTP funcionar.
- As interceptações de SNMP identificadas como versão 1 são processadas, ao passo que as identificadas como versão 3 são apenas encaminhadas.
- Para interceptações SNMP, os níveis de gravidade são reportados no campo Tipo específico de interceptação. Os valores são 1 = desconhecido, 2 = info, 3 = OK, 4 = aviso, 5 = crítico.

# Configuração de conjunto de regras do alerta

Use a página **Conjunto de regras do alerta** para criar um novo conjunto. Antes de poder configurar alertas, você deve configurar ações. (Consulte "Configurar ações de alerta" para ver mais informações.)

Por padrão, dois conjuntos de regras de alerta aparecem na página **Conjuntos de regras de alerta**:

- **Conjunto de regras de alerta núcleo**: Este conjunto de regras assegura que os alertas sejam enviados ao servidor núcleo quando o recurso **Monitor de dispositivos** é habilitado (consulte Monitoração de conectividade). Este conjunto de regras contém um grupo pré-definido de tipos de alerta, inclusive os tipos de alerta monitor de Dispositivos, o Alerta de Interruptor de Circuito AMT e Sessão Serial Over LAN (SOL). Você pode editar o status, a ação, a ação de alerta e as configurações do estado de funcionamento para os tipos de alerta núcleo, mas se tentar fazer quaisquer outras mudanças, elas serão ignoradas.
- **Conjunto de regras padrão**: Este conjunto de regras é distribuído a todos os dispositivos gerenciados e contém um número de tipos de alertas para uso geral pela maioria dos administradores de rede. É possível editar este conjunto de regras para adicionar outros tipos de alerta e modificar as configurações para os tipos de alerta padrão. A qualquer momento em que editar este conjunto de regras, as mudanças são distribuídas a todos os dispositivos gerenciados, mesmo se você explicitamente não redistribuir o conjunto.

Além desses conjuntos de regras, é possível criar conjuntos personalizados e aplicá-los a grupos alvo de dispositivos gerenciados. Esses conjuntos de regras devem ser gerados em formato XML para serem exibidos na **Configuração de agente**.

---

Ao criar um conjunto de regras personalizado para um dispositivo observe que, se um conjunto padrão já tiver sido distribuído para o dispositivo, poderá haver sobreposição ou conflito de regras de alerta. Se você distribuir o conjunto de regras quando configurar o dispositivo gerenciado e, em seguida, distribuir um conjunto de regras personalizado, ambos os conjuntos serão executados no dispositivo. Por exemplo, se ambos os conjuntos de regras alertarem com o mesmo tipo de alerta, mas executarem ações diferentes, pode ocorrer ações de alerta duplicadas ou imprevisíveis. Embora não seja possível remover o conjunto de regras padrão uma vez que já tenha sido distribuído, você pode editá-lo se quiser mudar uma parte do mesmo.

---

**Para criar um conjunto de regras de alertas**

1. No painel de navegação esquerdo, clique em **Alertas**, em seguida clique na guia **Conjunto de regras de alerta**(se necessário).
2. Clique em **Nova**, digite um nome no campo **Nome**, digite uma descrição do alerta no campo
   **Descrição**, em seguida clique em **OK**.
3. Clique no conjunto de regras que acabou de nomear e clique em **Editar conjunto de regras**.
4. Clique em **Novo**.

5. Na lista suspensa **Tipo de alerta**, selecione o tipo de componente, ação ou evento sobre o qual você deseja receber alertas.
6. Verifique cada status para o qual quiser gerar alerta: **Informativo**, **OK**, **Aviso** ou **Crítico**. Por exemplo, para receber um alerta se o tipo selecionado na etapa 5 exceder o limite crítico, selecione **Crítico**.
7. Na lista **Ação**, selecione a ação que você deseja que ocorra se as condições especificadas nas etapas 5 e 6 forem satisfeitas. Essas ações são definidas antecipadamente; se quiser uma ação que não esteja na lista, crie uma usando a página **Conjunto de regras de ações**.

   **Nota:** Lembre-se de que certos alertas designados a grupos de máquinas podem gerar simultaneamente um grande número de respostas. Por exemplo, você pode configurar o alerta “Alteração da configuração do computador” e associá-lo a uma ação de email. Se um patch de distribuição de software for aplicado nessas máquinas com essa configuração de alerta, esta ação iria gerar um número de emails do servidor núcleo igual ao número de máquinas nas quais o patch foi aplicado, potencialmente “inundando” seu servidor de email. Neste caso, uma opção seria simplesmente gravar o alerta no log do núcleo, em vez de enviar um email.

8. Na lista suspensa **Ação de alertas**, selecione uma configuração. Pode haver somente uma configuração disponível (o conteúdo dessa lista muda, dependendo do que foi selecionado na etapa 7).
9. Selecione **Afeta o funcionamento do dispositivo** se quiser que o alerta seja aplicado à condição do servidor quando ele for mostrado no **Todos os dispositivos**. Se o nível de gravidade do alerta for apenas **Informativo**, o alerta não afetará o funcionamento do dispositivo.
10. Clique em **Adicionar**.
11. Repita as etapas de 5 a 10 para adicionar outros alertas ao conjunto de regras.
12. Ao concluir, clique em **Fechar**.

Para editar um conjunto de regras de alertas, selecione o conjunto (etapa 3) e clique em **Editar conjunto de regras**, em seguida prossiga com as etapas acima.

Alguns minutos após criar ou editar um conjunto de regras, o serviço de distribuição de conjunto de regras automaticamente tenta atualizar todos os computadores que receberam, anteriormente, uma distribuição daquele conjunto de regras. Ou, para distribuir o conjunto de regras imediatamente, clique na guia **Distribuir conjunto de regras** e clique em **Distribuir.**

# Distribuição do conjunto de regras

Use a página **Distribuir conjuntos de regras** para mover o alerta selecionado para os dispositivos alvo.

A fim de distribuir um conjunto de regras a um dispositivo gerenciado, é necessário primeiro instalar um agente de gerenciamento naquele dispositivo. Ao distribuir o agente padrão de gerenciamento, o conjunto de regras padrão é distribuído. Após a configuração do agente ser completada, você pode atualizar ou distribuir novos conjuntos de regras. Para começar, você deve definir os dispositivos alvo aos quais quer distribuir o conjunto de regras.

**Para distribuir um conjunto de regras de alerta**

1. No painel esquerdo de navegação, clique em **Meus dispositivos**, em seguida, clique no grupo **Todos os dispositivos**.
2. Selecione os dispositivos para os quais quer distribuir o conjunto de regras de alerta, em seguida, clique em **Alvo** para colocar os dispositivos na lista **Dispositivos alvo**.
3. No painel de navegação esquerdo, clique em **Alertas**, em seguida clique na guia **Distribuir conjuntos de regras**.
4. Na caixa **Conjuntos de regras de alerta**, selecione o conjunto de regras que desejar distribuir.
5. Clique no link para ver a lista de dispositivos alvo. Para remover um dispositivo da lista, clique nele com o botão direito, em seguida clique em **Excluir**. Para remover todos os dispositivos, clique com o botão direito em qualquer nome do dispositivo e clique em **Redefinir**. Para adicionar dispositivos, é necessário acrescentá-los à lista de alvos (etapas de 1 a 2, acima).
6. Feche a janela da **Lista de alvos**, em seguida clique em **Distribuir** para distribuir a configuração selecionada aos dispositivos alvo.

Como parte do processo de distribuição, é criada uma página em XML contendo os conjuntos de regras distribuídos e os dispositivos para os quais os conjuntos de regras foram distribuídos. Este relatório é salvo no servidor núcleo no diretório \ldlogon\alertrules e é nomeado com um número sequencial atribuído pelo banco de dados. Se quiser ver essa página XML separadamente da distribuição de um conjunto de regras, clique no botão **Gerar XML** e clique no link para ver o arquivo XML.

Lembre-se que somente um conjunto de regras personalizado por vez pode estar ativado em um dispositivo gerenciado. Se você tiver distribuído um conjunto de regras personalizado e, em seguida, distribuir um segundo conjunto no mesmo dispositivo, o primeiro será sobregravado e o segundo entrará em efeito.

# Como ver os conjuntos de regras de alerta de um dispositivo

Use a página **Conjunto de regras de alerta** para ver uma lista do conjunto de regras de alerta designadas a um dispositivo selecionado, e para ver os detalhes de cada alerta.

**Para ver os conjuntos de regras de alerta**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar. O console de Informações do servidor é aberto em outra janela do navegador.
2. No painel de navegação esquerdo, clique em **Conjuntos de regras**.
3. Clique na guia **Conjuntos de regras de alerta**.

O seguinte descreve os detalhes fornecidos sobre cada conjunto de regras. Para mais informações sobre a modificação desses detalhes, consulte Uso de alertas.

- **Quando o estado atingir:** Quando o estado do alerta atingir o estado exibido, será gerado um alerta.

- **Afeta o funcionamento:** Indica se o status do alerta será aplicado ao estado de funcionamento do servidor quando este for mostrado no  na lista **Todos os dispositivos**.
- **Nome do conjunto de regras:** O nome do conjunto de regras do alerta, como definido no diálogo Conjuntos de regras do alerta.
- **Tipo de alerta:**  Descrição da fonte do alerta (hardware, software, evento, etc.).
- **Configuração de ação:** A ação que ocorre quando o alerta é gerado, conforme definida no diálogo Configurações da ação.
- **Nome do manipulador:**  O tipo de alerta a ser gerado, por exemplo, um email, uma interceptação SNMP ou a execução de um programa.
- **Instância:** Indica a origem específica do alerta.

Você também pode clicar no botão **Log de alertas** para ir ao alerta do dispositivo e ver os detalhes sobre os alertas. (Consulte Ver o log de alertas para ver mais informações.)

# Ver o log de alertas

Use a página **Log de alertas** para ver os alertas enviados para o núcleo (log de alerta global) ou dispositivos gerenciados. O log é ordenado pela Hora (GMT). O evento mais recente encontra-se na parte superior do log.

O Log de alertas contém as seguintes colunas:

- **Nome do alerta:** O nome associado ao alerta, conforme definido na página **Configurações de alerta**.
- **Hora:** A data e a hora em que o alerta foi gerado (GMT).
- **Status:** O status do alerta, que pode ser um dos seguintes:
  - **Desconhecido:**  O status não pode ser determinado.
  - **Informativo:**  Suporta mudanças de configuração ou eventos que os fabricantes incluem em seus sistemas.
  - **OK:** Indica que o status é um nível aceitável.
  - **Aviso:** Fornece algum tipo de advertência antecipada de um problema antes que este atingir um ponto crítico.
  - **Crítico:** Indica que o problema precisa de atenção imediata.
- **Instância:** Indica a origem específica do alerta.
- **Nome do dispositivo:** O nome do dispositivo no qual o alerta foi gerado. Este deve ser um nome de domínio totalmente qualificado. (Somente log de alerta global.)
- **Endereço IP:** O endereço IP do dispositivo no qual o alerta foi gerado. (Somente log de alerta global.)

Se o nome do dispositivo não aparecer como nome de domínio totalmente qualificado, é porque este produto não conseguiu resolvê-lo para o dispositivo.

**Para ver o log de alertas globais**

1. No painel de navegação esquerdo, clique em **Logs**.
2. Para ordenar entradas por hora, nome, status ou instância, clique em um cabeçalho de coluna.
3. Para ver uma descrição mais detalhada do alerta, clique duas vezes na entrada, na coluna **Nome do alerta**.

4. Para mostrar as entradas por nome, status ou exemplo, selecione o critério de filtro na lista suspensa Filtro. Por exemplo, selecione **Nome do alerta** e digite um nome completo (por exemplo, Desempenho) ou um nome parcial com o caracter curinga * (por exemplo, Remoto*). Para fazer uma busca por data, selecione **Habilitar filtro de data**, insira uma faixa de datas com uma data inicial e outra final, e clique em **Buscar.**
5. Para limpar o status de funcionamento de um alerta, selecione o alerta clicando no número na coluna **Nome do alerta**, clique em **Limpar alerta** e clique em **OK**. Para excluir uma entrada de log, selecione o alerta e clique em **Excluir entrada.**
6. Para excluir todas as entradas no log, clique em **Purgar log**.

**Para ver o log de alertas de um dispositivo específico**

1. Clique duas vezes no dispositivo na lista **Meus dispositivos**.
2. No painel esquerdo, clique em **Informações do sistema**.
3. Clique em **Logs**, em seguida clique duas vezes em **Log de alertas**.
4. Para ordenar entradas por hora, nome, status ou instância, clique em um cabeçalho de coluna.
5. Para ver uma descrição mais detalhada do alerta, clique na entrada, na coluna **Nome do alerta**.
6. Para mostrar as entradas de log por nome, status ou instância, clique no botão **Filtrar** na barra de ferramentas e selecione os critérios de filtro. Por exemplo, selecione **Nome do alerta** e digite um nome completo (por exemplo, Desempenho) ou um nome parcial com o caracter curinga * (por exemplo, Remoto*). Em seguida, clique em Buscar na barra de ferramentas para ver os alertas associados às opções de filtro que você escolheu.
7. Para ver as entradas do log relativas a um intervalo de datas, desselecione a caixa de seleção **Mostrar eventos para todas as datas** e selecione o intervalo de datas específico. Clique em **Atualizar** para ver as entradas relativas àquele intervalo de datas.

# Atualizações de software

O System Manager contém uma ferramenta de atualizações de software que permite procurar atualizações para software de gerenciamento, software de sistemas operacionais e drivers de dispositivo. Esses tipos de atualização podem ser descarregados para corrigir dispositivos afetados através da distribuição e instalação das atualizações apropriadas a cada caso (que são também chamadas de patchs).

Este capítulo contém informações sobre:


- Visão geral das atualizações
- Sobre a janela Atualizações de software
- Configuração de dispositivos para análise de atualizações de software
- Atualização das definições de vulnerabilidades
- Agendamento de downloads de atualizações de software
- Como ver as informações de regras de atualização e detecção de software
- Depuração de informações de atualizações de software
- Análise de atualizações de software nos dispositivos
- Como ver as atualizações detectadas
- Download de patchs
- Correção de atualizações de software


## Visão geral das atualizações de software

As ferramentas de atualização de software ajuda a manter uma segurança contínua nos dispositivos gerenciados na sua rede. Você pode automatizar processo repetitivos de atualização de software, descarregando os arquivos corretos de atualização e distribuindo e instalando aquelas que são necessárias aos dispositivos afetados.

Este produto utiliza a administração baseada em funções padrão para permitir aos usuários acessarem a ferramenta de atualizações de software. A administração baseada em funções é o modelo de acesso e segurança do produto que permite aos administradores restringir acesso a ferramentas e dispositivos. Cada usuário recebe direitos e escopo específicos que determinam quais recursos podem usar e quais dispositivos podem gerenciar. Um administrador atribui esses direitos a outros usuários (consulte Sobre a administração baseada em funções para ver mais informações). Para usar a ferramenta de atualizações de software, o usuário deve estar conectado com direitos Gerenciador de patch (Patch Manager), Console básico de web, Relatórios e Relatório.

## Plataformas de servidores suportadas

A ferramenta Atualizações de software suportam a maioria das plataformas padrão de servidores, permitindo analisar atualizações e distribuí-las para servidores gerenciados que executam os seguintes sistemas operacionais:

- Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4

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

## Sobre a janela Atualizações de software

Usuários que têm o direito de gerenciamento de patch podem ver a ferramenta **Atualizações de software** no painel de navegação esquerdo do console. Quando você clica em **Atualizações de software**, aparece uma barra de ferramentas e dois painéis no lado direito da janela. O painel esquerdo mostra uma tela de árvore hierárquica dos grupos de atualização de software. Clique em um grupo para exibir seu conteúdo no painel direito. O painel direito exibe os detalhes de definição das atualizações de software em uma lista colunada. No topo, ele contém um botão **Localizar** que permite procurar rapidamente pelos critérios especificados. Na caixa **Localizar** não são suportados os seguintes caracteres estendidos: <, >, ', ", !.

## Botões da barra de ferramentas

- **Atualizar:** Abre a caixa de diálogo **Atualizar configurações das vulnerabilidades** na qual você pode especificar as plataformas e os idiomas cujas atualizações deseja fazer. Também é possível configurar se as atualizações serão adicionadas ao grupo **Analisar**, se o download das correções associadas será feito simultaneamente, o local onde as correções serão armazenadas após o download e as configurações do servidor proxy.
- **Agendar o download:** Abre a tarefa de download no diálogo **Tarefa agendada**, onde você pode configurar as opções da tarefa. Quando você clica em **Salvar**, a tarefa de download é colocada na janela **Tarefas agendadas**e na guia **Tarefas de vulnerabilidade**.
- **Agendar tarefas de patch:** Abre o diálogo **Agendar análise de vulnerabilidades**, onde você pode nomear a tarefa e configurar as opções do analisador.
- **Atualizar:** Atualiza a lista no painel direito com as informações de atualizações descarregadas mais recentes.
- **Purgar:** Abre o diálogo **Purgar definições de segurança e de patch** onde você pode especificar as plataformas e os idiomas cujas informações de vulnerabilidades deseja remover do banco de dados do núcleo.

## Painel esquerdo (tela de árvore)

O painel esquerdo da janela mostra os seguintes grupos:

- **Analisar:** Relaciona todas as atualizações que são pesquisadas quando a ferramenta de atualização de software é executada nos dispositivos gerenciados. Em outras palavras, se houver uma atualização nesse grupo, ela fará parte da próxima operação de análise; caso contrário, ela não fará parte da análise.

  A análise pode ser considerada um dos três estados de vulnerabilidade, em conjunto com Não analisar e Não atribuída. Assim, uma atualização de software pode existir em apenas um desses três grupos em um dado momento. A atualização é identificada por um ícone exclusivo para cada estado (ponto de interrogação (?) para Não designado, X vermelho para Não analisar e o ícone normal de vulnerabilidade para Analisar). A mudança de uma atualização de um grupo a outro muda o seu estado automaticamente.

  Para mover uma atualização de software de um grupo para outro, clique com o botão direito na atualização e selecione o grupo.

  Ao mover atualizações a um grupo Analisar, você pode controlar a natureza e o tamanho específicos da próxima análise de atualização de software.

  As novas atualizações também podem ser acrescentadas automaticamente ao grupo Analisar durante uma atualização selecionando a opção **Colocar as novas definições no grupo Analisar** no diálogo **Configurações da atualização de vulnerabilidades**.

  **Precaução ao mudar atualizações de software do grupo Analisar**
  Quando você transfere atualizações de software do grupo Analisar para o grupo Não analisar, as informações atuais contidas no banco de dados núcleo sobre quais dispositivos analisados detectaram essas atualizações são removidas do banco de dados e não ficam mais disponíveis no diálogo Propriedades das atualizações de software nem no diálogo Informações de servidores analisados. Para restaurar as informações de avaliação, é necessário transferir as atualizações de software de volta ao grupo Analisar e executar novamente a análise.

- **Não analisar:** Relaciona as atualizações de software que não serão pesquisadas na próxima vez em que o analisador for executado nos dispositivos. Conforme mencionado anteriormente, se uma atualização estiver neste grupo, ela não poderá estar no grupo Analisar ou Não designado. Você pode mover as atualizações para este grupo para removê-las de uma análise de atualizações de software.

- **Detectadas:** Relaciona todas as atualizações de software detectadas pela análise anterior, para todos os dispositivos alvo incluídos na tarefa de análise. O conteúdo deste grupo é sempre determinado pela última análise de atualizações de software, independente de um ou vários dispositivos terem sido analisados.

  A lista Detectadas é um conjunto de todas as atualizações de software detectadas encontradas pela análise mais recente. As colunas Analisadas e Detectadas são úteis para mostrar quantos dispositivos foram analisados e em quantos desses dispositivos foram detectadas atualizações. Para ver especificamente em quais servidores foram detectadas atualizações, clique com o botão direito na definição **Ver computadores afetados**. Observe que também é possível ver as informações de atualização de um servidor específico em seu diálogo Console de informações do servidor.

  As atualizações de software podem ser movidas somente do grupo Detectadas para os grupos Não analisar ou Não atribuídas.

- **Não atribuídas:** Relaciona todas as atualizações de software que não pertencem aos grupos Analisar ou Não Analisar. O grupo Não designadas é basicamente uma área de armazenamento das atualizações coletadas até que você decida se elas devem ser analisadas ou não.

  Como padrão, as atualizações de software coletadas são adicionadas ao grupo Analisar durante uma atualização.

  Você pode mover as atualizações de software do grupo Não atribuídas para os grupos Analisar ou Não analisar.

- **Visualizar por SO:** Relaciona todas as atualizações de software carregadas, organizadas em subgrupos de sistemas operacionais de distribuidores específicos. Esses subgrupos ajudam a identificar atualizações pela categoria SO. Utilize estes subgrupos de SO para copiar um conjunto de atualizações para o grupo Analisar, para que possa fazer uma análise de um SO específico.

  As atualizações de software podem ser copiadas de um grupo de SO para o grupo Analisar, Não analisar ou Não atribuídas. As atualizações podem residir em mais de um grupo de plataformas e/ou produtos simultaneamente.

- **Visualizar por produto:** Relaciona todas as atualizações de software descarregadas organizadas em subgrupos de produto específicos. Esses subgrupos ajudam a identificar atualizações por produto. Utilize estes subgrupos de produtos para copiar um conjunto de atualizações para o grupo Analisar, para que possa fazer uma análise de um produto específico.

## Painel direito (mostrar tela)

O painel direito da janela exibe os seguintes detalhes de atualizações de software, listadas em colunas que podem ser ordenadas:

- **ID:** Identifica a atualização com um código alfanumérico exclusivo, definido pelo fornecedor.

- **Gravidade:** Indica o nível de gravidade da atualização. Os níveis possíveis de gravidade são: Service Pack, Crítica, Alta, Média, Baixa, Não aplicável (N/A) e Desconhecida.
- **Título:** Descreve a natureza ou alvo da atualização em um breve texto.
- **Idioma:** Indica o idioma do SO afetado pela atualização.
- **Data de publicação:** Indica a data em que a atualização foi publicada pelo fornecedor.
- **Instalação silenciosa:** Indica se o arquivo do patch associado à atualização será instalado silenciosamente (sem interação com o usuário). Algumas atualizações podem ter mais de um patch. Se algum dos patchs da atualização não puder ser instalado silenciosamente, o atributo Instalação silenciosa da atualização mostrará Não.
- **Reparável:** Indica se a atualização pode ser consertada com a distribuição e instalação do arquivo de correção. Os possíveis valores são os seguintes: Sim, Não e Alguns (para uma atualização que inclua várias regras de detecção e nem todas as atualizações detectadas podem ser reparadas).

Clique duas vezes na ID da atualização para ver informações mais detalhadas no diálogo Propriedades. No diálogo propriedades de uma atualização de software, você pode ver as regras de detecção da atualização, baixar arquivos de patches associados e clicar na regra para ver seu diálogo de propriedades detalhadas.

## Configuração de dispositivos para análise de atualizações de software

Para os dispositivos gerenciados serem analisados à procura de vulnerabilidades de software e receberem distribuições de patchs, o agente de Atualizações de software deve estar instalado.

A maneira mais fácil de distribuir o agente de Atualizações de software para vários dispositivos gerenciados é criar uma nova configuração de agentes com o agente de Atualizações de software selecionado (configuração padrão), e, em seguida, agendar a configuração para os dispositivos alvo desejados com a ferramenta **Tarefas agendadas**.

Quando um dispositivo é configurado para suportar atualizações de software, os arquivos necessários para a análise de atualizações e correção (por exemplo, distribuição e instalação de patchs) são instalados no dispositivo alvo.

## Atualização das definições de atualizaç ão de software

A sua rede é continuamente vulnerável a problemas de manutenção como atualizações de software e correções de defeitos (bugs). A ferramenta de atualizações de software facilita e acelera o processo de coleta das informações mais recentes sobre patchs permitindo a atualização de software por meio de um banco de dados da LANDesk. Esse serviço de segurança consolida as atualizações, obtidas de fontes confiáveis da indústria ou de fornecedores.

Ao estabelecer e manter informações atualizadas de patch, você pode compreender melhor a natureza e a extensão da atualizações de software necessárias para cada sistema operacional de servidor que você suporta. A primeira etapa é manter-se atualizado com as mais recentes e conhecidas informações sobre atualizações.

Você pode configurar e fazer atualizações de software de uma só vez ou criar uma tarefa agendada de atualização de vulnerabilidades a ser realizada em um determinado momento ou como uma tarefa recorrente.

**Para atualizar as informações de software**

1. No painel de navegação esquerdo, clique em **Atualizações de software**. (Para ver uma descrição do diálogo, consulte Sobre a janela Atualizações de software.)
2. Clique no botão **Atualizar** da barra de ferramentas.
3. Selecione o site de origem de downloads na lista de servidores de conteúdo disponíveis.
4. Selecione as plataformas cujas informações de atualização de software deseja atualizar. Selecione uma ou mais plataformas na lista. Quanto mais plataformas você selecionar, maior será o tempo necessário para a atualização.
5. Selecione os idiomas cujas informações de atualização de software deseja atualizar para as plataformas que especificar. Você pode selecionar um ou mais idiomas na lista. Quanto mais idiomas você selecionar, maior será o tempo necessário para a atualização.
6. Se desejar que novas definições de atualizações de software (aquelas que ainda não existem no banco de dados) sejam colocadas automaticamente no grupo Não atribuídas em vez de no local padrão, que é o grupo Analisar, desmarque a caixa de seleção **Colocar as novas definições no grupo Analisar**.
7. Se desejar fazer automaticamente o download dos arquivos executáveis dos patches, selecione **Fazer o download dos patchs para definições selecionadas acima**, em seguida clique em uma das opções de download.

    - **Para definições detectadas somente:** Faz o download apenas dos patches associados às atualizações de software detectadas pela última análise de atualizações (por exemplo, as atualizações que atualmente residem no grupo Detectadas).
    - **Para todas as definições referenciadas:** Faz o download de TODOS os patchs associados às atualizações de software que atualmente residem no grupo Analisar. Isso leva muito tempo.

Os patches são baixados para o local especificado na seção Configurações do patch do diálogo (veja os procedimentos abaixo).

8. Se tiver um servidor proxy na rede usado para transmissões externas da Internet (necessárias para atualizar as informações de atualizações de software e fazer o download das correções), clique na guia **Configurações de proxy** e marque a caixa **Usar o servidor proxy**. Especifique o endereço do servidor, número da porta e as credenciais de autenticação se um login for requerido para acessar o servidor proxy.
9. Clique em **Aplicar** a qualquer momento para salvar as configurações.
10. Clique em **Atualizar agora** para executar a atualização de software. O diálogo **Atualização de definições de segurança e patch** mostra a operação atual e o status.
11. Quando a atualização estiver concluída, clique em **Fechar**. Observe que se você clicar em**Cancelar** antes do término da atualização, somente as informações de atualização de software que já foram processadas até este ponto são inseridas no banco de dados núcleo. Seria necessário executar a atualização novamente para obter as informações de vulnerabilidades restantes.

**Nota:** Não feche o console enquanto estiver ocorrendo um processo de atualização de atualização ou o processo será interrompido. Isso não se aplica a uma tarefa agendada de download.

Se tiver instalado o System Manager e o LANDesk® Management Suite no mesmo servidor núcleo, ambos os produtos usarão as mesmas configurações para determinar que tipos de vulnerabilidades estão atualizadas. Em alguns casos você pode ver atualizações no System Manager as quais só são configuráveis do Management Suite quando a atualização for executada. Por exemplo, se tiver selecionado Ameaças de segurança como opção no Management Suite e decidir atualizar as Atualizações de software no System Manager, quando executar a atualização no System Manager você verá as Atualizações de software e as ameaças de segurança nos itens atualizados.

**Para configurar o local de download dos patches**

1. No diálogo **Atualização das configurações de vulnerabildiade**, clique na guia **Configurações do patch**.
2. Digite um caminho UNC para onde os arquivos de patches serão copiados. O local padrão é o diretório \LDLogon\Patch do servidor núcleo.
3. Se o caminho UNC digitado for de um local diferente do servidor núcleo, digite um nome de usuário e uma senha válidos para autenticar-se nesse local.

   Compartilhamento de arquivos e web, e acesso Anônimo devem estar habilitados na pasta.

4. Digite um URL da Web onde os servidores possam acessar os patches baixados para distribuição. O URL da Web deve ser igual ao caminho UNC acima.
5. Você pode clicar em **Testar configurações** para verificar se pode ser feita uma conexão com o endereço da Web especificado acima.
6. Se desejar restaurar o caminho UNC e o URL da Web para seus locais padrão, clique em **Restaurar configurações de patch**. O local padrão é o diretório \LDLogon\Patch do servidor núcleo.

## Agendamento de downloads de atualizações de software

Você também pode configurar as atualizações de software como uma tarefa agendada a ser realizada futuramente ou como uma tarefa recorrente. Para fazer isto, clique no botão da barra de ferramentas **Agendar o download** para abrir o diálogo **Propriedades de tarefa agendada**, onde você pode nomear a tarefa e configurar suas opções . Quando você clicar em **Salvar**, a tarefa aparecerá na janela Tarefas agendadas.

Todas as tarefas agendadas de atualização de software utilizarão as configurações atuais encontradas nos diálogo **Atualização das configurações de vulnerabilidades**. Assim, se desejar mudar o site de origem, as plataformas, os idiomas, o site de download de patchs ou as configurações do servidor proxy para uma determinada tarefa de atualização, você deverá primeiro alterar essas configurações no diálogo **Atualização das configurações de vulnerabilidades** antes da tarefa ser agendada para execução.

**Para configurar uma tarefa de download**

1. No painel de navegação esquerdo, clique em **Atualizações de software**.
2. Clique em **Agendar o download**.
3. Na página **Agendar tarefa**, configure o agendamento.

4. Clique em **Salvar**.

Ao clicar em **Agendar download**, é criada uma tarefa (ela não tem dispositivos alvo e é não agendada). Se você cancelar este procedimento de **Tarefas agendadas**, esteja ciente que elas ainda estão sendo criadas e aparecem na lista **Minhas tarefas**.

## Como ver as informações de regras de atualização e detecção de software

Após as atualizações de software terem sido atualizadas com as informações mais recentes do serviço de segurança da LANDesk, você pode ver as listas de atualizações de software no console, ver as listas por plataforma e produto, e mover as atualizações para diferentes grupos de status. Para ver informações sobre os diferentes grupos na janela e sobre como usá-los, consulte Sobre a janela de atualizações de software, anteriormente neste capítulo.

Para ver os detalhes de atualização de software, clique duas vezes em um ID de atualização de software para abrir o respectivo diálogo Propriedades. Desse diálogo, você também pode acessar os detalhes das regras de detecção, se clicar duas vezes no nome do arquivo do patch na lista **Regras de detecção** para abrir o diálogo Propriedades do patch (consulte Sobre o diálogo Propriedades do patch).

Essas informações podem ajudá-lo a determinar quais atualizações são relevantes para as plataformas de servidores suportadas na rede, como as regras de detecção de uma atualização verificam a presença da vulnerabilidade, quais patchs estão disponíveis, e como configurar e realizar correções nos dispositivos afetados.

Você também pode ver informações de atualização de software e regras de detecção específicas para os dispositivos analisados diretamente do console, acessando o console de informações de servidor em **Meus dispositivos**, e clicando em **Atualizações de software** no painel de navegação esquerdo.

## Depuração de informações de atualizações de software

Você pode purgar as informações de atualizações de software da janela de atualizações de software (e do banco de dados núcleo) se decidir que elas não são relevantes para seu ambiente.

Quando são purgadas as informações de atualizações de software, as informações das regras de detecção associadas também são removidas do banco de dados. Entretanto, os arquivos executáveis do patch não são removidos por este processo. Os arquivos dos patches devem ser removidos manualmente do repositório local, que normalmente se encontra no servidor núcleo.

**Depuração de informações de atualizações de software**

1. Clique no botão da barra de ferramentas **Purgar**. (Para ver uma descrição do diálogo, consulte Sobre o diálogo Purgar definições de segurança e patch.)

2. Selecione as plataformas cujas informações de atualização de software que deseja remover. Você pode selecionar uma ou mais plataformas na lista.

   Se uma atualização é associada com mais de uma plataforma, você deve selecionar todas as plataformas associadas para que as informações de atualização sejam removidas.

3. Selecione os idiomas cujas informações de atualização você quer remover (associada à plataforma selecionada acima).

   Se selecionou uma plataforma Windows acima, você deve especificar o idioma das informações de atualização que quer remover. Se você selecionar uma plataforma UNIX acima, deverá especificar a opção Independente de idioma para remover as informações de atualização em vários idiomas.

4. Clique em **Remover**.

## Análise de atualizações de software nos dispositivos

Avaliação de atualização de software significa verificar as versões atualmente instaladas de arquivos específicos do sistema operacional e as chaves de registro em um dispositivo quanto às atualizações de software conhecidas mais recentes para identificar as necessidades de atualização de seus servidores. Depois de revisar as informações conhecidas de atualização de software (atualizadas em fontes da indústria) e decidir quais atualizações devem ser analisadas, você poderá realizar avaliações personalizadas de vulnerabilidades nos dispositivos gerenciados que tenham o agente de Atualizações de software instalado. (Para ver informações sobre a configuração dos dispositivos para a análise de vulnerabilidades e distribuição de patchs, consulte "Configuração de dispositivos para a análise de atualização de software", anteriormente neste capítulo).

Quando a análise de atualização de software é executada, ela sempre lê o conteúdo do grupo Analisar e faz a análise verificando se essas atualizações existem. Antes de fazer a análise de servidores a procura de atualizações, certifique-se de que somente as atualizações de software que deseja analisar se encontram naquele grupo. É possível mover atualizações de software de e para o grupo Analisar de modo a personalizar o tamanho e a natureza da análise.

## Execução do analisador de atualização de software

O analisador de atualizações de software também pode ser enviado, do console para dispositivos, como uma tarefa de análise agendada.

**Para criar uma tarefa de análise de atualizações de software**

1. No painel de navegação esquerdo, clique em **Atualizações de software**.
2. Certifique-se de que as definições de atualização de software tenham sido atualizadas recentemente.
3. Certifique-se de que o grupo Analisar contenha somente as atualizações a serem analisadas.
4. Clique no botão **Agendar tarefas de patch** na barra de ferramentas. (Para ver uma descrição do diálogo, consulte "Sobre o diálogo Agendar análise de vulnerabilidades".)

5. Digite um nome exclusivo para a análise. Se o script da tarefa já existir, você pode escolher se deseja substituir o script existente.
6. Especifique se deseja que o analisador de atualizações de software mostre um diálogo de andamento no dispositivo alvo. É também possível especificar se você deseja que seja mostrado o botão Cancelar no diálogo do analisador, para que o usuário final tenha a opção de cancelar a análise.
7. Especifique como você deseja que o diálogo do analisador de atualizações de software se feche após terminar a sua execução nos dispositivos alvo. É possível exigir a interação do usuário final ou configurar o diálogo para se fechar após um tempo de espera especificado.
8. Clique em **OK**.
9. Selecione a tarefa no painel inferior (sob **Tarefas de vulnerabilidade**) e clique em **Editar**. Defina os parâmetros de alvo e de agendamento, e clique em **Salvar**.

## Como ver as atualizações detectadas

Se a análise descobrir atualizações para qualquer uma das atualizações de software habilitadas que estão incluídas em qualquer um dos dispositivos alvo, essas informações serão enviadas ao servidor núcleo e adicionadas à lista **Detectadas**.

Você pode usar qualquer um dos métodos abaixo para ver atualizações detectadas após executar uma análise de atualizações de software:

### Pelo grupo Detectadas

Selecione o grupo **Detectadas** na janela Atualizações de software para ver uma lista completa de todas as que tiverem sido detectadas pela análise mais recente.

### Por dispositivo individual

Clique duas vezes no nome de um dispositivo em **Meus dispositivos** e, em seguida, clique em **Atualizações de software** para ver informações detalhadas de avaliação de atualizações de software para o dispositivo.

## Download de patches

Para distribuir patchs de segurança para dispositivos com atualizações de software detectadas, o arquivo executável do patch deve primeiramente ser carregado em um repositório local de patchs na sua rede. O local padrão para downloads de arquivos de patchs é o diretório /LDLogon do servidor núcleo. Você pode mudar esse local na guia **Configurações do patch** do diálogo **Configurações da Atualização de vulnerabilidades**.

**Configurações do local de download de patchs e do servidor proxy**
Os downloads de patchs sempre utilizam as configurações do local de download presentes na guia **Configurações do patch** do diálogo **Configurações da atualização de vulnerabilidades**. Observe também que, se a rede usar um servidor proxy para acesso à Internet, você deverá primeiro definir as configurações do servidor proxy na guia **Configurações do proxy** no diálogo **Configurações da atualização de vulnerabilidades**, antes de fazer o download de arquivos de patchs.

O produto tenta primeiro descarregar um arquivo de correções do URL, mostrado na caixa de diálogo Propriedades de correção. Se não for possível fazer uma conexão, ou se a correção não estiver disponível por alguma razão, o produto fará o download do patch do serviço de segurança da LANDesk, que é um banco de dados hospedado da empresa contendo patchs de fontes confiáveis da indústria.

Você pode fazer o download de um patch de cada vez ou de um conjunto de patches simultaneamente.

**Para fazer o download de patches únicos**

1. Clique duas vezes no nome de uma atualização de software para abrir o seu diálogo **Propriedades**.
2. Na seção **Regras de detecção**, selecione os arquivos de patches da regra de detecção que deseja baixar, em seguida clique em **Fazer o download dos patches selecionados**.
3. A operação de download e o status são mostrados no diálogo **Fazendo o download** dos patches. Você pode clicar em **Cancelar** a qualquer momento para interromper o processo de download.
4. Quando o download estiver concluído, clique no botão **Fechar**.

**Para fazer o download de múltiplos patches**

Todas as tarefas agendadas de atualização de software utilizarão as configurações atuais encontradas nos diálogo **Atualização das configurações de vulnerabilidades**. Assim, se desejar mudar o site de origem, as plataformas, os idiomas, o site de download de patchs ou as configurações do servidor proxy para uma determinada tarefa de atualização, você deverá primeiro alterar essas configurações no diálogo **Atualização das configurações de vulnerabilidades** antes da tarefa ser agendada para execução.

1. No painel de navegação esquerdo, clique em **Atualizações de software**.
2. Clique em **Agendar o download**.
3. Na página **Agendar tarefa**, configure o agendamento.
4. Clique em **Salvar**.

## Remoção dos arquivos de patches

Para remover arquivos de patchs, você deve excluir os arquivos manualmente do repositório de patchs, que normalmente se encontram no servidor núcleo do diretório LDLogon.

## Correção de atualizações de software

Após ter atualizado as definições de atualizações de software, colocado as atualizações que desejar analisar no grupo Analisar, executado uma análise nos dispositivos gerenciados, determinado quais atualizações de software exigem a sua atenção, e carregados os patchs necessários, o próximo passo é executar o reparo das mesmas através da distribuição e instalação dos patchs necessários nos dispositivos afetados.

A correção de atualizações de software é feita individualmente. Em outras palavras, você cria uma tarefa de correção para uma atualização de software específica que distribui e instala os arquivos patch necessários.

Observe que as correções, como a análise de atualizações de software, funcionam apenas em dispositivos que foram configurados com o agente das Atualizações de software. Ser precisar de mais informações, consulte Configuração de dispositivos para a análise de atualizações de software, anteriormente neste capítulo.

A correção Linux é suportada. Você pode usar a ferramenta Atualizações de software para descobrir vulnerabilidades em dispositivos Linux e decidir se vai corrigí-las. Se quiser, você pode usar uma assinatura de suporte do fornecedor do Linux para o download dos RPMs necessários e, a seguir, distribuir os RPMs para dispositivos.

**Aviso:** Muitos patchs reinicializarão automaticamente o dispositivo ao terminar.

**Para criar um script de reparo personalizado**

1. No painel de navegação esquerdo, clique em **Atualizações de software**.
2. Selecione o grupo **Detectadas** para ver as atualizações de software detectadas pela análise mais recente. (Você não tem de selecionar este grupo. Se desejar criar um script de reparo personalizado para atualizações que ainda não foram analisadas, ou que ainda não foram detectadas, clique em qualquer um dos outros grupos de vulnerabilidades para ver seu conteúdo, e selecione uma vulnerabilidade específica).
3. Clique com o botão direito na definição e selecione **Ver dispositivos afetados** para ver os dispositivos que são afetados por essa atualização de software.
4. Clique duas vezes na definição e selecione **Criar tarefa de correção**.
5. (opcional) Modifique o nome na caixa de texto **Nome da tarefa**.
6. Selecione uma opção e clique em **OK**.
    - **Cópia dos computadores afetados à cesta alvo:** Copia os computadores afetados pela atualização de software à cesta alvo, para correção.
    - **Exibir o andamento ao executar:** Habilita a análise para mostrar informações sobre os dispositivos do usuário final enquanto estiver sendo executada. Clique nesta opção se quiser mostrar a atividade da análise e se quiser configurar outras opções de exibição e interação nesta caixa de diálogo. Se não clicar nesta opção, nenhuma das outras opções desta caixa de diálogo estará disponível para configurar e a análise será executada de modo transparente nos dispositivos.
    - **Requer informações fornecidas pelo usuário antes de fechar o diálogo análise de vulnerabilidade**: Clique nesta opção se quiser que a análise avise o usuário antes de seu diálogo fechar no dispositivo. Se selecionar esta opção e o usuário final não responder, o diálogo permanece aberto, o que pode fazer com que o limite de outras tarefas agendadas vença.
    - **Fechar automaticamente o diálogo após a espera:** Clique nesta opção se quiser que o diálogo da tela da análise feche após a duração que especificar.

# Scripts

## Gerenciamento de scripts

Este produto usa scripts para executar tarefas personalizadas em dispositivos. Completar as caixas de diálogos de criação de script gera um arquivo ASCII no formato INI Windows com uma extensão .INI. Esses scripts são armazenados no servidor núcleo, na pasta \Arquivos de programas\LANDesk\ManagementSuite\Scripts. O nome de arquivo do script torna-se o nome do script no console. Crie scripts de agendador local para dispositivos Windows usando a janela **Scripts** (clique em **Scripts** no painel esquerdo de navegação) ou crie manualmente seus próprios arquivos de script e salve-os na pasta Scripts.

A janela **Scripts** é dividida nas seguintes categorias:

- **Meus scripts:** Scripts associados a este grupo.
- **Todos os outros scripts:** Todos os scripts no servidor núcleo.
- **Scripts de usuário** (somente visível aos administradores): Scripts criados por todos os usuários do produto. Esses scripts são ordenados pelo nome de quem criou.

Você pode criar grupos sob o item **Meus scripts** para categorizar mais seus scripts. Para criar um novo script de agendador local, clique no botão **Local**.

Ao terminar de criar um script, você pode clicar em **Agendar** no menu de atalho do script. Na janela **Meus dispositivos**, você pode selecionar dispositivos com alvo nos quais deve ser executada a tarefa e agendar o horário de execução da tarefa na janela **Tarefas agendadas**. Consulte a seção Tarefas agendadas para ver mais informações sobre o agendamento de tarefas.

### Mudanças ao script e propriedade da tarefa para usuários de versões Management Suite anteriores

Nas versões Management Suite anteriores a 8.70, todos os scripts eram globais e todos os usuários podiam vê-los. Agora os scripts são apenas visíveis ao criador do script e aos administradores.

A janela **Scripts** contém a coluna Estado. A coluna Estado aparece como Público se todos os usuários puderem ver o script ou Privado se apenas o usuário que criou o script ou os administradores puderem vê-lo. Os usuários podem clicar com o botão direito nos scripts que tiverem criado e em Privado ou em Público para mudar o estado do script. Os administradores podem mudar o estado de qualquer script.

O PE (Ambiente de pré-inicialização) DOS é o padrão. Se selecionou outro PE, não será possível criar um script de comando. Com os PEs Windows e Linux só é possível gerar script de captura ou de distribuição.

Se escolher o PE Linux, só estará disponível o LANDesk ou Outras opções de ferramenta de imagem. Se escolher o PE Windows, estarão disponíveis LANDesk, Outro e Microsoft* XImage.

# Criação de um script de agendador local

O agendador local é um serviço executado nos computadores dispositivos. Ele é instalado quando você distribui uma configuração de agente como parte do agente padrão de gerenciamento. Em geral, o planejador local cuida das tarefas do produto como, por exemplo, execução do analisador de inventário periodicamente. Outras tarefas que você agenda, são executadas pelo servidor núcleo em vez do planejador local. Você pode usar o planejador local para agendar suas próprias tarefas de forma a executá-las periodicamente nos dispositivos. Ao ser criado o script do agendador local, você pode distribuí-lo aos dispositivos gerenciados, da mesma forma como faria com outro script.

O planejador local atribui a cada tarefa um número de ID. Os scripts do agendador local têm uma faixa de IDs diferente dos scripts de agendador local padrão utilizado pelo produto. Você pode ter somente um script de agendador personalizado ativo em cada dispositivo. Se você criar um novo script e distribuí-lo aos dispositivos, ele substituirá o script antigo (qualquer script na faixa de IDs do planejador local personalizado) sem afetar os scripts de planejador local padrão como, a agenda de varredura de inventário local.

Ao selecionar opções de agendar para o script, lembre-se das qualidades restritivas das várias opções. Por exemplo, se selecionar segunda-feira para o dia da semana e 17 para o dia do mês, a tarefa só será executada numa segunda-feira que seja também 17 do mês, o que ocorre com pouca freqüência.

Você pode criar um script para executar o restartmon.exe em um computador local imediatamente ou no momento que preferir. Se estiver fazendo um relatório de um computador específico que parece ter parado, você pode usar o restartmon.exe na pasta LDClient para reiniciar o coletor e todos os provedores de monitoração. Esse utilitário é para computadores onde foi instalada a opção de relatório e essa função parou. Use esse utilitário para reiniciar o coletor e os provedores sem ter que reinicializar o dispositivo.

1. No painel de navegação esquerdo, clique em **Scripts**.
2. Clique em **Local**.
3. Digite um nome de script.
4. Clique em **Adicionar** para definir as opções do script.
5. Configure as opções do planejador local conforme descrito anteriormente. Ao terminar, clique em **Salvar**.
6. Clique em **Salvar** para salvar o script.
7. Selecione o script no grupo **Meus scripts**, em seguida, clique em **Agendar** para distribuir o script que criou para os dispositivos.

# Opções de largura de banda

Ao configurar comandos do agendador local, você pode especificar os critérios mínimos de largura de banda necessários que o dispositivo gerenciado deve ter para a tarefa ser executada. Quando for o momento de execução da tarefa, cada dispositivo que estiver executando a tarefa do planejador local enviará uma pequena quantidade de tráfego de rede de ICMP para o computador que você especificar e avaliará o desempenho. Se o computador alvo de teste não estiver disponível, a tarefa não será executada.

Podem ser selecionadas as seguintes opções de largura de banda:

- **RAS:** A tarefa é executada se a conexão de rede do dispositivo ao computador de destino tiver pelo menos RAS ou velocidade de dial-up. A seleção dessa opção, em geral, significa que a tarefa sempre será executada se o dispositivo tiver algum tipo de conexão de rede.
- **WAN:** A tarefa é executada se a conexão do dispositivo ao computador de destino tiver pelo menos velocidade de WAN. Velocidade WAN é definida como uma conexão não RAS que é mais lenta que o limite da LAN.
- **LAN:** A tarefa é executada se a conexão do dispositivo ao computador alvo exceder o parâmetro de velocidade de LAN. Como padrão, a velocidade da LAN é definida como 262.144 bps.

## Agendamento de tarefas de scripts

A janela **Tarefas agendadas** mostra o status da tarefa agendada enquanto a tarefa está em execução e na sua conclusão. O serviço de agendador tem dois meios de se comunicar com os dispositivos:

- Por meio do agente padrão de gerenciamento (que já deve estar instalado nos dispositivos).
- Por meio de uma conta de sistema em nível de domínio. A conta escolhida deve ter o login como privilégio de serviço e você deve ter especificado credenciais no utilitário Configurar serviços. Para ver mais informações sobre a configuração da conta do agendador, consulte a "Configuração do serviço do agendador".

O LANDesk instala vários scripts padrão que podem ser agendados para executar tarefas de manutenção de rotina, tais como a execução de varreduras de inventário nos computadores selecionados.  Clique em **Scripts** no painel esquerdo de navegação e clique em **Todos os outros** para ver e agendar esses scripts.

**Para agendar uma tarefa**

1. No painel de navegação esquerdo, clique em **Scripts**.
2. Clique para navegar para o grupo script.
3. Clique em um script e clique em **Agendar**.
4. Digite um nome para a tarefa e clique em **OK**.
5. Na guia **Tarefas de script personalizado**, clique em **Todas as tarefas**, clique na tarefa que nomeou na etapa 3 e clique em **Editar**.
6. Preencha as páginas da tarefa de script personalizado. Clique no botão Ajuda para ver a ajuda sobre qualquer página ou consulte a ajuda Agendador de tarefa.

Ao clicar em **Agendar**, é criada uma tarefa (ela não tem dispositivos alvo e é não agendada). Se você cancelar este procedimento de Tarefa agendada, lembre-se que a tarefa ainda foi criada e aparecerá na lista de Tarefas.

## Uso de scripts padrão

Este produto é vendido com dois scripts padrão. Você pode usá-los para ajudar a realizar algumas tarefas típicas. Esses scripts estão disponíveis na árvore **Todos os outros scripts** na janela **Scripts** (painel esquerdo de navegação **| Scripts**).

- **Varredura de inventário:** Executa a varredura de inventário nos dispositivos selecionados. Este script contém a documentação sobre como criar um arquivo de script; leia ou imprima este arquivo de script se precisar de mais informações sobre o uso correto de comandos e parâmetros.
- **Restaurar os registros do cliente:** Executa o analisador de inventário em dispositivos selecionados, mas o analisador reporta ao núcleo de onde o dispositivo foi configurado. Se tiver que reconfigurar o banco de dados, esta tarefa ajuda a adicionar dispositivos de volta ao banco de dados núcleo correto em ambiente com vários núcleos.

# Agendamento de tarefas


- Grupos de tarefas personalizadas
- Página Dispositivos alvo
- Página Agendar tarefa
- Página Scripts personalizados


**Tarefas agendadas** é uma configuração comum para a Configuração de agente, Atualização software, Scripts e Descoberta de dispositivos. As tarefas são filtradas no painel inferior das páginas de recurso específicas para mostrar apenas as tarefas relacionadas. Por exemplo, se você abrir a ferramenta **Descoberta de dispositivo**, as tarefas de descoberta serão mostradas na guia **Tarefas descobertas** no painel inferior. Todas as tarefas ainda são visíveis através da ferramenta **Tarefas agendadas**. Aqui é possível agendar configurações para serem executadas imediatamente no futuro, de forma recorrente ou serem executadas somente uma vez.

O painel esquerdo da página **Tarefas agendadas** mostra os seguintes grupos de tarefas:

- **Minhas tarefas:** As tarefas que você agendou. Somente você e os usuários administrativos podem ver essas tarefas.
- **Todas as tarefas:** Suas tarefas e as tarefas marcadas como públicas.
- **Tarefas comuns:** Tarefas que os usuários tenham marcado como comuns. Qualquer pessoa que editar ou agendar uma tarefa deste grupo, tornar-se-á o proprietária da tarefa. A tarefa permanecerá no grupo Tarefas comuns e também será visível no grupo Tarefas do usuário daquele usuário.
- **Tarefas do usuário** (Somente para usuários administrativos): Tarefas que os usuários criaram.

Quando você clica em **Minhas tarefas**, **Tarefas comuns** ou **Todas as tarefas**, o painel da direita mostra as seguintes informações:

- **Tarefa:** Mostra os nomes das tarefas.
- **Iniciar em:** Quando a tarefa está programada para execução. Clique no nome de uma tarefa e clique em **Editar** para editar a hora de início ou para reagendá-la.
- **Status:** Mostra o status geral da tarefa. Veja a coluna Status no painel da direita para mais detalhes. A coluna do painel direito mostra o status da tarefa, que pode ser: Trabalhando, 100% concluído, 0% concluído ou Com falha.
- **Pacote de distribuição:** O nome do pacote que a tarefa distribui. Este campo aplica-se à distribuição de software.
- **Método de entrega:** O método de entrega que a tarefa utiliza. Este campo aplica-se à distribuição de software.
- **Proprietário:** O nome da pessoa que originalmente criou o script que a tarefa está usando.

Quando você clica duas vezes em uma tarefa agendada, o painel da direita mostra as seguintes informações de resumo:

- **Nome:** O nome do estado da tarefa.
- **Quantidade:** O número de dispositivos em cada estado da tarefa.

- **Percentagem:** A porcentagem de dispositivos em cada estado da tarefa.

Antes de você poder agendar tarefas para um dispositivo, ele deve estar instalado no dispositivo, e o dispositivo deve estar no banco de dados do inventário. Configurações de servidores são uma exceção. Elas podem ser aplicadas a um dispositivo que não tenha o agente padrão de gerenciamento. As tarefas podem ser reagendadas (editadas) ou excluídas nas guias Tarefas. Após agendar uma tarefa, consulte a guia Tarefas para ver o status da tarefa.

Você pode editar uma tarefa selecionando aquela que quer editar e clicando **Editar**. A tarefa abre com opções de edição aplicáveis à tarefa.

## Grupos de tarefas personalizadas

Você pode criar grupos personalizados para os tipos de tarefa **Minhas tarefas**, **Todas as tarefas** e **Tarefas comuns**. Com os grupos personalizados, você pode agrupar tarefas relacionadas como, análise de vulnerabilidades e execução de um script. Os grupos e subgrupos podem ter 20 níveis.

**Para criar um grupo de tarefa personalizada**

1. No painel de navegação esquerdo, clique em **Tarefas agendadas**.
2. No painel esquerdo, clique no Tipo de tarefa no qual deseja criar o grupo.
3. Clique em **Novo grupo** na barra de ferramentas.
4. Digite um nome na caixa de texto **Nome do grupo** e clique em **OK**.

Após ter criado um grupo personalizado, você pode mover ou copiar tarefas ou outros grupos para o grupo selecionando-os de uma lista e clicando em **Mover** na barra de ferramentas.

## Sobre a página Dispositivos de destino

Use esta página para adicionar os dispositivos alvo para a tarefa que você está configurando. Você pode ver os dispositivos alvo, consultas e grupos de dispositivos para a tarefa nesta guia. Se tiver vários produtos de gerenciamento LANDesk instalados, os grupos de dispositivos criados em um console de produto podem ser vistos também em todos os consoles. Esta página não é necessária para as tarefas de descoberta.

- **Adição da lista alvo:** Adiciona os dispositivos previamente colocados na lista de alvos **Meus dispositivos**.
- **Adicionar consulta:** Define como alvo os resultados de uma consulta criada anteriormente.
- **Remover:** Remove os alvos selecionados.

Embora esta página mostre os grupos de dispositivos alvo, note que os grupos serão mostrados apenas se o LANDesk Management Suite estiver instalado no servidor núcleo. Se estiver executando Server Manager, System Manager ou o Web console no Management Suite, os grupos de dispositivos não serão selecionados como grupos alvo. Em vez disso, se selecionar um grupo e torná-lo alvo, os dispositivos individuais no grupo serão adicionados à lista de dispositivos alvo e serão mostrados em **Dispositivos alvo** em vez de **Grupos alvo**.

## Sobre a página Agendar tarefa

O Agendador contém a guia **Propriedades da tarefa agendada** que contém essas opções.

- **Deixar sem agendar**: (padrão) Deixa a tarefa na lista Tarefas para agendamento futuro.
- **Iniciar agora**: Executa a tarefa assim que possível. Pode levar até um minuto para a tarefa iniciar, dependendo de outra definição.
- **Iniciar na hora agendada**: Inicia a tarefa na hora em que você especificar. Se você clicar nessa opção, precisará digitar o seguinte:
  - **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.
  - **Hora**: A hora em que você deseja que a tarefa inicie.
  - **Repetir a cada**: Se quiser que a tarefa seja repetida, clique para repetição por **Hora**, **Dia**, **Semana** ou **Mês**. Se escolher **Mês** e a data não existir em todos os meses (por exemplo, 31), a tarefa só será executada nos meses que tiver esse dia.
- **Agendar estes dispositivos:** Na primeira vez que uma tarefa for executada, deixe o padrão como Aguardando ou atualmente funcionando. Para execuções subseqüentes, escolha entre Todos, Dispositivos que não tiveram êxito ou Dispositivos que não tentaram executar a tarefa. Essas opções são explicadas abaixo em maiores detalhes.
  - **Dispositivos que não tiveram êxito:** Selecione esta opção somente se quiser que a tarefa seja executada em todos os dispositivos que não completaram a tarefa da primeira vez. Isso exclui os dispositivos com o estado de Bem-sucedido. A tarefa será executada em dispositivos em todos os outros estados, inclusive Aguardando ou Ativo. Considere o uso desta opção se precisar executar a tarefa no maior número possível de dispositivos que falharam, mas só é necessário que a tarefa seja completada com êxito uma vez em cada dispositivo.
  - **Aguardando ou atualmente trabalhando:** Selecione esta opção se quiser que a tarefa seja executada em dispositivos que estão aguardando para serem processados ou estão sendo processados no momento.
  - **Todos:** Selecione esta opção se desejar que a tarefa seja executada em todos os dispositivos, independentemente do estado do dispositivo. Considere o uso desta opção se você tiver uma tarefa, especialmente uma tarefa repetitiva, que precisa ser executada no maior número de dispositivos possível.
  - **Dispositivos que não tentaram executar a tarefa:** Selecione esta opção somente se desejar que a tarefa seja executada em dispositivos que não completaram a tarefa e nos quais não houve falha da tarefa. Isso exclui dispositivos que estavam nos estados Desligado, Ocupado, Com falha ou Cancelado. Considere o uso desta opção se houver um grande número de dispositivos alvo nos quais a tarefa falhou, e que não são importantes como alvos.

## Sobre a página Scripts personalizados

- **Script personalizado selecionado no momento:** Selecione o script que quiser agendar.

# Relatórios

## Sobre relatórios

O System Manager inclui uma ferramenta de relatórios que pode ser usada para gerar uma grande variedade de relatórios especializados, que fornecem informações críticas sobre os dispositivos gerenciados na sua rede.

O System Manager usa um utilitário de análise ou varredura de inventário para adicionar dispositivos (e coletar dados de hardware e software sobre esses dispositivos) ao banco de dados do 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 relatórios aproveita as vantagens desses dados de análise de inventário através da coleta e organização desses dados em relatórios em formatos úteis.

Você pode usar os relatórios predefinidos de serviços e de recursos do inventário. Após executar um relatório, você pode vê-lo do console.

Se o Server Manager e o Management Suite estiverem instalados juntos, os relatórios executados no Server Manager incluirão somente servidores. Se for executada uma consulta, o resultado incluirá servidores e outros dispositivos, a não ser que a consulta tenha sido configurada para excluir outros dispositivos.

Se estiver fazendo um relatório de um computador específico que parece ter parado, você pode usar o restartmon.exe na pasta LDCLIENT para reiniciar o coletor e todo os provedores de monitoração. Esse utilitário é para computadores onde foi instalada a opção de relatório e essa função parou. Use esse utilitário para reiniciar o coletor e os provedores sem ter que reinicializar o dispositivo.

### Grupos de relatórios e relatórios predefinidos

Os relatórios são organizados em grupos na janela **Relatórios** (painel de navegação esquerdo **| Relatórios**). Os administradores podem ver o conteúdo de todos os grupos de relatórios. O System Manager inclui uma função específica denominada Relatórios, para permitir a outros verem relatórios sem dar-lhes acesso a outros recursos de gerenciamento. (Para ver mais informações, consulte "Uso da administração baseada em funções".) Os usuários com o direito Relatórios também podem ver e executar relatórios, mas apenas nos dispositivos que fazem parte do seu escopo.

A janela **Relatórios** tem os seguintes grupos de relatórios:

- Hardware
- Software

## Ver relatórios

Você pode executar qualquer relatório da janela **Relatórios**.

Na janela **Relatórios**, clique em um grupo de relatórios, em seguida, clique no relatório que desejar executar. Os dados do relatório são mostrados na **Tela do relatório**.

## Sobre a janela da tela do Relatório

Os relatórios permitem acessar rapidamente uma representação gráfica dos recursos nos computadores clientes. Os relatórios são criados de dados que a varredura armazena no banco de dados. Você pode ver ou imprimir relatórios usando o seu navegador.

**Para abrir um relatório**

1. No painel esquerdo de navegação, clique em **Relatórios**. As categorias de relatórios estão no painel direito. Clique no cabeçalho de uma categoria para ver a lista de relatórios. Há um ícone próximo a cada relatório que indica seu tipo.

    O relatório com um ícone de gráfico próximo é mostrado como gráfico de fatias ou de barras (bi ou tri-dimensional). Em um gráfico, clique em qualquer barra colorida ou em qualquer fatia para ir até o resumo.

    O relatório com um ícone de documento próximo é mostrado como texto.

2. Clique no nome do relatório para ver o relatório.
3. No caso de resumo de datas de análise de hardware ou de software, clique nas datas de início e de término para determinar o intervalo, em seguida clique em **Executar**.

O relatório Resumo de espaço no disco contém dados apenas para os dispositivos baseados em Windows.

Para imprimir um relatório, clique com o botão direito na página, em seguida clique em **Imprimir**. No diálogo Imprimir, clique em **Imprimir**. Caso um relatório tenha várias páginas, você deverá clicar com o botão direito em cada página para imprimi-la.

**Para distribuir um relatório**

- Para enviar um relatório por email, o método recomendado é converter o relatório em um arquivo .PDF e anexá-lo à mensagem de email.

---

O console mostra gráficos de relatórios como gráficos de fatias ou de barras. Para definir o tipo de gráfico, clique na lista suspensa no gráfico de relatório e mude o tipo.

Para poder ver os tipos de gráficos interativos de barra e de fatias, mostrado em muitos dos relatórios, é necessária ter instalado o Macromedia Flash Player* 7.

# Consultas

## Utilização de consultas

Consultas são pesquisas personalizadas aos bancos de dados núcleo.  Este produto fornece ferramentas que permitem criar consultas de banco de dados para dispositivos localizados no seu banco de dados núcleo Você cria consultas de banco de dados núcleo na tela **Consultar** do console. As consultas públicas de System Manager são visíveis em LANDesk® Management Suite e vice-versa, forem se ambos forem usados.

Leia esta seção para obter informações sobre:

- Visão geral das consultas
- Grupos de consultas
- Criação de consultas ao banco de dados
- Execução de consultas
- Importação e exportação de consultas

### Visão geral das consultas

As consultas ajudam a gerenciar a rede, permitindo que você pesquise e organize os dispositivos no banco de dados núcleo, com base em critérios específicos do sistema ou do usuário.

Por exemplo, você pode criar e executar uma consulta que capture somente dispositivos com uma velocidade do clock do processador menor do que 166 MHz ou com menos de 64 MB de RAM ou, então, com uma unidade de disco rígido de menos de 2 GB. Crie uma ou mais instruções de consultas que representem essas condições e relacione as instruções umas às outras usando operadores lógicos padrão. Quando as consultas são executadas, é possível imprimir os resultados e acessar e gerenciar os dispositivos correspondentes.

### Grupos de consulta

Consultas podem ser associadas a grupos na tela **Meus dispositivos**. Esses grupos são chamados de grupos dinâmicos, e o conteúdo de um grupo dinâmico é o resultado da consulta associada àquele grupo dinâmico. Por exemplo, um grupo que contém todos os dispositivos em uma área geográfica pode ser associado a uma consulta da memória, do tamanho do disco rígido, etc.

Para mais informações sobre como executar consultas em grupos e exibir as consultas na tela **Todos os dispositivos**, e sobre o que você pode fazer com elas, consulte "Como agrupar dispositivos para ações".

### Criação de consultas no banco de dados

Use o diálogo **Nova consulta** para criar uma consulta selecionando entre atributos, operadores relacionais e valores de atributos. Compile uma instrução de consulta escolhendo um atributo de inventário e relacionando-o a um valor aceitável. Relacione logicamente as instruções de

consultas umas às outras para garantir que sejam avaliadas como um grupo, antes de relacioná-las a outras instruções ou a outros grupos.

**Para criar uma consulta ao banco de dados**

1. Na tela do console **Consultas** , clique em **Nova**.
2. Na lista de atributos de inventário, selecione um **componente**.
3. Na **Etapa 1: Critério de pesquisa**, clique em **Editar**.
    1. Percorra essa lista a fim de selecionar os atributos que constituirão seu critério de pesquisa. Por exemplo, para localizar todos os clientes que executam um determinado tipo de software, você deve selecionar Computer.Software.Package.Name.
    2. Depois de selecionar os atributos, você verá uma série de campos no lado direito da janela. Nesses campos, selecione um operador e um valor para completar um critério de pesquisa. Por exemplo, para localizar todos os clientes que executam o Internet Explorer 5.0, os atributos seriam "Computer.Software.Package.Name, "o operador "=" e o valor "Internet Explorer 5".
    3. Na parte inferior da janela, clique em **Adicionar** para preencher o campo vazio com seu critério de pesquisa.
    4. Você pode continuar a refinar a consulta criando outro critério de pesquisa e, em seguida, adicionando-o ao primeiro critério com um operador booleano (AND ou OR). Você também pode usar os botões para adicionar, excluir, substituir, agrupar ou desagrupar os critérios criados.
    5. Ao concluir, clique em **OK**.
4. Na **Etapa 2: Atributos a serem mostrados**, clique em **Editar**.
    1. Percorra essa lista a fim de selecionar um atributo a ser mostrado na lista de resultados da consulta. Lembre-se de selecionar atributos que ajudarão a identificar os clientes retornados na consulta. Se não conseguir encontrar atributos que deseja exibir, você pode adicioná-los no diálogo Atributos personalizados. Entretanto, esses atributos devem ser atribuídos a máquinas antes que elas apareçam no diálogo.

    2. Após selecionar um atributo, clique em **Adicionar** para transferi-lo para o campo vazio na base da janela. Se desejar enumerar a lista de resultados da consulta, clique em **Incluir número**.
    3. Repita o processo se quiser adicionar mais atributos. Use o botão **Remover** para remover atributos e clique em **Mover para cima/Mover para baixo** para mudar a ordem dos atributos.
    4. Clique em **Tornar os resultados selecionáveis** para habilitar os resultados da consulta a serem selecionáveis para qualquer ação que você especificar.
    5. Ao concluir, clique em **OK**.
5. (opcional) Na **Etapa 3: Ordenação dos resultados por atributo**, clique em **Editar** para personalizar a ordem dos resultados da consulta.
6. Se quiser executar a consulta mais vezes, clique em **Salvar consulta** e insira um nome exclusivo para a consulta. Se você executar a consulta antes de salvá-la, seus parâmetros serão perdidos e precisarão ser reconstruídos para executar a mesma consulta novamente.
7. Na **Etapa 4: Execução da consulta**, clique em **Executar consulta**.

**Instruções de consultas são executadas na ordem mostrada.**
Se nenhum agrupamento for feito, as instruções de consultas listadas nesta caixa de diálogo

serão executadas de baixo para cima. Agrupe itens de consultas relacionadas para que elas sejam avaliadas como um grupo. Caso contrário, os resultados de sua consulta podem ser diferentes do esperado.

## Execução de consultas

**Para executar uma consulta**

1. No painel esquerdo de navegação, clique em **Consultas**.
2. Selecione a consulta e clique em **Executar**.

   ou

   Para fazer modificações em uma consulta antes de executá-la, clique duas vezes em **Editar**, modifique as etapas de 1 a 3 e clique em **Executar consulta**.

   **Nota**: Se você modificou a consulta e quer salvar as mudanças, clique em **Salvar a consulta** para salvar as modificações ou em **Salvar consulta como** para dar um novo nome à consulta modificada. Isso deve ser feito antes de executar a consulta. Se você não salvar suas mudanças antes de executar a consulta, as mudanças não serão salvas com a consulta.

3. Os resultados (dispositivos correspondentes) aparecem no painel direito da tela **Todos os dispositivos**.

## Importação e exportação de consultas

Você pode usar Importar e Exportar para transferir consultas de um banco de dados núcleo para outro. As consultas exportadas são arquivadas no formato de arquivo XML.

**Para importar uma consulta**

1. Clique com o botão direito do mouse no grupo de consultas em que você deseja colocar a consulta importada.
2. No menu de atalhos, selecione **Importar**.
3. Navegue até a consulta a ser importada e selecione-a.
4. Clique em **Abrir** para adicionar a consulta ao grupo de consultas selecionado na tela **Todos os dispositivos**.

**Para exportar uma consulta**

1. Clique com o botão direito do mouse na consulta a ser exportada.
2. No menu de atalhos, selecione **Exportar**.
3. Navegue até o local em que deseja salvar a consulta (como um arquivo .XML).
4. Digite um nome para a consulta.
5. Clique em **Salvar** para exportar a consulta.

# Consultas personalizadas

As consultas personalizadas são úteis quando você deseja detalhes do inventário sobre o hardware e o software instalados nos dispositivos. Use uma consulta personalizada para criar uma lista de computadores com inventário semelhante. Consultas personalizadas também são utilizadas para definir grupos e escopos.

A página **Consultas personalizadas** (clique em **Consultas** no painel de navegação à esquerda) mostra uma lista das consultas salvas. Para executar uma consulta salva, selecione a consulta, em seguida, selecione **Executar**.

Se a lista de consultas ocupar várias páginas, use as setas no topo da página para navegar entre elas. Digite o número de itens para mostrar por página e clique em **Definir**.

# Criação de consultas personalizadas

As consultas personalizadas são úteis quando você deseja detalhes do inventário sobre o hardware e o software instalados nos dispositivos. Use uma consulta personalizada para criar uma lista de dispositivos com inventários semelhantes. Por exemplo, se quiser atualizar todos os dispositivo para um processador de pelo menos 750 MHz, você pode consultar todos os dispositivos no banco de dados com velocidades de processador menores do que 750 MHz. Consultas personalizadas também são utilizadas para definir grupos e escopos.

Você pode consultar qualquer dos itens do inventário (conhecidos como "atributos") que a análise de inventário armazena no banco de dados, e também quaisquer atributos personalizados.

## Gerenciamento de consultas

Gerencie consultas na tela **Consultas**. Use esta tela para criar, editar ou excluir consultas:

- Para executar uma consulta existente, selecione-a e clique em **Executar**.
- Para criar uma nova consulta, clique em **Nova**. Depois que a consulta for criada e salva, seu nome aparecerá na lista dessa página.
- Para editar uma consulta na lista, clique duas vezes no nome da consulta. A página **Editar consulta** aparece com os parâmetros da consulta que você pode editar.
- Para editar a consulta mais recente, clique em **Editar a consulta atual**.
- Para excluir uma consulta, selecione-a e clique em **Excluir**.

A criação de uma consulta é um processo de quatro etapas:

1. **Criar uma condição de pesquisa:** Especifique um conjunto de atributos de inventário que será a base de sua consulta.
2. **Selecionar os atributos a serem mostrados:**Refine ainda mais ou "filtre" a consulta, de modo que os resultados exibam os atributos mais úteis, como os endereços IP ou os nomes dos dispositivos do computador.
3. **Ordenar os resultados por atributos (opcional):** Especifique como deseja ordenar os resultados da consulta. (Aplicável somente se, na Etapa 2, for selecionado para exibir um ou mais tipos de atributos nos resultados da consulta.)

4. **Executar a consulta:** Execute a consulta que você acabou de criar. Também é possível salvar a consulta para uso futuro ou eliminar todas as informações da consulta para começar novamente.

# Etapa 1: Criação de um critério de pesquisa (obrigatório)

Um critério de pesquisa é um conjunto de atributos de inventário e valores associados utilizado em uma consulta. Você pode usar um critério de pesquisa ou agrupar vários critérios para formar a base de uma consulta.

As etapas a seguir são executadas na página **Editar consulta**. Na tela **Executar consultas**, clique em **Nova**, ou selecione uma consulta existente e clique em **Editar**.

**Para criar um critério de pesquisa:**

1. Na **Etapa 1**, clique em **Editar**. Aparece uma janela mostrando uma lista que representa todos os dados de inventário armazenados no banco de dados no momento.
2. Percorra essa lista a fim de selecionar os atributos que constituirão seu critério de pesquisa. Por exemplo, para localizar todos os clientes que executam um determinado tipo de software, você deve selecionar Computer.Software.Package.Name.
3. Depois de selecionar os atributos, você verá uma série de campos no lado direito da janela. Nesses campos, selecione um operador e um valor para completar um critério de pesquisa. Por exemplo, para localizar todos os clientes que executam o Internet Explorer 5.0, os atributos seriam "Computer.Software.Package.Name, "o operador "=" e o valor "Internet Explorer 5".
4. Na parte inferior da janela, clique em **Adicionar** para preencher o campo vazio com seu critério de pesquisa.
5. Você pode continuar a refinar a consulta criando outro critério de pesquisa e, em seguida, adicionando-o ao primeiro critério com um operador booleano (AND ou OR). Você também pode usar os botões para adicionar, excluir, substituir, agrupar ou desagrupar os critérios criados.
6. Ao concluir, clique em **OK**.

Para executar e armazenar uma consulta sobre o status de funcionamento de servidores (Computer.Health.State), é preciso estar alerta para o fato de que o estado no banco de dados é representado por um número. Use a tabela abaixo para criar condições de busca. Por exemplo, para criar uma condição de busca para computadores com  estado de funcionamento “Desconhecido”, use o operador “NOT EXIST”.

| Condição de funcionamento | Operador |
|---|---|
| Desconhecido | NOT EXIST |
| Normal | 2 |

| Condição de funcionamento | Operador |
|---|---|
| Aviso | 3 |
| Crítico | 4 |

# Etapa 2: Seleção dos atributos a serem mostrados (obrigatório)

Para a Etapa 2, selecione os atributos que serão úteis para identificar os computadores incluídos nos resultados da consulta. Por exemplo, se quiser resultados que o ajudem a localizar fisicamente cada computador correspondente ao critério de pesquisa definido na Etapa 1, especifique atributos como, o nome de exibição de cada computador (Computer.DisplayName) ou endereço IP (Computer.Network.TCPIP.Address).

As etapas a seguir são executadas na página **Editar consulta**.

**Para selecionar os atributos a serem mostrados:**

1. Na **Etapa 2**, clique em **Editar**. Aparece uma janela mostrando uma lista que representa todos os dados de inventário armazenados no banco de dados no momento.
2. Percorra essa lista a fim de selecionar um atributo a ser mostrado na lista de resultados da consulta. Lembre-se de selecionar atributos que ajudarão a identificar os clientes retornados na consulta. Se não conseguir encontrar atributos que deseja exibir, você pode adicioná-los no diálogo Atributos personalizados. Entretanto, esses atributos devem ser atribuídos a máquinas antes que elas apareçam no diálogo.

   **Nota:** Se estiver usando um banco de dados Oracle, selecione pelo menos um atributo definido nativamente pela análise de inventário (por exemplo, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, etc.).

3. Após selecionar um atributo, clique em **>>** para transferi-lo para o campo vazio no lado direito da janela. Se desejar enumerar a lista de resultados da consulta, clique em **Incluir número**.
4. Repita o processo se quiser adicionar mais atributos. Use os botões de setas para adicionar ou remover atributos e clique em **Mover para cima/Mover para baixo** para mudar a ordem dos atributos.
5. Clique em **Tornar os resultados selecionáveis** para habilitar os resultados da consulta a serem selecionáveis para qualquer ação que você especificar.
6. Ao concluir, clique em **OK**.

Você também pode adicionar cabeçalhos de colunas à lista de resultados da consulta.

**Para mudar cabeçalhos de colunas (opcional)**

1. Na **Etapa 2**, clique em **Editar**.

2. Na caixa inferior, clique num cabeçalho de coluna e clique em **Editar**. Edite o cabeçalho e pressione **Enter**. Repita o procedimento, se necessário.
3. Clique em **OK**.

Nesse ponto, é recomendável salvar a consulta; o procedimento a seguir no processo de criação de consulta é opcional e aplica-se somente aos resultados da consulta que contenham duas ou mais colunas. Para salvar a consulta, clique em **Salvar consulta** na parte superior da página. Aparecerá uma janela solicitando um nome para essa consulta. Digite um nome e, em seguida, clique em **Salvar** no canto superior direito da janela.

# Etapa 3: Ordenação de resultados por atributos (opcional):

Este procedimento será necessário somente se você definiu mais de um atributo e cabeçalho de coluna na Etapa 2 e agora deseja ordenar os resultados por ordem alfabética ou numérica dentro de uma dessas colunas.

Por exemplo, suponhamos que tenham sido especificados dois atributos diferentes para serem exibidos nos resultados da consulta: o endereço IP e o tipo de processador de cada computador retornado. Na Etapa 3, é possível ordenar os resultados por ordem alfabética pelo tipo de processador.

Caso você pule essa etapa, a consulta será ordenada automaticamente pelo primeiro atributo selecionado na Etapa 2.

**Para ordenar os resultados por atributo**

1. Na **Etapa 3**, clique em **Editar**. É exibida uma janela mostrando os atributos que foram selecionados na **Etapa 2**.
2. Selecione o atributo pelo qual deseja classificar e clique em **>>** para mudá-lo para a caixa de texto vazia.
3. Clique em **OK**.

# Etapa 4: Execução da consulta

Depois de criar sua consulta, ela poderá ser executada, salva ou limpa para iniciar novamente.

Para salvar a consulta para uso futuro, clique no botão **Salvar**da barra de ferramentas. A consulta aparece agora na lista da página **Consultas personalizadas**. Caso sua consulta seja uma versão modificada de outra, clique no botão **Salvar como** da barra de ferramentas para dar-lhe um novo nome.

Por padrão, as consultas salvas só podem ser visualizadas pela pessoa que as salvou. Caso seja marcada a opção **Consulta pública** antes de salvar, a consulta salva será visível a todos os usuários. Somente administradores com o direito Gerenciamento de consultas públicas pode tornar pública uma consulta.

Se tiver produtos de várias famílias intalados, as consultas serão compartilhadas por esse produtos. Se você salvar uma consulta em um console de produto, ela também será visível em outros consoles de produto.

Para ver os resultados dessa consulta, clique no botão **Executar** na barra de ferramentas.

Para limpar os parâmetros da consulta da página **Editar consulta**, clique no botão **Limpar** na barra de ferramentas. Caso a consulta já tenha sido salva, ela será limpa dessa página, mas permanecerá na lista **Consultas personalizadas**.

# Como ver os resultados da consulta

Os resultados correspondem aos critérios de pesquisa que foram especificados no processo de criação da consulta. Se os resultados não forem os esperados, retorne à página **Editar consulta** e refine as informações.

Para encontrar mais informações sobre um dos dispositivos na lista de resultados da consulta, clique duas vezes nos dados da consulta, ou clique com o botão direito e clique em **Visualizar computador** no menu que aparece.

Na página **Resultados da consulta**, clique no botão da barra de ferramentas **Salvar como CSV**para exportar os resultados em um formato compatível com uma planilha ou outro aplicativo.

Para imprimir os resultados da pesquisa, clique em **Imprimir tela** na página de resultados da pesquisa.

# Como ver os resultados de consulta da pesquisa

Os resultados correspondem aos critérios de pesquisa que foram especificados no processo de criação da consulta. Se os resultados não forem os esperados, retorne à página **Editar consulta** e refine as informações.

Para encontrar mais informações sobre um dos dispositivos na lista de resultados da consulta, clique duas vezes nos dados da consulta, ou clique com o botão direito e clique em **Visualizar computador** no menu que aparece.

# Exportação de resultados de consultas para arquivos CSV

Para ver os dados do resultado de sua consulta em uma planilha, exporte-os como um arquivo de valores separados por vírgulas (CSV). Na página **Resultados da consulta**, clique no ícone da barra de ferramentas **Salvar como CSV** para salvar suas informações como um arquivo CSV. Você pode usar um aplicativo como o Microsoft Excel* para importar e trabalhar com o arquivo CSV.

# Mudança dos cabeçalhos de colunas da consulta

1. Abra uma consulta existente ou crie uma nova consulta.
2. Na caixa inferior, clique num cabeçalho de coluna e clique em **Editar**. Edite o cabeçalho e pressione **Enter**. Repita o procedimento, se necessário.
3. Clique em **OK**.

# Exportação e importação de consultas

Você pode exportar e importar quaisquer consultas que criar. Todas as consultas são exportadas como arquivos XML. Se você exportar o mesmo nome de arquivo de consulta mais de uma vez, o arquivo existente será substituído. Para evitar isso, você deve copiar o arquivo para outro local ao exportá-lo.

Os recursos exportar e importar são úteis em duas situações:

- Se for necessário reinstalar seu banco de dados, use os recursos exportar/importar para salvar as consultas existentes a fim de serem usadas em um novo banco de dados.

  Por exemplo, é possível exportar as consultas e mudá-las para um diretório não afetado pela reinstalação de um banco de dados. Após reinstalar o banco de dados, é possível mover as consultas novamente para o diretório de consultas no seu servidor web e importá-las para seu novo banco de dados.
- Você pode usar os recursos de exportar/importar para copiar consultas para outros bancos de dados.

  Por exemplo, você pode exportar uma consulta para um diretório de consultas no seu servidor de web e, depois, enviá-la para alguém por email ou FTP. Essa pessoa poderia colocar as consultas no diretório de consultas em outro servidor Web e importá-las para um banco de dados diferente. Também é possível mapear uma unidade e copiar as consultas diretamente para o diretório de consultas em outro servidor de web.

**Para exportar uma consulta**

Conclua essas etapas ainda conectado a um banco de dados que tenha uma consulta que você quer exportar.

1. No painel esquerdo de navegação, clique em **Consultas**.
2. Na página **Consultas personalizadas**, clique no nome da consulta a ser exportada. Clique em **Editar**.
3. Na página **Editar consulta**, clique no botão **Exportar** na barra de ferramentas para exportar a consulta para disco.
4. Na página **Consulta exportada**, clique com o botão direito na consulta para baixá-la como um arquivo XML para um diretório selecionado. A consulta torna-se um arquivo XML.

Observe que se exportar o mesmo nome de arquivo de consulta mais de uma vez, o arquivo existente será substituído. Para evitar isso, você deve copiar o arquivo para outro local ao exportá-lo.

Se você quiser importar a consulta novamente para um banco de dados, ela deverá ser movida para o diretório de consultas reconhecido pelo servidor de web, por padrão c:\inetpub\wwwroot\LANDesk\LDSM\queries.

**Para importar uma consulta**

Execute estas etapas ainda conectado a um banco de dados para o qual deseja importar uma consulta.

1. No painel esquerdo de navegação, clique em **Consultas**.
2. Na página **Consultas personalizadas**, clique em **Nova**.
3. Na página **Editar consulta**, clique no botão **Importar**da barra de ferramentas.
4. Selecione a consulta a ser importada. Se quiser verificar os parâmetros dessa consulta antes de importá-la, clique em **Exibir**.
5. Clique em **Importar** para carregar a consulta na página **Editar consulta**.
6. Quando a consulta for carregada, role a tela para baixo e clique em **Salvar consulta** para salvá-la nesse banco de dados.

# Gerenciamento de inventário

## Gerenciar inventários

Você pode usar o utilitário de análise de inventário para adicionar dispositivos ao banco de dados núcleo e para coletar dados de hardware e software dos dispositivos. Você pode ver, imprimir e exportar os dados de inventário. Também é possível usá-lo para definir consultas, agrupar dispositivos e gerar relatórios especializados.

Leia esta seção para obter informações sobre:

- Visão geral da análise de inventário
- Como ver dados de inventário

## Visão geral da análise de inventário

Ao configurar um dispositivo com o recurso de configuração de dispositivos, o analisador de inventário é um dos componentes que são instalados. Ao criar a configuração de um cliente, você pode especificar quando a varredura de inventário será executada no dispositivo.

A varredura de inventário é automaticamente executada quando o dispositivo é inicialmente configurado. O executável do analisador se chama LDISCAN32.EXE para o Windows e LDISCAN para o Linux. A análise de inventário 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. Para configurar as configurações de análise de software, no servidor núcleo, clique em **Iniciar | Arquivos de programas | LANDesk | LANDesk Configurar serviços**.

Para mais informações sobre a configuração do serviço do inventário, consulte "Configuração do serviço de inventário", no Apêndice C.

Após a análise inicial, a análise de inventário pode ser executada do console como uma tarefa agendada. O agente de gerenciamento padrão deve estar em execução nos dispositivos remotos para se poder agendar uma análise de inventário neles.

**Nota:** Um dispositivo adicionado ao banco de dados núcleo, usando o recurso descoberta ainda não terá analisado seus dados de inventário no banco de dados núcleo. É preciso executar uma varredura de inventário em cada dispositivo para que todos os dados de inventário sejam exibidos para esse dispositivo.

Você pode ver os dados de inventário e usá-los para:

- Personalizar as colunas da lista **Todos os dispositivos** para mostrar atributos de inventário específicos
- Consultar o banco de dados núcleo quanto a servidores com atributos de inventário específicos
- Agrupar dispositivos para acelerar tarefas de gerenciamento,

- Gerar relatórios especializados com base nos atributos de inventário
- Manter o controle das mudanças de hardware e software nos dispositivos e gerar alertas ou entradas no arquivo de log quando essas mudanças ocorrerem.

Leia as seções a seguir para aprender mais sobre como funciona a análise de inventário.

## Análise delta

Depois que a análise completa inicial é executada em um dispositivo, uma execução subseqüente da análise de inventário captura apenas as modificação delta e as envia ao banco de dados núcleo. Use a opção do analisador /RSS para coletar informações de software no registro do Windows.

## Como forçar uma análise completa

Se quiser forçar uma análise completa dos dados de hardware e software do dispositivo, você pode apagar o arquivo delta de análise atual e mudar um parâmetro no miniaplicativo **Configurar serviços de software LANDesk**.

1. Apague o arquivo **invdelta.dat** do servidor. Há uma cópia da última análise de inventário armazenada localmente como arquivo oculto denominado invdelta.dat na raiz no disco rígido. (A variável de ambiente LDMS_LOCAL_DIR define o local desse arquivo.)
2. Adicione a opção **/sync** à linha de comandos do utilitário de análise de inventário. Para editar a linha de comandos, clique em **Iniciar | Todos os programas | LANDesk Management**, clique com o botão direito no ícone de atalho **Análise de inventário**, selecione **Propriedades | Atalho** e, em seguida, edite o caminho **Alvo**.
3. No servidor núcleo, clique em **Iniciar | Todos os programas | LANDesk | Configurar serviços LANDesk**
4. Clique na guia **Inventário** e clique em **Configurações avançadas**.
5. Clique no parâmetro **Do Delta** (Executar Delta). Digite **0** na caixa **Valor**.
6. Clique em **OK** duas vezes e clique em **Sim** ao ser avisado para reiniciar o serviço.

## Compactação da análise

As análises de inventário executadas pela análise de inventário do Windows (LDISCAN32.EXE) são compactadas por padrão. A análise compacta as análises completas e delta com uma taxa de compactação de aproximadamente 8:1. Em primeiro lugar, as análises são compiladas totalmente na memória, em seguida, são compactadas e enviadas ao servidor núcleo usando um tamanho de pacote maior. A compactação da análise requer menos pacotes e reduz o uso da largura de banda.

## Criptografia da análise

As análises de inventário são criptografadas (apenas as análises TCP/IP). Você pode desativar a criptografia de análise de inventário mudando um parâmetro no miniaplicativo Configurar serviços LANDesk.

1. No servidor núcleo, clique em **Iniciar | Todos os programas | LANDesk | Configurar serviços LANDesk**
2. Clique na guia **Inventário** e clique em **Configurações avançadas**.
3. Clique no parâmetro **Disable Encryption**. Digite **1** na caixa **Valor**.
4. Clique em **Definir**, em seguida clique em **OK**.
5. Clique em **OK** duas vezes e clique em **Sim** ao ser avisado para reiniciar o serviço.

# Como ver os dados de inventário

Quando um dispositivo é analisado pela análise de inventário, é possível ver suas informações de sistema no console.

Os inventários do dispositivo são armazenados no banco de dados núcleo e incluem as informações de hardware, driver de dispositivo, software, memória e ambiente. É possível usar o inventário para ajudar a gerenciar e configurar dispositivos e rapidamente identificar problemas no sistema.

Você pode ver os dados de inventário das seguintes maneiras:

- Resumo de inventário
- Inventário completo
- Como ver propriedades de atributos
- Informações do sistema

Também é possível ver os dados de inventário em relatórios que você gera. Para ver mais informações, consulte "Visão geral dos relatórios".

## Ver o resumo de inventário do console de informações do servidor

O resumo de inventário é encontrado na página de **Resumo** no console de informações do servidor e fornece uma vista rápida da configuração básica de SO e das informações de sistema do dispositivo.

**Nota:** Se você adicionou um dispositivo ao banco de dados núcleo usando a ferramenta de descoberta, seus dados de inventário ainda não terão sido analisados no banco de dados núcleo. É preciso executar uma análise de inventário no servidor para que o recurso Resumo de inventário seja completado com êxito.

**Para ver o resumo de inventário**

1. Na tela **Todos os dispositivos** do console, clique duas vezes em um dispositivo.
2. No painel esquerdo, clique em **Informações do sistema**, em seguida clique em **Resumo do sistema**.

## Dados de resumo de servidores Windows 2000/2003

Essas informações aparecem quando você vê o resumo de inventário de um servidor Windows 2000/2003.

- **Funcionamento:** O estado do funcionamento atual do servidor.
- **Tipo:** O tipo de servidor, por exemplo, de aplicativo, de arquivos, de email, etc.
- **Fabricante:** O fabricante do servidor.
- **Modelo:** O tipo do modelo do servidor.
- **Versão do BIOS:** A versão do BIOS da ROM.
- **Sistema operacional:** SO Windows ou Linux em execução no servidor: Red Hat.
- **Versão do SO:** Número da versão do SO do Windows 2000/2003 em execução no servidor.
- **CPU:** O tipo do processador ou processadores em execução no servidor.
- **Analisador de vulnerabilidades:** A versão do agente instalado.
- **Varredura de inventário:** A versão do agente instalado.
- **Monitoração:** A versão do analisador de monitoração instalado.
- **Última inicialização:**A data e o horário da última vez em que o servidor foi reinicializado.
- **Uso da CPU:** Porcentagem atual em uso do processador.
- **Memória física utilizada:** Quantidade de RAM disponível no servidor.
- **Memória virtual utilizada:** Quantidade de memória disponível para o servidor, incluindo a RAM e a memória do arquivo de troca.
- **Espaço usado da unidade:** Porcentagem de espaço da unidade em uso no momento. Se houver mais de uma unidade de disco, todas as unidades serão mostradas.

Os servidores habilitados para IPMI mostrarão dados adicionais específicos do IPMI. Servidores Linux também mostram informações semelhantes na tela do **Resumo**.

## Como ver um inventário completo

Um inventário completo fornece uma listagem completa dos componentes de hardware e software detalhados de um dispositivo. A lista contém objetos e atributos de objetos.

**Para ver um inventário completo**

1. Na tela **Todos os dispositivos** do console, clique em um dispositivo.
2. Na guia **Propriedade**, clique em **Ver inventário**.

## Como ver propriedades de atributos

É possível visualizar as propriedades de atributo dos objetos Inventário de um dispositivo na listagem de inventários. As propriedades de atributo informam as características e os valores de um objeto do inventário. Também é possível criar novos atributos personalizados e editar os atributos definidos pelo usuário.

Para ver as propriedades de um atributo, clique no atributo no painel esquerdo.

Para imprimir essas informações no Internet Explorer, clique com o botão direito no quadro e clique em **Imprimir**. Para imprimir no Mozilla, clique com o botão direito no quadro, clique em

**Este quadro | Salvar quadro como**, clique em **Salvar**, em seguida abra o arquivo em um aplicativo e clique em **Imprimir**.

## Informações do sistema

No console de informações do servidor, você pode ver e modificar as informações de sistema do dispositivo. As informações nas categorias **Hardware**, **Software**, **Logs** e **Outros** são dados armazenados ou dados em tempo real. Quando clica em um link de informações, você pode ver informações detalhadas sobre o componente selecionado e, quando apropriado, definir limites e inserir informações.

1. Na tela **Todos os dispositivos** do console, clique duas vezes em um dispositivo.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Informações do sistema**.
3. Expanda o grupo e clique no link das informações que deseja ver.

# Opções de personalização de inventário

O console inclui o utilitário o Configurar serviços, que você pode utilizar para personalizar opções de inventário. Os padrões da maioria das opções deve ser OK, mas se precisar mudá-los, use esse utilitário. Para abrir o miniaplicativo Configurar serviços, no servidor núcleo, clique em **Iniciar | Arquivos de programas | LANDesk | LANDesk Configurar Serviços**. (O nome de arquivo deste utilitário é svccfg.exe.)

Use o utilitário Configurar serviços para configurar:

- o nome da base de dados, o nome do usuário e a senha;
- o intervalo de varredura do software do dispositivo, a manutenção, os dias para realizar varreduras do inventário e o histórico do tempo de duração em que o cliente esteve registrado;
- o tratamento dos IDs de dispositivos duplicados;
- a definição do planejador, incluindo intervalos de avaliação de tarefas e consultas agendadas
- a definição das tarefas personalizadas, incluindo o tempo limite de uma execução remota

Clique em **Ajuda** em cada guia do utilitário Configurar serviços para ver mais informações.

# Editar o arquivo LDAPPL3.TEMPLATE

Informações relacionadas especificamente aos parâmetros de inventário da varredura contidas no arquivo LDAPPL3.TEMPLATE. Esse arquivo modelo trabalha com o arquivo LDAPPL3 para identificar o inventário de software de um dispositivo. Este arquivo é colocado em dispositivos gerenciados Windows como parte da configuração de agente. Seus parâmetros são configurados na guia Inventário da Configuração de agente.

Nos dispositivos Linux, um arquivo de configuração parecido (/etc/ldappl.conf) contém informações sobre os parâmetros do analisador. Você pode editar este arquivo para mudar a operação do analisador. O arquivo contém instruções de como modificar a operação do analisador Linux.

É possível editar a seção [LANDesk Inventory] do arquivo modelo para configurar os parâmetros que determinam como a varredura identifica o inventário de software. Como padrão o LDAPPL3.TEMPLATE está localizado no compartilhamento LDLogon do servidor núcleo.

Use a tabela a seguir como guia para ajudar a editar a seção [LANDeskInventory] em um editor de texto.

| Opção | Descrição |
|---|---|
| Modo | Determina como a varredura analisa o software nos dispositivos. O padrão é Listed. As configurações são as seguintes:<br><br>• **Listed:** Registra os arquivos listados em LDAPPL3.<br>• **Unlisted:** Registra os nomes e as datas de todos os arquivos com as extensões listadas na linha ScanExtensions, mas não definidas no LDAPPL3. Esse modo ajuda a descobrir o software não autorizado na rede.<br>• **Todos:** Localiza arquivos listados e não listados. |
| Duplicate | Registra instâncias múltiplas de arquivos. Defina o valor como OFF para registrar apenas a primeira instância ou como ON para registrar todas as instâncias detectadas. O padrão é ON. |
| ScanExtensions | Define as extensões dos arquivos (.EXE, .COM, .CFG, etc.) a serem analisados. Use um espaço para separar as extensões de arquivos. Por padrão, apenas arquivos .EXEs são analisados. |
| Version | O número da versão do arquivo LDAPPL3. |
| Revisão | O número de revisão do arquivo LDAPPL3; ajuda a garantir a compatibilidade futura. |
| CfgFiles 1-4 | Registra a data, a hora, o tamanho e o conteúdo dos arquivos especificados. É possível omitir a letra da unidade (por exemplo, c:), se quiser pesquisar todas as unidades locais. É possível especificar mais de um arquivo em cada uma das quatro linhas, mas o tamanho da linha é limitado a 80 caracteres.<br><br>Separe por um espaço os nomes dos caminhos contidos na mesma linha.<br><br>A análise compara a data e o tamanho do arquivo atual com o arquivo analisado anteriormente. Se a data e o tamanho forem diferentes, a análise registrará o conteúdo do arquivo como uma nova revisão. |

| Opção | Descrição |
|---|---|
| ExcludeDir 1-3 | Exclui os diretórios específicos de uma análise. É possível omitir a letra da unidade (por exemplo, c:), se quiser excluir todas as unidades locais. A enumeração deve começar no 1 e ser contínua. Cada linha deve terminar com "\". |
| MifPath | Especifica o local no qual os arquivos MIF estão armazenados em uma unidade local do cliente. O local padrão é c:\DMI\DOS\MIFS. |
| UseDefaultVersion | Se definido como TRUE, a varredura reportará uma correspondência quando um arquivo corresponder a uma entrada exata de nome e tamanho do arquivo LDAPPL3 somente no nome do arquivo (a versão será reportada como EXISTS). Isso pode causar alguns falsos positivos para aplicativos que compartilham um nome de arquivo comum com um aplicativo desconhecido. No arquivo original LDAPPL3.TEMPLATE, esse parâmetro é definido como FALSE; ou seja, uma entrada será adicionada apenas se a correspondência for exata. Se o parâmetro não estiver presente, ele assumirá TRUE como padrão. |
| SendExtraFileData | Se definido como TRUE, envia dados adicionais do arquivo para o servidor núcleo. O padrão é FALSE. Isso significa que, por padrão, apenas o caminho, o nome e a versão serão inseridos no banco de dados núcleo. |

**Para editar o arquivo LDAPPL3.TEMPLATE:**

1. No servidor núcleo, vá para o diretório \Arquivos de programas\LANDesk\ManagementSuite\LDLogon e abra o LDAPPL3.TEMPLATE em Notepad ou outro editor de texto.
2. Role para baixo até chegar no parâmetro que deseja atualizar e faça as modificações.
3. Salve o arquivo.

## Atualização da lista de aplicativos

Os dados na lista de aplicativos, DEFAULTS.XML, são armazenados no banco de dados núcleo. Já que os nomes e os números das versões de aplicativos de software comumente usados mudam um tanto freqüentemente, o LANDesk publica um novo arquivo DEFAULTS.XML várias vezes ao ano (nas versões anteriores do software LANDesk, este arquivo tinha o nome de LDAPPL.INI).

**Para atualizar a lista de aplicativos**

1. Descarregue um novo arquivo DEFAULTS.XML ou LDAPPL3.TEMPLATE de http://www.landesk.com/support/downloads. Selecione um produto e clique em **Atualizar software** para baixar o arquivo.
2. Salve o arquivo no diretório LDLOGON.
3. Publique um novo LDAPPL3.INI seguindo as etapas em "Publicação da lista de aplicativos".

## Publicação da lista de aplicativos

A publicação da lista de aplicativos envolve a importação da lista de aplicativos mais atual em DEFAULTS.XML para o banco de dados e, em seguida, a combinação da lista de aplicativos com o conteúdo do arquivo LDAPPL3.TEMPLATE para gerar um arquivo LDAPPL3.INI atualizado. Há um utilitário standalone, o COREDBUTIL.EXE, no diretório \Arquivos de programas\LANDesk\ManagementSuite, que é usado para executar esses dois passos automaticamente .

**Para publicar a lista de aplicativos**

1. Inicie o CoreDBUtil.exe
2. Clique no botão **Publicar lista de aplicativos**.

Você deve publicar a lista de aplicativos após modificá-la ou fazer o download de uma versão atualizada do LDAPPL3.TEMPLATE ou DEFAULTS.XML.

# Configuração de hardware

## Suporte a Intel* AMT

O System Manager suporta dispositivos que usam a tecnologia Intel* AMT (Tecnologia de gerenciamento ativo Intel*), uma funcionalidade de hardware e firmware que habilita o gerenciamento de dispositivo remoto. A Intel AMT utiliza comunicação fora de banda (OOB) para o acesso a dispositivos independente do estado do sistema operacional ou da alimentação fornecida ao dispositivo.

O suporte Intel AMT neste produto inclui as versões 1 e 2. O processo para a configuração dos dispositivos da Intel AMT 2 inclui alguns dispositivos novos que não estavam presentes na versão 1. Consulte Configuração dos dispositivos Intel AMT para mais detalhes sobre a configuração com a versão 2. As informações nesta seção são válidas para as duas versões, exceto quando indicado o contrário.

A ferramenta de Configuração de hardware inclui os seguintes recursos para o gerenciamento dos dispositivos Intel AMT:

- Geração automática dos IDs de configuração (PID e PPS) (versão 2)
- Modificação no nome do usuário e senha para os dispositivos gerenciados
- Configuração e ativação das normas do System Defense (versão 2)
- Configuração e ativação da monitoração Presença do agente (versão 2)

### Gerenciamento de dispositivos com ou sem agentes de gerenciamento

Quando os dispositivos são configurados com a tecnologia Intel AMT, um número limitado de recursos de gerenciamento continua disponível mesmo se o dispositivo não tiver um agente do LANDesk instalado. Desde que os dispositivos estejam conectados à rede e tenham uma alimentação de espera, eles podem ser descobertos e podem ser adicionados ao inventário para serem gerenciados com outros dispositivos na rede.

Se um dispositivo tiver a tecnologia Intel AMT, mas não tiver um agente de gerenciamento instalado, ele pode ser descoberto com a descoberta de dispositivos não gerenciados, transferido para o banco de dados de inventário, e incluído na lista **Meus dispositivos**. Entretanto, muitas das opções de gerenciamento do System Manager não estarão disponíveis. Essas opções só são disponibilizadas quando o agente LANDesk é instalado. O recursos de gerenciamento disponíveis para os dispositivos configurados com a tecnologia Intel AMT são:

- **Resumo de inventário:** Um subconjunto dos dados de inventário normal do dispositivo pode ser consultado e examinado em tempo real mesmo se o dispositivo estiver desligado.
- **Log de eventos:** Um log com eventos específicos de Intel AMT, o qual mostra a gravidade e a descrição dos eventos, podem ser observados em tempo real.

- **Gerenciador de inicialização remota:** A ciclagem (ligar/desligar) de alimentação e várias opções de inicialização podem ser iniciadas do console de gerenciamento remoto, independente do estado do SO ou da alimentação do dispositivo. As opções disponíveis são baseadas no suporte para as opções no dispositivo. Alguns dispositivos podem não suportar todas as opções de inicialização.
- **Forçar análise de vulnerabilidade e desativar rede de SO:** Se um dispositivo parecer ter um software fraudulento sendo executado, pode ser feita uma análise de vulnerabilidade na próxima inicialização. Se necessário, o acesso de rede de nível de SO do dispositivo pode ser desativado para impedir a disseminação de pacotes indesejados na rede.

Para mais informações sobre as opções de gerenciamento, consulte Gerenciamento dos dispositivos Intel AMT.

## Requisitos de configuração da Intel AMT versão 1

Os dispositivos podem ser descobertos como Intel AMT somente após você ter acessado a Tela de configuração AMT no dispositivo e mudado a senha padrão do fabricante para uma senha protegida. (Consulte a documentação do fabricante para ver as informações sobre o acesso à Tela de configuração Intel AMT.) Se não fizer isso, os dispositivos serão descobertos, mas não serão identificados como Intel AMT e você não poderá ver as mesmas informações de resumo de inventário.

Para que o servidor núcleo se autentique com dispositivos Intel AMT descobertos, as credenciais nome de usuário/senha devem coincidir com as credenciais que você configurou usando o utilitário Configurar serviços. É possível mudar as credenciais usando-se a Tela de configuração Intel AMT.

Quando um dispositivo Intel AMT é adicionado ao banco de dados núcleo para ser gerenciado, o System Manager o configura automaticamente para o modo que você selecionar no utilitário Configuração de serviços, independente de já ter sido configurado. O modo Pequenas empresas fornece gerenciamento básico sem serviços de infra-estrutura de rede e não é seguro, enquanto que o modo Empresa é destinado a empresas de grande porte e fornece segurança com base em serviços de rede como DHCP, DNS e um serviço de autoridade de certificado TLS para assegurar uma comunicação segura entre o dispositivo gerenciado e o servidor núcleo.

Quando um dispositivo Intel AMT é configurado para o modo Empresa, o servidor núcleo instala um certificado no dispositivo para proteger a comunicação. Se o dispositivo for ser gerenciado por outro servidor núcleo, ele deve ser desconfigurado e reconfigurado pelo novo servidor núcleo. Se isso não for feito, o acesso à Intel AMT do dispositivo não responderá pois o novo servidor núcleo não tem certificado correspondente. Da mesma forma, se outro computador tentar acessar a funcionalidade Intel AMT no dispositivo, ele não terá sucesso pois não tem certificado correspondente.

# Configuração de dispositivos Intel* AMT

Os dispositivos equipados com a funcionalidade Intel AMT devem ser configurados ao serem ligados. O processo de configuração inclui várias medidas de segurança para assegurar que somente os usuários autorizados tenham acesso aos recursos de gerenciamento do Intel AMT.

Os dispositivos do Intel AMT comunicam-se com um servidor de configuração na rede. Esse servidor de configuração ouve as mensagens dos dispositivos Intel AMT na rede e permite que o grupo da TI gerencie os servidores através de comunicação fora da banda, independente do estado do SO dos dispositivos. O !ProductName! age como um servidor de configuração para os dispositivos Intel AMT e inclui recursos para ajudar você a configurar dispositivos. Você poderá, então, gerenciar os dispositivos com ou sem agentes de gerenciamento !ProductName! adicionais.

Esta seção descreve o processo recomendado para a configuração de novos dispositivos Intel AMT (versão 2). Durante este processo, você usará o System Manager para gerar um conjunto de IDs de configuração (PID e PPS). Esses IDs, ao serem inseridos na Tela de configuração Intel AMT do dispositivo, confirmam uma conexão segura com o servidor de configuração que está ciente desses IDs a fim de que o dispositivo Intel AMT possa completar seu processo inicial de configuração.

Os dispositivos com a versão 1 do Intel AMT usam um processo parecido mas não usam as chaves PID e PPS. Consulte as notas no final desta seção para ver mais detalhes.

## Configuração para os dispositivos Intel AMT 2

Quando um dispositivo Intel AMT 2 é recebido, o técnico da IT monta o computador e o ativa. Após ativar o dispositivo, o técnico faz a conexão à Tela de configuração Intel ME (Management Engine) baseada em BIOS e muda a senha padrão (admin) para uma senha forte. Isso permite o acesso à Tela de configuração Intel AMT.

Na Tela de configuração Intel AMT, as seguintes informações de pré-configuração são inseridas:

- Um ID de configuração (PID)
- Uma PPS (pre-provisioning passkey), também conhecida como PSK (pre-shared key)
- O endereço IP do servidor de configuração
- Porta 9982 como a porta para a comunicação com o servidor de configuração
- Modo empresa deve ser excluído
- O nome host do dispositivo Intel AMT

A PPS deve ser conhecida pelo servidor de configuração e dispositivo gerenciado, mas não pode ser transmitida na rede, por motivos de segurança. Ela precisa ser inserida manualmente no dispositivo (na Tela de configuração Intel AMT) e armazenada no servidor de configuração, que nesse caso também é o servidor núcleo para o System Manager. Pares PID/PPS são gerados pelo System Manager e armazenados no banco de dados. Você pode imprimir uma lista dos pares de ID gerados para uso na configuração.

O técnico da IT deve inserir o endereço IP do servidor núcleo System Manager como servidor de configuração e especificar a porta 9982. Caso contrário, por padrão, o dispositivo Intel AMT envia uma multidifusão que pode ser recebida se o servidor de configuração estiver ouvindo na porta 9971.

O nome de usuário e senha padrão para o acesso à Tela de configuração Intel AMT são "admin" e "admin". Eles são mudados durante o processo de configuração. O nome do usuário pode permanecer o mesmo mas é necessário mudar a senha para uma senha forte. A nova combinação de nome de usuário/senha é inserida no utilitário Configurar serviços, incluído com o System Manager, conforme descrito nas etapas a seguir.  Após cada dispositivo ter sido

configurado, você pode mudar o nome do usuário/senha individualmente por dispositivo, mas para fins de configuração, você usa o nome do usuário/senha encontrados em Configurar serviços.

Após as informações acima terem sido inseridas na Tela de configuração Intel AMT, o dispositivo envia mensagens “alô” quando for inicialmente conectado à rede, tentando comunicar-se com o servidor de configuração. Se esta mensagem for recebida pelo servidor de configuração, o processo de configuração iniciará conforme o servidor estabelecer uma conexão com o dispositivo gerenciado.

Quando o servidor núcleo recebe a mensagem de alô e verifica as chaves PID/PPS, ele configura o dispositivo Intel AMT ao modo TLS. O modo
TLS (Transport Layer Security) estabelece um canal seguro de comunicações entre o servidor núcleo e o servidor gerenciado enquanto a configuração é completada. Este process inclui a criação de um registro no banco de dados com o UUID do dispositivo e as credenciais criptografadas. Quando os dados do dispositivo estiverem no banco de dados, o dispositivo aparece na lista de dispositivos não-gerenciados.

Quando um dispositivo Intel AMT tiver sido configurado pelo servidor núcleo, ele poderá ser gerenciado somente usando a funcionalidade Intel AMT. Você pode selecioná-lo na lista de dispositivos não-gerenciados e acrescentá-lo aos seus dispositivos gerenciados. Você pode também distribuir os agentes de gerenciamento System Manager ao dispositivo para usar um conjunto maior de recursos de gerenciamento.

O processo recomendado para o uso do System Manager para configurar dispositivos Intel AMT 2 é o seguinte: Instruções específicas para os itens 1 e 2 são dadas nas seguintes etapas.

1. Execute o utilitário Configurar serviços para especificar uma senha nova e forte para configurar os dispositivos Intel AMT. (Veja detalhes a seguir.)
2. Use o System Manager para gerar um lote dos IDs de configuração Intel AMT (PID e PPS) e imprima a lista de chaves. (Veja detalhes a seguir.)
3. Conecte-se à Tela de configuração Intel ME do dispositivo do BIOS e mude a senha padrão para uma forte.
4. Acessa a Tela de configuração Intel AMT. Insira um par de chave PID/PPS da lista de IDs de configuração que você imprimiu. Insira o endereço IP do servidor núcleo (servidor de configuração) e especifique a porta 9982. Não deixe de selecionar o Modo empresa na configuração. Insira o nome host do dispositivo Intel AMT.
5. Após sair da tela do BIOS, o dispositivo iniciará o envio das mensagens "alô".
6. O servidor núcleo recebe uma mensagem "alô" e verifica o PID/PPS na lista de chaves geradas. Se houver uma correspondência, ele configura o dispositivo ao modo TLS.
7. O dispositivo é acrescentado à lista de descoberta de dispositivos não-gerenciados.
8. Selecione o dispositivo e acrescente-o aos seus dispositivos gerenciados. Ele será gerenciado como um dispositivo sem agente, como padrão, e você também pode distribuir agentes de gerenciamento ao mesmo.

**Para configurar o nome de usuário e senha Intel AMT no Configurar serviços**

1. No servidor núcleo, clique em **Iniciar |** LANDesk **| Configurar serviços**.
2. Clique na guia **Configuração Intel AMT**.
3. Digite **admin** como nome de usuário e senha sob as **Credenciais Intel AMT atuais**.

4. Digite um novo nome de usuário (opcional) e uma senha forte em **Configuração com as novas credenciais Intel AMT**.
5. Clique em **OK**.

Esses campos de nome de usuário e senha devem ser inseridos aqui antes da geração de um lote de IDs de configuração.

**Para gerar um lote de IDs de configuração Intel AMT**

1. No servidor núcleo, clique em **Configuração de hardware** no painel esquerdo de navegação.
2. Expanda o **AMT** e percorra **Configuração** até chegar em **Gerar IDs AMT**.
3. Digite o número de IDs a serem gerados (geralmente, o número de dispositivos que deseja provisionar).
4. Se quiser usar um prefixo diferente para os PIDs, digite-o na caixa de texto **Prefixo PID**. Esse prefixo só pode conter caracteres alfabéticos maiúsculos e números do conjunto de caracteres ASCII. Só podem ser inseridos o máximo de 7 caracteres para um prefixo.
5. Digite um nome de lote para identificar este grupo de IDs gerados.
6. Marque **Mostrar IDs AMT gerados** para mostrar os IDs gerados na lista. Se não marcar esta caixa, os IDs são gerados e salvos no banco de dados mas não são mostrados aqui.
7. Clique em **Gerar IDs**.
8. Após os IDs terem sido gerados, clique em **Imprimir lista de IDs** para abrir uma nova janela com a lista de IDs. (Somente os IDs mostrados no momento, na lista, são exibidos na nova janela.) Use o recurso de impressão do navegador para imprimir a lista.
9. Para ver todos os IDs gerados anteriormente, deixe em branco a caixa **Nome do lote** e clique em **Ver IDs de lote**.
10. Para ver um lote de IDs gerados, digite o nome do lote na caixa de texto **Nome do lote** e clique em **Ver IDs de lote**.

É possível gerar qualquer número de chaves de configuração de uma só vez. As chaves são armazenadas no banco de dados para referência futura à medida que você configura novos dispositivos Intel AMT. À medida que os dispositivos são configurados e as chaves de configuração são consumidas, a página **Gerar IDs AMT** mostrará IDs acinzentados para os que tiverem sido consumidos - assim você pode controlar quais IDs foram usados.

Um prefixo PID é acrescentado para facilitar a identificação dos IDs como PIDs, mas não lhe será requerido usar um prefixo. Recomendamos o uso de 0 a 4 caracteres; você pode usar um máximo de 7 caracteres para o prefixo.

Para identificar lotes de chaves de configuração, especifique um nome de lote. Este deve ser um nome descritivo que indique os dispositivos aplicados aos IDs. Por exemplo, você pode gerar lotes para cada organização na sua empresa e nomear os lotes Desenvolvimento, Marketing, Finanças, etc. Se mais tarde quiser ver os IDs gerados, digite o nome do lote e clique em **Ver IDs de lote** para ver uma lista somente com esses IDs.

## Senhas fortes

O Intel AMT requer o uso de uma senha forte para habilitar comunicações seguras. As senhas devem satisfazer aos seguintes requisitos:

- ter pelo menos oito caracteres

- incluir pelo menos um número (de 0 a 9)
- incluir pelo menos um caracter ASCII não-alfanumérico (por exemplo !, &, %)
- conter caracteres latinos maiúsculos e minúsculos ou caracteres não ASCII (UTF+00800 e acima)

## Erros no processo de configuração

Se você digitar PID e PPS que não formarem um par correto (por exemplo, o PPS deve formar um par com um PID diferente), aparecerá um erro no registro de alerta e a configuração não prosseguirá para aquele dispositivo. Será necessário reiniciar o dispositivo e reinserir um par PID/PPS correto na Tela de configuração Intel AMT.

Se, ao digitar um PID, a Tela de configuração Intel AMT mostrar um erro, você digitou o PID incorreto. É feito um checksum (soma de verificação) para confirmar se o PID é correto.

## Descoberta de dispositivos Intel AMT 1.0.

Ao executar uma análise de descoberta de dispositivo, os dispositivos Intel AMT versão 1 são descobertos e acrescentados à pasta Intel AMT na lista de dispositivos **Não-gerenciados**. Eles são reconhecidos como dispositivos Intel AMT se tiverem sido configurados com um nome de usuário e senha segura, substituindo os padrões definidos pelo fabricante.

Ao acrescentar um nome de usuário e senha segura na Tela de configuração Intel AMT, você poderá também digitar o endereço IP do servidor de configuração e especificar a porta 9982, como é feito com os dispositivo Intel AMT 2. Nenhum par PID/PPS, porém, é usado na configuração dos dispositivos Intel AMT 1. Se você especificar um endereço IP do servidor de configuração, o servidor núcleo age como servidor de configuração e você pode gerenciá-lo como agente sem dispositivo.

Observe que o Intel AMT versão 1 não usa o mesmo nível de segurança da versão 2. A Intel recomenda que os dispositivos com a versão 1 sejam configurados em uma rede isolada e segura. Após a configuração estar completa, eles podem ser movidos a uma rede menos segura, para gerenciamento.

# Modificação no nome do usuário e senha para os dispositivos Intel* AMT

Um nome de usuário e senha segura são requeridos para a configuração de novos dispositivos Intel AMT (versão 1). Para os dispositivos gerenciados com o System Manager, o nome do usuário e a senha inseridos na Tela de configuração Intel AMT devem ser os mesmos inseridos no utilitário Configuração de serviços do System Manager. O nome do usuário e a senha no utilitário Configuração de serviços são salvos no banco de dados e aplicados globalmente para a provisão dos dispositivos Intel AMT.

O Intel AMT requer o uso de uma senha forte para habilitar comunicações seguras. As senhas devem satisfazer aos seguintes requisitos:

- ter pelo menos oito caracteres

- incluir pelo menos um número (de 0 a 9)
- incluir pelo menos um caracter ASCII não-alfanumérico (por exemplo !, &, %)
- conter caracteres latinos maiúsculos e minúsculos ou caracteres não ASCII (UTF+00800 e acima)

Após a configuração, é necessário mudar os nomes de usuários e senhas, regularmente, como parte da manutenção da TI. É possível usar uma combinação diferente de nome de usuário/senha para cada dispositivo Intel AMT ou aplicar uma combinação de nome de usuário/senha para múltiplos dispositivos. As novas combinações de nome de usuário/senha inseridas na página de Configuração de hardware são armazenadas no banco de dados e usadas pelo System Manager para a comunicação segura com os dispositivos gerenciados Intel AMT.

**Para modificar o nome do usuário e senha dos dispositivos Intel AMT**

1. No servidor núcleo, clique em **Configuração de hardware** no painel esquerdo de navegação.
2. Expanda o **AMT** e percorra a árvore até a **Configuração**.
3. Na lista **Todos os dispositivos**, selecione um ou mais dispositivos nos quais quiser mudar o nome do usuário e a senha. Clique em **Alvo** na barra de ferramentas.
4. No painel inferior, digite um novo nome de usuário, em seguida digite e confirme a nova senha.
5. Clique em **Dispositivos alvo**, em seguida clique em **Aplicar**.

   Para um dispositivo único ou múltiplos na mesma lista, é possível selecionar os dispositivos e clicar em **Dispositivos selecionados**, em seguida clique em **Aplicar**.

# Configuração de diretivas do System Defense

O Intel AMT* 2.0 inclui um recurso deSystem Defense, que faz cumprir as diretivas de segurança da rede nos dispositivos com a funcionalidade Intel AMT 2.0. Você pode selecionar e aplicar as diretivas do System Defense para os dispositivos gerenciados usando a ferramenta **Configuração de hardware**.

Quando a diretiva do System Defense for aplicada a um dispositivo AMT, o dispositivo filtra os pacotes de entrada e saída da rede, de acordo com as diretivas definidas. Quando o tráfego na rede coincidir com as condições de alerta definidas em um filtro, um alerta é gerado e o acesso à rede do dispositivo é bloqueado. O dispositivo é então isolado da rede até você completar as etapas de correção para aquela diretiva.

O System Managercontém diretivas pré-definidas do System Defense que podem ser aplicadas aos seus dispositivos Intel AMT. Cada diretiva contém um conjunto de filtros que define qual tipo de tráfego de rede não é permitido e as ações resultantes quando o tráfego satisfizer os critérios do filtro. A seguir está o processo de seleção e aplicação das diretivas:

1. Selecione como alvo um ou mais dispositivos gerenciados
2. Selecione a diretiva de System Defense a ser aplicada; se necessário, edite a diretiva
3. Aplique a diretiva aos dispositivos alvo

Quando uma diretiva de System Defense está ativa em um dispositivo gerenciado, o dispositivo monitora todo o tráfego de entrada e saída da rede. O seguinte ocorre se as condições do filtro forem detectadas:

1. O dispositivo gerenciado envia um alerta ASF ao servidor núcleo e uma entrada é acrescentada ao log de alerta
2. O servidor núcleo determina qual diretiva foi invalidada e fecha o acesso à rede no dispositivo gerenciado
3. O dispositivo é listado na fila de correção do System Defense (na ferramenta **Configuração de hardware**)
4. Para restaurar o acesso do dispositivo à rede, o administrador segue as etapas necessárias de correção e, em seguida, remove o dispositivo da fila de correção; isso restaura a diretiva original do System Defense no dispositivo

Este processo é descrito com mais detalhes nas seções a seguir.

## Seleção e aplicação das diretivas do System Defense

O System Managercontém as seguintes diretivas predefinidas do System Defense que podem ser aplicadas aos dispositivos do Intel AMT 2.0. As diretivas são definidas com parâmetros, como, por exemplo, número da porta, tipo do pacote e número de pacotes dentro de um período específico de tempo. Ao habilitar uma diretiva, ela é registrada com o Intel AMT nos dispositivos selecionados. As diretivas são salvas como arquivos XML no dispositivo gerenciado, na pasta CircuitBreakerConfig.

- **BlockFTPSrvr:** Esta diretiva impede o tráfego através da porta FTP. Quando os pacotes são enviados ou recebidos na porta 21 do FTP, os mesmos são soltos e o acesso à rede é suspenso.
- **LDCBKillNics:** Esta diretiva bloqueia o tráfego em todas as portas da rede com exceção das seguintes portas de gerenciamento:

| Descrição da porta | Número da faixa | Direção do tráfego | Protocolos |
|---|---|---|---|
| LANDesk management | 9593-9595 | Enviar/receber | TCP, UDP |
| Gerenciamento Intel AMT | 16992-16993 | Enviar/receber | Somente TCP |
| DNS | 53 | Enviar/receber | Somente UDP |
| DHCP | 67-68 | Enviar/receber | Somente UDP |

Quando o servidor núcleo termina o acesso à rede em um dispositivo gerenciado, ele aplica esta diretiva ao dispositivo. Em seguida, quando o dispositivo é removido da fila de correção, a diretiva original é reaplicada ao dispositivo.

- **LDCBSYNFlood:** Esta diretiva detecta um ataque de recusa de serviço SYN flood, pois ela não permite mais que 10,000 pacotes TCP com o sinalizador SYN ativado, em um minuto. Quando o número é excedido, o acesso à rede é suspenso.
- **UDPFloodPolicy:** Esta diretiva detecta um ataque de recusa de serviço UDP flood, pois ela não permite mais que 20.000 pacotes UDP por minuto nas portas numeradas entre 0 e 1023. Quando esse número é excedido, o acesso à rede é suspenso.

**Para selecionar uma diretiva do System Defense**

1. No painel de navegação esquerdo, clique em **Configuração do hardware**.
2. Clique em **AMT** e percorra a árvore até as **Diretivas**.
3. Na lista, selecione os dispositivos aos quais quiser aplicar a diretiva (use Ctrl+click ou Shift+click para selecionar vários dispositivos).
4. Clique em **Alvo** na barra de ferramentas para adicionar os dispositivos à lista **Dispositivos alvo**.
5. No painel inferior, selecione uma diretiva na lista suspensa.
6. Clique em **Dispositivos alvo**, em seguida clique em **Aplicar**.

## Restauração do acesso à rede aos dispositivos na fila de correção

Se o acesso à rede de um dispositivo estiver suspenso por causa de uma diretiva do System Defense, o dispositivo aparece na fila de correção. Ele permanecerá lá até que você o remova da lista, o que reintegra a diretiva ativa naquele dispositivo. Antes de fazê-lo, é necessário resolver o problema que colocou o dispositivo na fila. Por exemplo, se o tráfego FTP foi detectado, você precisará confirmar que as ações apropriadas foram tomadas para impedir mais tráfego FTP no dispositivo.

**Para remover um dispositivo da fila de correção**

1. No painel de navegação esquerdo, clique em **Configuração do hardware**.
2. Clique em **AMT** e percorra a árvore até a **Correção CB**.
3. Selecione os dispositivos cujas diretivas de System Defense possam ser restauradas e clique em **Remover**.

# Configuração da Presença do agente AMT Intel*

Intel* AMT 2.0 inclui uma ferramenta de segurança que pode monitorar a presença de agentes de software nos dispositivos gerenciados. É possível habilitar a monitoração da Presença do agente para assegurar que os agentes de gerenciamento nos seus dispositivos estejam sendo executados continuamente e alertados quando um agente pára - mesmo quando outros agentes, baseados em software, não possam detectar o problema.

O System Manager usa a Presença do agente Intel AMT para monitorar dois agentes: o agente padrão de gerenciamento e o serviço de monitoração. Ele é útil quando a comunicação normal de monitoração não está disponível. Por exemplo, uma camada de comunicação do dispositivo

pode não estar funcionando ou o agente de monitoração pode ter parado de funcionar. Por padrão, a Presença do agente também monitora o próprio processo de monitoração - neste caso, você recebe um alerta se ela parou de funcionar.

A monitoração da Presença do agente é feita ao configurar-se um temporizador que ouve as mensagens de "pulsações" dos agentes de gerenciamento no dispositivo para verificar que os agentes estão em execução. Se um temporizador vencer por não ter recebido a mensagem de pulsação, o Intel AMT envia um alerta ao servidor núcleo.

Quando você configurar a Presença do agente, o agente no dispositivo faz o registro com o Intel AMT para enviar as pulsações diretamente ao Intel AMT; se as pulsações pararem, o Intel AMT pode, então, alertar o servidor núcleo através de comunicação fora de banda que o agente do dispositivo não está respondendo. O Intel AMT envia um alerta PET (platform event trap - interceptação de evento de plataforma) ao servidor núcleo com uma descrição do estado modificado. Como padrão, este alerta é registrado com o funcionamento do dispositivo. Você pode configurar outras ações de alerta a serem iniciadas quando este alerta for recebido (para informações sobre a configuração de ações de alertas, consulte Configuração de ações de alertas).

Ao configurar a monitoração da Presença do agente, você pode habilitar ou desabilitar a monitoração para dois agentes e definir os seguintes valores:

- **Pulsação:** A maior quantidade de tempo (em segundos) que pode passar entre os sinais de pulsação. Se este limite de tempo for excedido sem que uma nova pulsação tenha sido recebida, o agente é considerado sem resposta. O valor padrão é de 120 segundos para o agente padrão de gerenciamento e 180 segundos para o serviço de monitoração; o valor mínimo para ambos é de 30 segundos.
- **Tempo de inicialização:** A tempo máximo (em segundos) que pode decorrer após o início do sistema operacional antes que uma pulsação tenha sido recebida por um agente. Se este limite de tempo for excedido, o agente é considerado sem resposta. A Presença do agente é configurada no Intel AMT quando o agente é instalado; dessa forma, isso deve dar tempo suficiente para que o agente comece a ser executado e a enviar a sua primeira pulsação. O valor padrão é de 360 segundos; o valor mínimo é de 30 segundos.

**Para editar a configuração da Presença do agente AMT Intel**

1. No painel de navegação esquerdo, clique em **Configuração do hardware**.
2. Expanda o **AMT** e percorra a árvore até a **Configuração do AP**.
3. Para desabilitar a monitoração da Presença do agente nos dispositivos Intel AMT 2.0, desmarque o quadro **Habilitar a monitoração da Presença do agente**.
4. Para desabilitar a monitoração para um agente específico, desmarque o quadro próximo ao nome do agente. (Mesmo se ambos os quadros estiverem desmarcados, a Presença do agente continuará a monitorar seu próprio processo de monitoração enquanto estiver habilitado.)
5. Digite um novo valor no quadro **Pulsação** para mudar o tempo máximo permitido entre as pulsações( o mínimo é de 30 segundos).
6. Digite um novo valor no quadro **Tempo de inicialização** para mudar o tempo máximo permitido ao agente para enviar a primeira pulsação após o sistema operacional iniciar no dispositivo (o mínimo é de 30 segundos; 120 segundos é recomendado).

# Suporte IPMI

O System Manager oferece suporte para IPMI (Intelligent Platform Management Interface) 1.5 e 2.0. 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 não, ou do estado do SO. Para obter mais detalhes sobre o IPMI, visite o site da web da Intel.

A monitoração IPMI é feita pelo BMC (controlador de gerenciamento de baseboard). O BMC opera com energia de espera e faz polling autônomo do status da condição do sistema. Se o BMC detectar que um elemento está com funcionamento anormal ou inativo (fora de banda), você pode configurar as ações resultantes da IPMI, por exemplo, registro de eventos, geração de alertas ou realizar ações de recuperação automática como o desligamento ou reinicialização do sistema.

É necessário ter o SMBIOS 2.3.1 ou mais recente instalado para o BMC ser detectado no sistema. Se o BMC não é detectado, podem não aparecer algumas informações que a IPMI reporta, exporta, etc.

A IPMI identifica as interfaces comuns do hardware usado para monitorar as características da condição física como temperatura, voltagem, ventiladores, fontes de alimentação e intrusão no chassi. Além da monitoração da condição, a IPMI contém outros recursos de gerenciamento do sistema como alertas automáticos, desativação e reativação automáticas do sistema, recursos de reinicialização e controle de energia remotos e controle de recursos.

As escolhas de menu do System Manager variam ligeiramente para um dispositivo habilitado para IPMI, dependendo do estado do sistema operacional.

## Recursos de gerenciamento para os dispositivos habilitados para IPMI

Os recursos de monitoração dependem do que foi instalado no dispositivo sendo monitorado. Qualquer dispositivo habilitado para IPMI com BMC (baseboard management controller) pode ser monitorado pelo console do administrador de maneiras limitadas sem a necessidade de agentes de gerenciamento adicionais, após o BMC ter sido configurado. Isso inclui gerenciamento fora de banda quando o dispositivo está desligado ou o SO não funciona. O gerenciamento completo se torna disponível quando o agente de gerenciamento é instalado, um BMC está presente, o dispositivo está ligado e o SO funciona. A tabela abaixo compara a funcionalidade disponível com essas diferentes configurações.

| | **Apenas BMC*** | **BMC + agente** | **Agente (sem IPMI)** |
|---|---|---|---|
| Gerenciamento fora da banda habilitado | X | X | |
| Gerenciamento dentro da banda | | X | X |

| | Apenas BMC* | BMC + agente | Agente (sem IPMI) |
|---|---|---|---|
| habilitado | | | |
| Dispositivo pode ser descoberto** | X | X | X |
| Leitura dos sensores de ambiente | X | X | Dependente de hardware |
| Alimentação ligada/desligada remotamente | X | X | X |
| Leitura e limpeza do log de eventos | X | X | |
| Configuração de alertas | X | X | X |
| Leitura de informações do SO | | X | X |
| Desativação suave | | X | X |
| Leitura das informações do SMBIOS (processador, slots, memória) | | X | X |
| Sincronização de IP (SO para BMC) | | X | |
| Temporizador de vigia | | X | |
| BMC se comunica com o servidor núcleo | X | X | |
| Componentes locais do System Manager comunicam-se com o servidor núcleo | | X | X |
| Uma gama completa de recursos de gerenciamento do System | | X | |

| | Apenas BMC* | BMC + agente | Agente (sem IPMI) |
|---|---|---|---|
| Manager | | | |

*Standard BMC. O mini BMC é uma versão reduzida de um controlador de gerenciamento de placa básica. Ele contém as funcionalidades acima descritas com as seguintes limitações:

- Não suporta redireção serial por LAN (SOL)
- Só tem um nome de usuário para gerenciamento BMC
- Utiliza apenas um canal para comunicar-se com BMC
- Tem um menor repositório de registro de eventos (SEL) de sistema

**Se o BMC não estiver configurado, ele não responderá aos pings ASF que são usados pelo produto para descobrir o IPMI. Isso significa que você terá que descobrí-lo como um computador normal. Quando distribuir um agente de gerenciamento, o executável da configuração do servidor analisará o sistema e detectará que é IPMI e configurará o BMC.

## Conflitos com outros drivers IPMI

Se tiver instalado outro software de gerenciamento que inclua dispositivos ou drivers IPMI nos dispositivos que quiser gerenciar com o System Manager, você precisará desinstalar tais produtos antes de distribuir os agentes do Management Suite com recursos de gerenciamento IPMI.

Por exemplo, o Microsoft* Windows* Server 2003 inclui suporte IPMI na instalação do WinRM (Windows Remote Management), que inclui um provedor WMI (Windows Management Instrumentation) e um driver IPMI. O System Manager, porém, não suporta a instalação daquele driver IPMI e instala o seu próprio driver IPMI. Se o WinRM foi instalado em um dispositivo que você quiser gerenciar com o System Manager, é necessário primeiro desinstalar o WinRM através do Adicionar/Remover programas do Windows (**Iniciar | Painel de controle | Adicionar ou remover programas | Adicionar/remover componentes do Windows | Ferramentas de gerenciamento e monitoração |** limpe o quadro **Gerenciamento de hardware** | clique em **OK**).

# Configuração IPMI BMC

Use a página **Configuração IPMI BMC** para personalizar os parâmetros com dispositivos habilitados com o IPMI. Os recursos descritos abaixo estão disponíveis para dispositivos em banda. Se um dispositivo estiver fora de banda, apenas a configuração de energia e os parâmetros de usuário de BMC estarão disponíveis.

**CUIDADO**: É recomendado enfaticamente não mudar os parâmetros de IPMI a menos que você esteja familiarizado com a especificação IPMI e tenha uma compreensão das tecnologias utilizadas com esses parâmetros. O uso incorreto dessas opções de configuração pode impedir o System Manager de comunicar-se com os dispositivos habilitados com IPMI.

As seguintes opções de configuração estão disponíveis:

- Temporizador de vigia
- Configuração de energia

- Parâmetros do usuário
- Senha BMC
- Configuração LAN
- Configuração SOL
- Configuração IMM

## Mudanças dos parâmetros de temporizador de vigia

O IPMI fornece uma interface para o temporizador de vigia do BMC. Esse temporizador pode ser definido para vencer periodicamente e é configurado para iniciar determinadas ações se vencer (como, por exemplo, ciclagem de alimentação). O System Manager é configurado para redefinir o temporizador periodicamente de forma que o limite não vença. Se o dispositivo tornar-se indisponível (por exemplo, for desativado ou travar), o temporizador não será redefinido e o limite vencerá iniciando, assim, a ação.

Você pode especificar o tempo limite do temporizador e selecionar uma ação para ser executada se o limite não vencer. Você pode escolher não fazer nada, fazer uma reinicialização manual (desligar e reiniciar) do dispositivo, desativar o dispositivo ou executar uma ciclagem de alimentação (desativar e, em seguida, reiniciar novamente).

Também pode definir o BMC para parar as mensagens de multidifusão ARP (Address Resolution Protocol) enquanto o temporizador de vigia estiver ativado, o que reduzirá o tráfego da rede sendo gerado. Se você suspender os ARPs, eles continuarão automaticamente se o temporizador de vigia vencer.

**Para mudar os parâmetros de temporizador de vigia**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Temporizador de vigia**.
4. Selecione **Ativar o temporizador de vigia** para ativar o temporizador.
5. Especifique a freqüência de consulta ao temporizador (número de minutos ou segundos).
6. Selecione uma ação a ser iniciada quando o limite estabelecido do temporizador de vigia vencer.
7. Se quiser que o BMC páre de emitir mensagens ARP quando o temporizador de vigia estiver ativado, selecione **Suspender ARPs de BMC**.
8. Clique em **Aplicar**.
9. Se tiver mudado os parâmetros de temporizador de vigia, você pode reverter para os parâmetros padrão clicando em **Restaurar padrões**.

## Mudança dos parâmetros de configurações de energia

Quando há queda de energia em um computador habilitado com IPMI, é possível especificar a ação esperada quando a energia for restaurada. Recomenda-se restaurar o computador a qualquer que for o estado no momento em que houve queda da energia, mas você também pode optar por mantê-lo desligado ou ligá-lo.

**Para mudar os parâmetros de configurações de energia**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Congiruação IPMI BMC** e clique em **Configuração de energia**.
4. Selecione uma opção para quando a energia for restaurada.
5. Clique em **Aplicar**.
6. Se tiver mudado os parâmetros de alimentação, você pode reverter para os parâmetros padrão clicando em **Restaurar padrões**.

## Parâmetros do usuário do BMC

O System Manager autentica-se no BMC com uma combinação de nome de usuário/senha exclusiva ao BMC (separada de qualquer outro nome de usuário do System Manager). O System Manager reserva o primeiro nome de usuário para poder comunicar-se sempre com o BMC. Se o BMC permitir a definição de outros nomes de usuário, eles podem ser definidos com senhas para autenticação no BMC.

Também é possível especificar os níveis de privilégio para cada usuário. Para IMMs avançados, você pode especificar níveis de privilégio (telnet, http e https) para cada canal.

**CUIDADO:** Use de extremo cuidado ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

**Para mudar os parâmetros do usuário do BMC**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configurações do usuário**.
4. Para limpar os dados de um nome de usuário, clique no número do índice e clique em **Limpar**.
5. Para adicionar ou mudar um nome de usuário, clique no número do índice e clique em **Editar**.
6. Digite um nome de usuário.
7. Para definir uma senha, marque o quadro **Definir senha**, em seguida digite a senha e confirme.
8. Selecione os níveis de privilégio para LAN e acesso serial.
9. Clique em **Salvar as alterações**.

## Modificação da senha do BMC

O System Manager autentica-se a um BMC de dispositivo usando o nome de usuário (usuário 1) e senha padrão. Não é possível mudar o nome do usuário, mas é possível mudar a sua senha. Quando você mudar essa definição de senha, a mudança é salva no banco de dados e no BMC.

**Para mudar a senha padrão do BMC**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Senha**.
4. Digite a nova senha e confirme-a.
5. Clique em **Aplicar**.

## Mudança das configurações de LAN

As mensagens de IPMI podem ser transmitidas diretamente do BMC através de uma interface LAN, além da interface do sistema do dispositivo. A habilitação da comunicação por LAN permite ao servidor núcleo receber alertas específicos de IPMI se o dispositivo estiver desativado. O servidor núcleo mantém essa comunicação enquanto o dispositivo tiver uma conexão física com a rede com endereço de rede válido e enquanto a alimentação principal do dispositivo permanecer conectada.

**CUIDADO:** Se escolher a configuração personalizada para a comunicação LAN ou serial ao BMC, use de extremo cuidado ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

Se um canal LAN estiver definido, é possível usar as configurações padrão para o BMC do dispositivo, ou mudar o endereço IP e configurações do gateway. Use essas opções para definir destinos às interceptações SNMP enviadas pelo BMC a cada evento PET (Platform Event Trap).

Também é possível mudar as configurações da string da comunidade SNMP para enviar alertas com a LAN. Ao configurar esses parâmetros, é necessário especificar a string da comunidade SNMP usada para a autenticação SNMP. Para cada configuração, é possível editar o destino da interceptação para especificar onde e como as interceptações são enviadas e se são reconhecidas.

**Para definir as propriedades de configuração do canal LAN**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Congiruação IPMI BMC** e clique em **Configuração LAN**.
4. Selecione **Sempre disponível** na lista suspensa de comunicações LAN para manter aberto o acesso ao BMC. Se você selecionar **Desativado**, não terá acesso LAN ao BMC quando o dispositivo estiver fora de banda.
5. Selecione o nível de privilégio de usuário para o canal: O **Nível de administrador** tem acesso a todos os comandos, mas o **Nível de usuário** é limitado ao acesso de somente leitura (haverá uma configuração de recurso restrito se selecionar o Nível de usuário).
6. Marque **Desativar permanentemente os ARPs do BMC** para desativar as mensagens ARP do the BMC. Isso reduz o tráfego na rede mas pode impedir a comunicação com o BMC quando o dispositivo estiver fora de banda.
7. Marque **Desativar as respostas do ARP** para que o BMC páre de enviar respostas de mensagens ARP quando o SO não estiver disponível. Se você ativar essa configuração, poderá impedir a comunicação com o BMC quando o dispositivo estiver fora de banda.

8. As configurações IP para o canal LAN são definidas automaticamente se o BMC estiver sincronizado com o canal do SO. Se não estiver, a caixa de seleção sob a guia **Configurações IP** estará ativada. A caixa pode permanecer marcada para usar as configurações DHCP fornecidas automaticamente ou desmarcada para que você edite os campos de texto com configurações estáticas. São preferíveis as configurações automáticas.
9. Clique na guia **Enviar alertas com a LAN** para definir as configurações de string de comunidade SNMP (veja os detalhes a seguir).
10. Clique em **Aplicar** para salvar as mudanças.

**Para mudar as propriedades da opção Enviar alertas com a LAN**

1. Abra a **Configuração LAN** página (etapas de 1 a 3, acima).
2. Clique na guia **Enviar alertas com a LAN**.
3. Marque a caixa de seleção **Ativado** para ativar o envio de alertas SNMP.
4. Especifique a **String de comunidade SNMP** para ser usada com a autenticação SNMP.
5. Para configurar os destinos da interceptação, clique duas vezes no número do índice para abrir a caixa de diálogo **Propriedades**.
6. Especifique o endereço IP ao qual os alertas serão enviados pelo BMC, assim como o endereço MAC correspondente.
7. Especifique o número de vezes para as tentativas, a freqüência de tentativas e o gateway preferencial a ser usado.
8. Se você quiser que os alertas sejam reconhecidos (o que aumenta o tráfego gerado na rede), marque a caixa de seleção **Reconhecimento de alertas**.
9. Clique em **OK**.
10. Na página de configuração da LAN, clique em **Aplicar** quando todos os parâmetros estiverem completos.

## Mudança das configurações SOL (Serial Over LAN)

Use as opções de configuração SOL (Serial Over LAN) para personalizar os parâmetros de modem serial em utilizações especiais, como, por exemplo, redirecionar mensagens POST do BIOS à porta serial. Se o BMC for necessário para discar uma conexão de modem, serão também necessários parâmetros específicos de modem como, por exemplo, strings de inicialização e strings de discagem.

Para a operação com modem serial, pode ser necessário configurar o BIOS e as configurações de jumper. Consulte a documentação para ver os detalhes sobre o dispositivo específico.

**CUIDADO:** Se escolher a configuração personalizada para a comunicação LAN ou serial ao BMC, use de extremo cuidado ao modificar os parâmetros. Parâmetros incorretos podem desabilitar a comunicação BMC dos dispositivos com este produto.

**Para mudar os parâmetros de configurações do SOL**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configuração do hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração do SOL**.
4. Marque **Ativar comunicações SOL** para ativar o SOL.

5. Selecione o mínimo **Nível de usuário requerido para ativar o SOL**.
6. Selecione **Taxa de transmissão para as sessões SOL** apropriadas para a configuração de hardware do dispositivo.
7. Clique em **Aplicar**.

## Mudança das configurações IMM

A página **Configuração IMM** só é mostrada para os dispositivos IPMI equipados com uma placa integrada IMM avançada. As opções nesta página permitem ativar ou desativar os protocolos e recursos para uso com o dispositivo habilitado para o IMM. Consulte a documentação do fabricante do IMM antes de efetuar quaisquer mudanças a essas configurações.

**Para mudar os parâmetros de configurações do IMM**

1. Na tela **Meus dispositivos**, clique duas vezes no dispositivo que deseja configurar.
2. No painel esquerdo de navegação do console de informações do servidor, clique em **Configurações de hardware**.
3. Expanda a **Configuração IPMI BMC** e clique em **Configuração IMM**.
4. Marque as caixas nos protocolos e recursos que quiser ativar e acrescente as definições necessárias. As opções disponíveis são:
   - KVM
   - SNMP
   - telnet
   - Alerta SMTP
   - HTTP
   - HTTPS
5. Clique em **Aplicar**.

## Gerenciamento de dispositivos Dell* DRAC

Este produto inclui integração de gerenciamento com dispositivos equipados com o Dell* DRAC (Remote Access Controller). O DRAC é um controlador remoto de hardware que fornece uma interface ao hardware de gerenciamento de servidor compatível com IPMI no dispositivo Dell. O DRAC tem um endereço IP, usado para identificar o dispositivo DRAC na descoberta de dispositivo e no gerenciamento do dispositivo.

Os dispositivos que contêm um Dell DRAC podem ser gerenciados com a mesma funcionalidade como outros dispositivos compatíveis com IPMI. Quando o dispositivo tiver sido descoberto e acrescentado à lista de dispositivos gerenciados, ele é gerenciado como outro dispositivo IPMI. Além disso, o System Manager também tem recursos Dell DRAC únicos.

O OpenManage Server Administrator é um console baseado na Web fornecido pela Dell para o gerenciamento do dispositivo Dell DRAC. Ele é normalmente acessado digitando-se o endereço IP do DRAC em um navegador e fazendo-se login com nome de usuário e senha. Quando um dispositivo Dell DRAC é gerenciado com o System Manager, também é possível abrir esse utilitário diretamente da interface do System Manager.

Além disso, o System Manager permite o gerenciamento de nomes de usuários e senhas para acesso ao OpenManager Server Administrator e mostra três logs desse utilitário no console de informações do servidor.

**Para abrir o OpenManage Server Administrator para um dispositivo Dell DRAC**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. No console de informações do servidor, expanda **Hardware** e clique em **Dell DRAC**. O endereço IP do dispositivo e outras informações de identificação são mostradas.
3. Clique em **Iniciar o utilitário Dell DRAC** para abrir o OpenManage Server Administrator do dispositivo em uma nova janela.

## Os logs do Dell DRAC estão disponíveis no System Manager

Três logs do utilitário OpenManage Server Administrator são mostrados no console de informações do servidor do System Manager.

- **Log Dell DRAC**: Controla todos os eventos registrados pelo Administrador do servidor como, por exemplo, atividade de login, status da sessão, status da atualização do firmware e interação entre o DRAC e outros componentes do dispositivo. As informações mostradas no System Manager incluem gravidade do evento, descrição e ações de correções sugeridas em caso de erros.
- **Log de comando do Dell DRAC**: Acompanha todos os comandos emitidos pelo Administrador do servidor. Mostra quais comandos foram realizados, por quem, quando, incluindo as tentativas de log in e log out e os erros de acesso.
- **Log de traço Dell DRAC**: Util para traçar detalhes sobre os eventos de comunicação da rede como, por exemplo, alerta, mensagem de pager ou conexões de rede do DRAC.

**Para ver os logs de um dispositivo Dell DRAC**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. No console de informações do servidor, expanda **Logs**.
3. Clique em **Log Dell DRAC**, **Log de comando Dell DRAC** ou **Log de traço Dell DRAC**.

## Gerenciamento de nomes de usuários para os dispositivos habilitados com o Dell DRAC

Para acessar a interface do OpenManage Server Administrator você faz o login com um nome de usuário e senha definidos para o dispositivo. O usuário padrão **raiz** é o primeiro usuário na lista e não pode ser excluído, mas sua senha pode ser modificada. Até 15 usuários podem ser acrescentados. Embora os nomes de usuários DRAC possam ter níveis diferentes de acesso, o System Manager só define nomes de usuários no mesmo nível de administração.

**Para acrescentar ou editar nomes de usuários e senhas para um dispositivo habilitado com o DRAC**

1. Clique duas vezes no dispositivo na lista **Todos os dispositivos**.
2. No console de informações do servidor, clique em **Configuração de hardware**.

3. No console de configuração de hardware, expanda a **Configuração Dell DRAC** e clique em **Usuários Dell DRAC**. Aparece uma lista dos usuários definidos atuais.
4. Para mudar a senha de um usuário, clique no número do usuário e clique em **Mudar senha**. Digite e confirme a nova senha, em seguida clique em **Aplicar**. (Para designar a mesma senha para vários usuários, selecione-os usando Ctrl +Clique ou Shift+clique.)
5. Para acrescentar um usuário, clique em **Adicionar usuário**. Digite um nome de usuário e senha e confirme a senha, em seguida clique em **Aplicar**. O usuário é acrescentado à lista.

   **Nota:** se você digitar um nome de usuário que já constar na lista, a nova senha especificada sobregravará a existente para aquele dado nome; não será acrescentado um segundo usuário com aquele nome à lista.

6. Para excluir um usuário, clique no número do usuário e clique em **Excluir usuário**, em seguida clique em **OK**. (Para excluir vários usuários, selecione-os usando Ctrl +Clique ou Shift+clique.)

Todos os usuários nessa lista têm acesso de nível de administração ao the OpenManage Server Administrator.

# Instalação e Manutenção do banco de dados núcleo

## Instalação do banco de dados núcleo

A instalação padrão deste produto instala o Microsoft MSDE no servidor núcleo. Esta é a única opção disponível de banco de dados para o System Manager, e somente um banco de dados núcleo pode ser instalado. Ele deve ser instalado somente em um servidor independente.

O esquema de banco de dados suporta o Microsoft SQL Server 2000 com SP4. Todos os servidores de banco de dados precisam do MDAC 2.8.

O banco de dados instalado no seu servidor núcleo pode ser completamente novo. Se estiver instalando o System Manager em um servidor com uma instalação anterior do LANDesk® Management Suite ou Server Manager, você não poderá usar a estrutura existente do banco de dados para a sua instalação do System Manager.

O utilitário LANDesk Configuração de serviços contém uma interface que permite configurar vários serviços. A guia Geral nesse utilitário mostra o nome do servidor atual, o nome do banco de dados e o nome de usuário/senha requeridos para acessar o banco de dados núcleo. Essas credenciais são usadas por todos os dispositivos que acessam o banco de dados núcleo. Como o System Manager só pode usar um banco de dados, não é necessário mudar o nome do servidor ou do banco de dados. Se necessário, as credenciais podem ser mudadas. Para mais informações, consulte o Apêndice C: Configurar serviços.

# Apêndice A: Requisitos do sistema e uso da porta

O núcleo deve ter um endereço IP estático.


- Núcleo administrativo
- Suporte do servidor (agentes)
- Navegadores
- Banco de dados
- Microsoft Data Access Components (MDAC)
- Uso da porta


## Núcleo administrativo

O núcleo administrativo oferece suporte aos seguintes sistemas operacionais:

- Microsoft Windows 2000 Server (com SP4)
- Microsoft Windows 2000 Advanced Server (com SP4)
- Microsoft  Windows 2003 Server Standard Edition (com SP1)
- Microsoft  Windows 2003 Server Enterprise Edition (com SP1)

## Suporte do servidor (agentes)

- Microsoft Windows 2000 Server (com SP4)
- Microsoft Windows 2000 Advanced Server (com SP4)
- Microsoft Windows 2000 Professional (com SP4)
- 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 – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (ES) 32 bits – U3
- Red Hat Enterprise Linux v4 (ES) EM64t – U3
- Red Hat Enterprise Linux v4 (WS) 32 bits – U3
- Red Hat Enterprise Linux v4 (WS) EM64t – U3

- 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

## Navegadores

- Microsoft Internet Explorer 6.x (com SP1)
- Mozilla 1.7 ou posterior
- Firefox 1,5 e posterior

## Banco de dados

- MSDE (com SP4)

## Microsoft Data Access Components (MDAC)

- MDAC 2.8 ou posterior

Se você desejar que mais que um produto de gerenciamento LANDesk utilize o mesmo banco de dados, instale os dois produtos no mesmo computador "núcleo". Da mesma forma, se desejar instalar vários produtos no mesmo computador "núcleo", você deve usar o mesmo banco de dados. Se os dois produtos usarem o mesmo banco de dados, eles devem também ser da versão 8.70.

## Uso da porta

### 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 genéricas 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 |
| 9595, 9594 | console para dispositivo | TCP | Configuração do servidor |
| 9595 | console para dispositivo | UDP | descoberta |
| 623 | console para dispositivo | UDP | descoberta de ASF, IPMI |
| 5007 | console para dispositivo | TCP | inventário |
| 9535 | console para dispositivo | TCP | controle remoto |
| 139, 145 | console para dispositivo | TCP | compartilhamento de arquivos e impressoras |
| 137, 138 | console para dispositivo | UDP | compartilhamento de arquivos e impressoras |

Este produto precisa descobrir nós com o agente de gerenciamento padrão 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).

# Apêndice B: Ativação do servidor núcleo

Antes de poder usar o console você deverá primeiramente ativar o seu servidor núcleo, com o utilitário de Ativação do servidor núcleo. Normalmente este é um procedimento que precisa ser executado somente uma vez, e somente precisa ser repetido se forem compradas licenças adicionais . Use o utilitário de Ativação do servidor núcleo para:

- Ativar um novo servidor pela primeira vez.
- Atualizar um servidor núcleo  ou fazer upgrade para Management Suite ou Server Manager.
- Ativar um novo servidor com uma licença de avaliação de 45 dias.

Inicie o utilitário clicando em **Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**. Se o seu servidor núcleo não tiver uma conexão com a Internet, consulte "Ativar um núcleo ou verificar os dados de contagem de nós manualmente", posteriormente nesta seção.

Cada servidor núcleo deve ter um certificado autorizado exclusivo. Não é possível para vários servidores núcleo compartilhar o mesmo certificado de autorização, embora possam verificar a contagem de nós para a mesma conta LANDesk. Este utilitário é executado automaticamente na primeira reinicialização após instalar o System Manager.

Periodicamente, o servidor núcleo gera informações de verificação de contagem de nós no 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.  Se o núcleo não estiver conectado, clique em **Fechar** na reinicialização e envie o arquivo de autorização por email para licensing@landesk.com.

O Utilitário de ativação do servidor núcleo não lança automaticamente conexões de discagem da Internet, mas se você lançar a conexão de discagem manualmente e executar o utilitário de ativação, ele pode usar essa conexão para fazer relatórios de dados de uso.

Se o seu servidor não tiver conexão de Internet, você pode verificar e enviar a contagem de nó manualmente, conforme descrito nesta seção.

## Ativação de um servidor com a conta da LANDesk Software

Antes de poder ativar um novo servidor com uma licença plena, você deve configurar uma conta com a LANDesk Software, que lhe fornece as licenças adquiridas para os produtos da LANDesk Software, e para o número de nós para os quais você tenha adquirido licenças. São necessárias

as informações de conta (nome de contato e senha) para ativar seu servidor. Se você não tiver essas informações, contate o seu representante de vendas da LANDesk Software.

Não mude a data ou o horário do servidor núcleo entre a instalação do produto e a ativação do núcleo. Haverá falha da ativação. Você terá de desinstalar e reinstalar o produto.

**Para ativar um servidor**

1. Clique em **Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**.
2. Clique em **Ativar**.

## Ativar um servidor com uma licença de avaliação

A licença temporária de 45 dias ativa seu servidor no servidor de licenciamento da LANDesk Software. Uma vez esgotado o período de avaliação de 45 dias, você não conseguirá fazer logon no servidor núcleo, e o servidor irá parar de aceitar varreduras de inventário, mas você não perderá nenhum dos dados existentes no software ou no banco de dados. Durante ou após os 45 dias de validade da licença de avaliação, você pode executar novamente o utilitário de Ativação do servidor núcleo e mudar para a ativação plena que utiliza uma conta da LANDesk Software. Se a licença de avaliação já estiver vencida, uma mudança para uma licença plena irá reativar o núcleo.

**Para ativar uma avaliação de 45 dias**

1. Clique em **Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**.
2. Clique em **Ativar este núcleo para uma avaliação de 45 dias**.
3. Clique em **Avaliar**.

## Atualização de uma conta existente

A opção de atualização envia as informações de uso para o servidor de licenciamento da LANDesk Software.  Os dados da utilização são enviados automaticamente se você tiver uma conexão com a Internet, portanto normalmente você não precisa usar esta opção para enviar a verificação da contagem de nós. Você também pode usar esta opção para mudar o servidor núcleo associado à conta da LANDesk Software. Esta opção também pode ser usada para mudar um servidor núcleo da licença de avaliação para a licença plena.

**Para atualizar uma conta existente**

1. Clique em **Iniciar | Todos os programas | LANDesk | Ativação do servidor núcleo**.
2. Clique em **Atualizar este servidor núcleo usando o nome do contato e a senha da LANDesk**.
3. Digite o **Nome do contato** e a **Senha** que desejar que o núcleo utilize. Se você digitar um nome e senha diferentes daqueles usados originalmente para ativar o núcleo, o núcleo será mudado para uma nova conta.
4. Clique em **Ativar**.

# Ativação manual de um núcleo ou verificação manual dos dados de contagem de nós

Se o servidor núcleo não dispor de uma conexão com a Internet, o utilitário de Ativação do servidor núcleo não poderá enviar os dados da contagem de nós. Você verá uma mensagem lhe pedindo para enviar os dados de verificação de contagem de nós 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 nós**

1. Quando o núcleo pedir para verificar manualmente os dados da contagem de nós, 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 "\Arquivos de programas\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.

# Apêndice C: Configurar serviços

Você pode usar o miniaplicativo Configurar serviços do !ServerName! para configurar os seguintes serviços para qualquer dos seus servidores núcleo e banco de dados:

- Seleção de um banco de dados e um servidor núcleo
- Configuração do serviço de Inventário
- Configuração do tratamento de nomes de dispositivos duplicados
- Configuração do tratamento de IDs de dispositivos duplicados
- Configuração do serviço de agendador
- Configuração do serviço de trabalhos personalizados
- Configuração do serviço de multidifusão
- Configuração da senha do BMC
- Configuração da senha da tecnologia Intel AMT

Para abrir o miniaplicativo Configurar serviços, no servidor núcleo, clique em **Iniciar | Arquivos de programas | LANDesk | LANDesk Configurar Serviços**.

Dois botões são mostrados fora das guias:

- **Credenciais:** Abre a caixa de diálogo Credenciais do servidor, na qual é possível acrescentar dispositivos que podem agir como servidores preferenciais. Para adicionar um dispositivo, clique em **Adicionar**. Isso abre a caixa de diálogo **Nome de usuário e senha** (segue descrição a seguir).
- **Validation OSD:** Para criar ambientes de pré-inicialização com base no Windows PE- ou DOS, é necessário fornecer acesso aos CDs de instalação do Windows PE 2005 e Windows NT 4. Clique em **Validar agora** em ambos os ambientes de imagem, digite o caminho ao CD correto e clique em **OK**.

## Caixa de diálogo Nome de usuário e senha

Use a caixa de diálogo **Nome de usuário e senha** para fornecer informações sobre o servidor preferencial que quiser adicionar.

**Para digitar as informações do servidor preferencial**

1. No miniaplicativo Configurar serviços, clique em **Credenciais**.
2. Na caixa de diálogo Credenciais do servidor, clique em **Adicionar**.
3. Digite uma descrição, as informações de autenticação e as faixas do endereço IP.
4. Clique em **Testar credenciais** para confirmar a validade das suas informações.
5. Clique em **OK** para acrescentar o servidor preferencial à caixa de diálogo Credenciais do servidor.

- **Nome do servidor:** O nome do servidor preferencial.
- **Nome de usuário:** O nome de usuário usado para autenticar no servidor. Este deve ser um nome de domínio totalmente qualificado (por exemplo, Meudomínio\nome do usuário).
- **Descrição:** Uma descrição do servidor preferencial.
- **Senha:** A senha do servidor preferencial.

- **Endereço IP inicial:** Digite o endereço IP iniciar do intervalo de endereços ao qual quiser limitar o uso do servidor preferencial. O endereço IP inicial não deve ser maior que o endereço IP final. Os primeiros três octetos dos endereços IP inicial e final devem coincidir como, por exemplo, 10.100.10.1 e 10.100.10.255.
- **Endereço IP inicial:** digite o endereço IP final do intervalo de endereços a ser analisado.
- **Adicionar:** adiciona os intervalos de endereços IP à fila de trabalho, na parte inferior do diálogo.
- **Excluir:** remove o intervalo de endereços IP selecionado da fila de trabalho.

# Configuração das guias de serviços

Antes de configurar um serviço, use a guia **Geral** para especificar o servidor núcleo e o banco de dados para os quais o serviço será configurado.

**Nota:** Qualquer mudança de configuração de serviço feita para um banco de dados e um servidor núcleo não terá efeito até que o serviço seja reiniciado no servidor núcleo.

## Seleção de um banco de dados e um servidor núcleo

A guia **Geral** permite selecionar um banco de dados e um servidor núcleo e fornece as credenciais de autenticação para que você possa configurar serviços para esse servidor núcleo.

### Sobre a caixa de diálogo Configurar serviços: Guia Geral

Use essa caixa de diálogo para selecionar o banco de dados e o servidor núcleo para os quais o serviço será configurado. Em seguida, selecione a guia do serviço e especifique as configurações para esse serviço.

- **Nome do servidor:** Mostra o nome do servidor núcleo ao qual você está conectado.
- **Servidor:** Permite digitar o nome de um outro servidor núcleo e seu diretório de banco de dados.
- **Banco de dados:** Permite digitar o nome do banco de dados núcleo.
- **Nome do usuário:** Identifica um usuário com credenciais de autenticação para o banco de dados núcleo (especificadas durante a Configuração).
- **Senha:** Identifica a senha do usuário necessária para acessar o banco de dados núcleo (especificada durante a Configuração).
- **Este é um banco de dados Oracle:** Indica que o banco de dados núcleo especificado é um banco de dados Oracle. (Não se aplica ao System Manager.)
- **Atualizar configurações:** Restaura as configurações que estavam em vigor quando a caixa de diálogo Configuração de serviços foi aberta.

## Configuração do serviço de Inventário

Use a guia **Inventário** para configurar o Serviço de inventário para o servidor núcleo e o banco de dados selecionados com a guia Geral.

# Sobre a caixa de diálogo Configurar serviços: guia Inventário

Use essa guia para especificar as seguintes opções de inventário:

- **Nome do servidor**: Mostra o nome do servidor núcleo ao qual você está conectado.
- **Estatísticas de log**: Mantém um log de ações e estatísticas do banco de dados núcleo.
- **Dados criptografados de transporte:** Habilita a análise de inventário a enviar dados de inventário do dispositivo analisado de volta para o servidor núcleo como dados criptografados através de SSL.
- **Analisar servidor em**: Especifica a hora em que o servidor núcleo será analisado.
- **Realizar manutenção em**: Especifica a hora da manutenção padrão do banco de dados núcleo.
- **Dias a manter as varreduras de inventário**:  Define o número de dias antes que o registro de análise do inventário seja excluído.
- **Logins do proprietário principal**:  Define o número de vezes em que a varredura de inventário acompanhará os inícios de sessão para determinar o proprietário principal de um dispositivo. O proprietário principal é o usuário que iniciou mais sessões dentro deste número específico de inícios de sessão. O valor padrão é 5 e os valores mínimo e máximo são 1 e 16, respectivamente. Se cada início de sessão for diferente do anterior, o último usuário a iniciar uma sessão será considerado o proprietário principal. Um dispositivo pode ter apenas um proprietário principal associado a ele por vez. Os dados de início de sessão do usuário principal incluem o nome totalmente qualificado do usuário no formato ADS, NDS, nome de domínio ou nome local (nessa ordem), além da data do último início de sessão.
- **Configurações avançadas:** Abre a caixa de diálogo **Configurações avançadas** onde é possível definir vários diferentes parâmetros avançados relacionados à análise do inventário. Para mudar uma configuração, clique nela, mude-a na caixa de texto **Valor**, em seguida clique em **Configurar**. Para ver uma descrição de uma configuração, clique na mesma e veja os detalhes na caixa de diálogo **Descrição**.
- **Software:** Abre a caixa de diálogo **Configurações da análise de software** onde é possível configurar a hora da análise do software do servidor e as definições de histórico.
- **Atributos:** Abre a caixa de diálogo Selecionar os atributos a serem armazenados onde é possível selecionar os atributos de análise de inventário armazenados no banco de dados.
- **Gerenciar duplicados: Dispositivos**: Abre a caixa de diálogo Configuração de tratamento de nome duplicado de dispositivo, onde é possível escolher uma opção para remover dispositivos com nomes duplicados, endereços MAC ou ambos (consulte **Dispositivos duplicados**, a seguir).
- **Gerenciar duplicados: IDs de dispositivo:**Abre a caixa de diálogo **ID de dispositivos duplicados**, na qual é possível selecionar atributos que identificam exclusivamente os clientes. Você pode usar essa opção para evitar a necessidade de duplicar IDs de dispositivos analisados no banco de dados núcleo (consulte  Configuração do tratamento de IDs de dispositivos duplicados abaixo).
- **Status do serviço de inventário**:lindica se o serviço está iniciado ou parado no servidor núcleo.
- **Iniciar**: Inicia o serviço no servidor núcleo.
- **Parar**:linterrompe o serviço no servidor núcleo.

## Sobre o diálogo Configurações de análise de software.

Use essa caixa de diálogo para configurar a freqüência das análises de software. O hardware de um dispositivo é analisado sempre que é executada a varredura de inventário no dispositivo, mas o software do dispositivo é analisado somente no intervalo especificado aqui.

- **A cada login:** Faz a análise de todo o software instalado no dispositivo cada vez que o usuário fizer logon.
- **Uma vez a cada (dias):** Faz a análise do software do dispositivo somente no intervalo de dias especificado, como uma análise automática.
- **Salvar histórico (dias):** Especifica o tempo durante o qual o histórico de inventário do dispositivo ficará gravado.

## Configuração do tratamento de nomes de dispositivos duplicados

Use a caixa de diálogo Dispositivos duplicados para excluir dispositivos do banco de dados.

1. Na guia Inventário, clique em **Dispositivos**.
2. Na caixa de diálogo Dispositivos duplicados, clique na opção que quer usar ao excluir dispositivos duplicados, em seguida, clique em **OK**.

   **Remove duplicado quando:**
   - **Correspondência de nomes de dispositivos:** Remove o registro antigo quando dois ou mais nomes de dispositivos corresponderem no banco de dados.
   - **Correspondência de endereço MAC:** Remove o registro antigo quando dois ou mais endereços MAC corresponderem no banco de dados.
   - **Correspondência de nomes e endereços MAC:**Rremove o registro antigo SOMENTE quando dois ou mais nomes e endereços MAC de dispositivos correspondem (no mesmo registro).

## Configuração do tratamento de IDs de dispositivos duplicados

Como as imagens são freqüentemente usadas para configurar dispositivos em uma rede, a possibilidade de haver IDs de dispositivos duplicados entre os dispositivos é maior. Esse problema pode ser evitado especificando outros atributos exclusivos de dispositivos que, combinados com o ID do dispositivo, criam um identificador exclusivo para os dispositivos. Exemplos desses outros atributos são o nome do dispositivo, o nome do domínio, BIOS, barramento, coprocessador, etc.

O recurso de ID duplicado permite selecionar atributos de dispositivos que possam ser usados para identificar exclusivamente o servidor. Especifique quais são esses outros atributos e quantos deles devem estar ausentes antes de o dispositivo ser designado como uma duplicação de um outro dispositivo. Se a varredura de inventário não puder detectar um dispositivo duplicado, ela gravará um evento no log de eventos de aplicativos para indicar o ID do dispositivo duplicado. O diálogo ID de dispositivo duplicado contém as seguinte opções:

- **Lista de atributos:** Contém todos os atributos que podem ser selecionados para identificar exclusivamente um dispositivo.
- **Atributos de identidade:** Mostra os atributos selecionados para identificar exclusivamente um dispositivo.
- **Ativações de ID de dispositivo duplicado:**
  - **Atributos de identidade:** Identifica o número de atributos que um dispositivo não deve encontrar antes de ser considerado uma duplicação de outro dispositivo.
  - **Atributos de hardware:** Identifica o número de atributos de hardware que um dispositivo não deve encontrar antes de ser considerado uma duplicação de outro dispositivo.
- **Rejeitar identidades duplicadas:** Faz com que a varredura de inventário registre o ID do dispositivo duplicado e rejeite todas as tentativas subseqüentes de analisar esse ID de dispositivo. Em seguida, a varredura de inventário gera um novo ID de dispositivo.

**Para configurar o tratamento de IDs duplicados:**

1. Na caixa de diálogo Configurar serviços, clique na guia **Inventário**, em seguida, clique em **IDs do dispositivo**.
2. Selecione os atributos na **Lista de atributos** que deseja usar para identificar exclusivamente um dispositivo e, em seguida, clique na seta para a direita para adicionar o atributo à lista **Atributos de identidade**. Você pode adicionar quantos atributos desejar.
3. Selecione o número de atributos de identidade (e atributos de hardware) que um dispositivo não deve encontrar antes de ser considerado uma duplicação de outro dispositivo.
4. Se quiser que a varredura de inventário rejeite os IDs de dispositivos duplicados, marque a opção **Rejeitar identidades duplicadas**.

# Configuração do serviço do Planejador

Use a guia **Agendador** para configurar o serviço agendador para o servidor núcleo e o banco de dados selecionados usando a guia **Geral**. É necessário ter os direitos corretos para realizar essas tarefas, inclusive privilégios totais de administrador para gerenciar dispositivos, permitindo que recebam distribuições de pacotes do System Manager. Você pode especificar credenciais múltiplas de login para usar nos dispositivos clicando em **Alterar login**.

## Sobre a caixa de diálogo Configurar serviços: guia Agendador

Use essa guia para ver o nome do banco de dados e do servidor núcleo selecionado anteriormente e para especificar as seguintes opções de Tarefas agendadas:

- **Nome do usuário**: O nome do usuário no qual o serviço Tarefas agendadas será executado. Essa definição pode ser alterada clicando no botão **Alterar login**.
- **Número de segundos entre as novas tentativas**: Quando uma tarefa agendada é configurada com várias novas tentativas, essa configuração controla o número de segundos que o serviço Tarefas agendadas irá aguardar antes de tentar executar a tarefa novamente.

- **Número de segundos para tentar ativar**: Quando uma tarefa agendada é configurada para usar Wake On LAN, essa configuração controla o número de segundos que o serviço Tarefas agendadas irá aguardar pela ativação de um dispositivo.
- **Intervalo entre as avaliações da consulta**: Um número que indica o tempo entre as avaliações de consultas e uma unidade de medida para o número (minutos, horas, dias ou semanas).
- **Configurações de Wake on LAN**: A Porta IP que será usada pelo conjunto de pacotes Wake On LAN para que o serviço Tarefas agendadas ative os dispositivos.
- **Status do serviço de agendamento**: Indica se o serviço está iniciado ou parado no servidor núcleo.
- **Iniciar**: Inicia o serviço no servidor núcleo.
- **Parar**: Interrompe o serviço no servidor núcleo.
- **Reiniciar:** Reinicia o serviço no servidor núcleo.
- **Avançada:** Abre a caixa de diálogo **Configurações avançadas do agendador**, onde é possível modificar as configurações controlando a maneira como o agendador vai funcionar. Para mudar uma configuração, clique na mesma, clique em **Editar**, mude a configuração e clique em **OK**.

## Sobre a caixa de diálogo Configurar serviços: Caixa de diálogo Alterar login

Use a caixa de diálogo **Alterar login** (clique em **Alterar login** na guia **Planejador**) para mudar o login padrão do planejador. Você também pode especificar credenciais alternativas que o serviço do planejador deve tentar quando precisar executar uma tarefa em dispositivos não gerenciados.

Para instalar os agentes System Manager em dispositivos não gerenciados, o serviço do agendador precisa poder conectar-se aos dispositivos com uma conta administrativa. A conta padrão que o serviço do planejador utiliza é LocalSystem. As credenciais LocalSystem geralmente funcionam com dispositivos que não estão em um domínio. Se os dispositivos estão em um domínio, é necessário especificar um conta de administrador de domínio.

Se desejar mudar as credenciais de login do serviço do planejador, você pode especificar uma conta administrativa a nível de domínio diferente para usar nos dispositivos. Se estiver gerenciando dispositivos em vários domínios, adicione credenciais adicionais para o serviço do planejador tentar. Se quiser usar uma conta diferente da LocalSystem para o serviço do agendador ou se quiser fornecer credenciais alternativas, é necessário especificar um login de serviço de agendador primário que tenha direitos administrativos no servidor núcleo. As credenciais alternativas não requerem direitos administrativos no servidor núcleo, mas devem ter direitos administrativos nos dispositivos.

O serviço do agendador experimentará as credenciais padrão, em seguida usará cada credencial que você especificou na lista **Credenciais alternativas** até conseguir ou terminarem as credenciais. As credenciais que você especificar são criptografadas com segurança e armazenadas no registro do servidor núcleo.

Você pode definir as seguintes opções para as credenciais do agendador padrão:

- **Nome do usuário:** Digite o domínio\nome de usuário padrão ou o nome do usuário que quiser que o planejador use.
- **Senha:** Digite a senha para as credenciais que especificou.

- **Confirmar senha:** Redigite a senha para confirmá-la.

Você pode definir as seguintes opções para as credenciais adicionais do agendador:

- **Adicionar:** Clique para adicionar o nome de usuário e a senha que especificou à a lista de Credenciais alternativas.
- **Remover:** Clique para remover as credenciais selecionadas da lista.
- **Modificar:** Clique para mudar as credenciais selecionadas.

Ao adicionar credenciais alternativas, especifique o seguinte:

- **Nome do usuário:** Digite o nome de usuário que quiser que o planejador use.
- **Domínio:** Digite o domínio do nome de usuário que especificou.
- **Senha:** Digite a senha para as credenciais que especificou.
- **Confirmar senha:R**redigite a senha para confirmá-la.

## Configuração do serviço trabalhos personalizados

Use a guia **Trabalhos personalizados** para configurar o serviço trabalhos personalizados para o servidor núcleo e o banco de dados selecionados na guia Geral. Exemplos de trabalhos personalizados incluem varreduras de inventário ou distribuição de software.

Quando o TCP é desabilitado como o protocolo de execução remota, o serviço Trabalhos personalizados usa o protocolo agente de Gerenciamento padrão como padrão, esteja ele marcado ou não como desabilitado. Além disso, se ambos os agentes de execução remota TCP e agente de gerenciamento padrão forem habilitados, o serviço Trabalhos personalizados tentará usar primeiro o protocolo TCP de execução remota e se este não estiver disponível, será usado o protocolo agente de produto padrão de execução remota.

Os **Trabalhos personalizados** também o habilitam a escolher opções para a descoberta de servidor. Antes do serviço trabalhos personalizados poder processar um trabalho, é necessário descobrir o endereço IP de cada servidor. Esta guia permite configurar a forma como o serviço contata os servidores.

## Sobre a caixa de diálogo Configurar serviços: guia Trabalhos personalizados

Use essa guia para definir as seguintes opções de Trabalhos personalizados:

**Opções de execução remota:**

- **Desabilitar execução de TCP**: Desativa o TCP como protocolo de execução remota utilizando, por isso, o protocolo CBA por padrão.
- **Desabilitar execução/transferência de arquivos via CBA**: Desabilitar o agente de gerenciamento padrão como o protocolo de execução remota. Se o agente de gerenciamento padrão for desabilitado e o protocolo TCP de execução remota não for localizado no dispositivo, a execução remota não ocorrerá.

- **Habilitar o tempo limite de execução remota**: Habilita um tempo limite de execução remota e especifica o número de segundos após os quais o tempo limite irá ocorrer. Os tempos limites de execução remota são ativados quando o dispositivo envia pacotes espaçados, mas o trabalho no dispositivo está suspenso ou em loop. Essa configuração aplica-se aos dois protocolos (TCP ou Agente de gerenciamento padrão). Esse valor pode variar entre 300 segundos (5 minutos) e 86.400 segundos (1 dia).
- **Habilitar o tempo limite de um cliente**: Habilita o tempo limite de um dispositivo e especifica o número de segundos após os quais o tempo limite irá ocorrer. Como padrão, o TCP de execução remota envia um pacote do dispositivo para o dispositivo em intervalos de 45 segundos até que a execução remota seja concluída ou o seu tempo limite seja atingido. Os tempos limites de clientes são ativados quando o dispositivo não envia uma pulsação ao dispositivo.
- **Porta de execução remota (o padrão é 12174)**: A porta pela qual ocorre o TCP de execução remota. Se essa porta for mudada, ela também deverá ser mudada na configuração do cliente.

**Opções de distribuição:**

- **Distribuir a <nn> servidores simultaneamente**:Oo número máximo de dispositivos aos quais o trabalho personalizado será distribuído simultaneamente.

**Opções de descoberta:**

- **UDP:** A seleção do UDP usa um agente ping de gerenciamento padrão via UDP. A maioria dos componentes do System Manager depende do agente de gerenciamento padrão, então os seus dispositivos gerenciados devem ter o agente de gerenciamento padrão neles. Este é o método de descoberta mais rápido e o padrão. Com UDP, você pode também selecionar **Novas Tentativas** e **Tempo limite** de ping UDP.
- **TCP:** A seleção de TCP usa uma conexão HTTP para o servidor na porta 9595. Esse método de descoberta oferece o benefício de ser capaz de funcionar através de uma firewall se você abrir a porta 9595, mas está sujeito a tempos limites de conexão de HTTP se os dispositivos não estiverem presentes. Esses tempos limite podem durar 20 segundos ou mais. Se um grupo de dispositivos alvo não responder à conexão TCP, a sua tarefa levará algum tempo para começar.
- **Ambos:A**a seleção de Ambos faz o serviço tentar a descoberta com UDP primeiro, em seguida, o TCP e por último DNS/WINS, se tiver sido selecionado.
- **Desabilitar transmissão de sub-rede:** Quando selecionada, esta opção desabilita a descoberta via difusão de sub-rede.
- **Pesquisa DNS/WINS) Desabilitar:** Quando selecionada, esta opção desabilita uma pesquisa de serviço de nomes para cada dispositivo se o método de descoberta TCP/UDP falhar.

## Configuração do serviço de multidifusão

Use a guia **Multidifusão** para configurar as opções de descoberta do representante do domínio multidifusão para o banco de dados e para o servidor núcleo selecionado com a guia **Geral**.

## Sobre a caixa de diálogo Configurar serviços: guia Multidifusão

Use essa guia para definir as seguintes opções de multidifusão:

- **Usar o representante de domínio de multidifusão:U**utiliza a lista de representantes de domínio de multidifusão armazenados no grupo **Configuração > Representantes de domínio de multidifusão** na tela da rede.
- **Usar arquivo em cache:** Consulta cada domínio de multidifusão para descobrir quem pode já ter feito cache do arquivo. O arquivo em cache pode, assim, ser usado em lugar do download do arquivo para um representante.
- **Usar arquivo em cache antesdo representante do domínio preferencial:** Muda a ordem de descoberta para que a opção **Usar arquivo em cache** seja a primeira selecionada.
- **Usar transmissão:** Envia uma transmissão direcionada a sub-rede para localizar qualquer dispositivo nessa sub-rede que possa ser um representante de domínio de multidifusão.
- **Período de descarte de log (dias):** Especifica onúmero de dias que as entradas no log serão retidas antes de serem excluídas.

## Configuração da senha do BMC

Use a guia **Senha BMC** para criar uma senha para o BMC (Baseboard Management Controller) IPMI.

- 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 ter mais que 15 caracteres, e cada um deles deve ser um número entre 0 e 9 ou letras maísculas/minúsculas de a a z.

## Configuração das opções Intel AMT

Use a guia **Configuração da Intel AMT** para criar ou mudar a senha em dispositivos habilitados com a tecnologia Intel AMT (Tecnologia de gerenciamento ativo) e ver as instruções para descoberta dos dispositivos AMT.

**Para configurar a senha da tecnologia Intel AMT**

1. Digite o nome de 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

**Descoberta e configuração dos dispositivos Intel AMT**

Para descobrir dispositivos AMT, digite o endereço IP do Servidor núcleo no campo Servidor de configuração do BIOS AMT e use a porta 9982. Pressione **Ajuda** em **Configurar serviços** para mais informações. Quando um dispositivo Intel AMT é descoberto e transferido para a lista **Meus dispositivos**, ele é automaticamente configurado usando o modo TLS.

# Apêndice D: Segurança de agente e certificados confiáveis

Cada servidor núcleo tem um certificado exclusivo e uma chave privada que são criados pela Instalação quando o console é instalado pela primeira vez o servidor núcleo em um dispositivo. Os dispositivos só se comunicam com os servidores núcleo para os quais eles têm um arquivo de certificado confiável correspondente.

Estes são os arquivos de chave privada e de certificados que são instalados:

- **<nome da chave>.key:** O arquivo .KEY é a chave privada do servidor núcleo e reside apenas no servidor núcleo. Se a privacidade desta chave for comprometida, o servidor núcleo e as comunicações com os servidores não estarão protegidas. Mantenha essa chave protegida. Por exemplo, não a envie por email.
- **<nome da chave>.crt:** O arquivo .CRT contém a chave pública do servidor núcleo. O arquivo .CRT é uma versão da chave pública que pode ser visualizada para se obter mais informações.
- **<hash>.0:** O arquivo .0 é um arquivo de certificado confiável cujo conteúdo é idêntico ao do arquivo .CRT. Mas ele é nomeado de forma que o computador possa localizar rapidamente o arquivo de certificado num diretório com muitos certificados diferentes. O nome é um hash (checksum) das informações do certificado. Para determinar o nome de arquivo hash de um certificado específico, abra o arquivo <nome da chave>.CRT. Existe uma seção [LDMS] no arquivo .INI. O par hash=value indica o valor de <hash>.

Todas as chaves são armazenadas no servidor núcleo em \Arquivos de programas\LANDesk\Shared Files\Keys. A chave pública <hash>.0 está também no diretório LDLOGON e, como padrão, precisar estar ali. <nome da chave> é o nome do certificado que você forneceu durante a instalação do servidor núcleo. É útil fornecer um nome descritivo durante a instalação, por exemplo, você pode utilizar o nome do servidor núcleo (ou mesmo o nome completo dele) para a chave (exemplo: ldcore ou ldcore.org.com). Isso facilitará a identificação dos arquivos de certificado/chave privada em um ambiente com vários núcleos.

## Backup e restauração dos arquivos de certificado/chave privada entre servidores núcleo

Quando um servidor núcleo é instalado, a configuração cria um novo certificado. Mesmo se ele for reinstalado sobre outro servidor núcleo, ainda assim a instalação criará um novo certificado. Se você instalou dispositivos com um certificado que não corresponde ao certificado do novo servidor núcleo, o servidor não conseguirá comunicar-se com eles. Se for necessário reinstalar o servidor núcleo, há duas opções:

1. Reinstalar os agentes do cliente manualmente com uma configuração incorporada no novo servidor núcleo. Não será possível utilizar a distribuição de software para atualizar os agentes, pois o servidor núcleo e os dispositivos não terão o certificado e a chave correspondentes.

2. Antes de reinstalar um servidor núcleo, faça backup dos arquivos de certificado e chave em local seguro. Após ter feito a instalação, copie as chaves antigas para a nova instalação do núcleo. As chaves novas e antigas podem coexistir. O núcleo usa a chave correta automaticamente.

Os núcleos podem conter vários arquivos de certificado/chave pública. Se um cliente puder autenticar-se com uma das chaves em um núcleo, ele poderá comunicar-se com esse núcleo.

Um utilitário é incluído neste produto, que realiza a segunda opção acima listada. O utilitário de migração de dados núcleo (CoreDataMigration.exe) é instalado na pasta \Arquivos de programas\LANDesk\ManagementSuite. Ele cuida do backup e cópia de dados, como, por exemplo, chaves e certificados quando um novo núcleo é instalado.

**Para salvar e restaurar um conjunto de certificado/chave privada**

1. No servidor núcleo de origem, vá para a pasta \Arquivos de programa\LANDesk\Shared Files\Keys.
2. Copie os arquivos <nome da chave>.key, <nome da chave>.crt, e <hash>.0 do servidor de origem em um disquete ou em outro local seguro.
3. No servidor núcleo de destino, copie os arquivos do servidor núcleo de origem para a mesma pasta (\Arquivos de programas\LANDesk\Shared Files\Keys). As chaves entram em vigor imediatamente.

**Aviso: Mantenha o arquivo da chave privada protegido**
Certifique-se de que a privacidade da chave privada <nome da chave>.key não seja comprometida. Não a transfira por meios desprotegidos como por email ou em um compartilhamento de arquivos público. O servidor núcleo utiliza esse arquivo para autenticar os dispositivos e qualquer computador com o arquivo <nome da chave>.key correto pode realizar execuções remotas e transferência de arquivos para um dispositivo gerenciado.

# Dicas de resolução de problemas

As seguintes dicas de resolução de problemas são para as questões que ocorrem com mais freqüência com o console.

**Não consigo ativar o núcleo.**
Se você instalou o núcleo e depois alterou o horário do dispositivo, não será possível ativá-lo. Será necessário reinstalar o produto para ativar o núcleo.

**Quando tentei ativar o núcleo, apareceu uma mensagem de falha de leitura do banco de dados do servidor núcleo.**
Verifique se o servidor núcleo está fisicamente conectado à rede e se tem uma conexão válida à internet. Se um cabo estiver desconectado ou a conexão do servidor núcleo à internet não for válida, o processo de ativação não pode ser completado.

**Não sei o URL das páginas do console.**
Entre em contato com a pessoa que instalou o servidor núcleo, provavelmente o administrador da rede de seu site. No entanto, o URL típico para o Server Manager e o System Manager é http:// *nome do servidor núcleo*/ldsm. O URL do Management Suite é http://*nome do computador do servidor núcleo*/remoto.

**Como estou conectado?**
Olhe acima da barra e abaixo do nome LANDeskSystem Manager, na seção **Conectado como**.

**A que máquina estou conectado?**
Olhe acima da barra e abaixo do nome LANDeskSystem Manager, na seção **Conectado a**.

**Inicio o System Manager e imediatamente aparece uma mensagem "Tempo de espera de sessão esgotado".**
Se você abrir o System Manager a partir do menu Favoritos ou Marcadores com a extensão "/frameset.asp" no final do URL, ele não será inicializado corretamente. Para resolver o problema, edite o link do Marcador ou Favoritos para remover a extensão, ou cole o URL (sem a extensão) diretamente na janela do navegador.

**Não estou vendo alguns dos links no painel de navegação à esquerda.**
Isso ocorre porque o seu administrador de rede está usando a opção de segurança a nível de recursos ou administração com base em função do LANDeskSystem Manager que limita a sua execução de certas tarefas às quais você teria direitos.

**O analisador não consegue conectar-se ao dispositivo.**
Se o analisador não conectar-se ao dispositivo, verifique se o diretório de aplicativos Web está configurado corretamente. Se estiver usando https, é necessário um certificado válido. Verifique se você tem um certificado válido.

**Recebo um erro de "permissão negada" quando tento acessar o console**.
Para usar segurança a nível de recursos no Windows 2000 e 2003, você deve desativar a autenticação anônima. Verifique as configurações de autenticação no site da Web e a pasta ..\LANDesk\ldsm no site da Web.

1. No servidor que é o host do Web console, clique em **Iniciar | Ferramentas administrativas | Gerenciador dos serviços de informações da internet (IIS)**.

2. No menu de atalho do **Site da web padrão** , clique em **Propriedades**.
3. Na guia **Segurança de diretório**, clique em **Editar** na caixa **Acesso anônimo e controle de autenticação.** Limpe a opção **Ativar acesso anônimo** e selecione **Autenticação integrada do Windows**.
4. Clique em **OK** para sair dos diálogos.
5. Na sub-pasta .\LANDesk\ldsm do site da web padrão, clique em **Propriedades**. Repita os passo 3-4.

**Sessão inválida aparece ao utilizar o console.**
É possível que a sessão do navegador tenha expirado. Use o botão **Atualizar** do navegador para iniciar uma nova sessão.

**Aparece um erro de ASP.NET quando eu tento iniciar o Web console.**
Se aparecer uma mensagem de erro do ASP.NET ao tentar acessar o Web console, as permissões do ASP e do diretório ASP podem não estar configuradas corretamente. Redefina a configuração de ASP.NET executando o seguinte comando:

```
ASPNET_REGIIS.EXE -i
```

**O número de itens por página é diferente do número que especifiquei.**
Quando você especifica quantos itens devem ser exibidos por página, esta configuração é armazenada no diretório de cookies do navegador da web e vence quando expira o tempo limite da sessão.

**A sessão do console expira muito freqüentemente.**
É possível mudar o tempo limite padrão da sessão para as páginas de web do console. O padrão do IIS é 20 minutos de inatividade antes de um login expirar. Para mudar o tempo limite da sessão IIS:

1. No servidor web, abra o Gerenciador de serviços IIS Internet.
2. Expanda o site padrão.
3. Clique com o botão direito do mouse na pasta **LDSM** e clique em **Propriedades**.
4. Na guia **Diretório virtual**, clique em **Configuração**.
5. Clique na guia **Opções de aplicativos** e, em seguida, altere o tempo limite da sessão para o valor desejado.

**Nota:**LANDeskSystem Manager8.70 é um produto com base em sessão. Não desabilita o estado da sessão.

**Os gráficos do relatório não são exibidos corretamente.**
Para ver os gráficos interativos de barras e de pizza exibidos em vários relatórios é necessário instalar o Macromedia Flash Player* 7. Verifique se o Flash está instalado, em seguida, execute o relatório novamente.

**Por que vejo duas instâncias do mesmo dispositivo no meu banco de dados?**
Você excluiu um dispositivo do banco de dados núcleo e o reinstalou usando o UninstallWinClient.exe?

O UninstallWinClient.exe se encontra no compartilhamento LDMain, que é a principal pasta de programas do ManagementSuite. Apenas os administradores têm acesso a esse compartilhamento. Este programa desinstala os agentes do LANDesk em qualquer dispositivo

em que é executado. Você pode mudá-lo para qualquer pasta que quiser ou adicioná-lo a um script de login. É um aplicativo Windows que é executado silenciosamente sem exibir nenhuma interface. Você pode ver duas instâncias do dispositivo 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. Consulte o *Guia de distribuição* para obter mais informações sobre o UninstallWinClient.exe.

**Quanto tento descobrir um dispositivo IPMI, o mesmo não está listado na pasta IPMI da página de dispositivos Não gerenciados.**
Os dispositivos IPMI devem ter um BMC (baseboard management controller) configurado, para serem descobertos como dispositivos IPMI e usar completa funcionalidade IPMI. Se o BMC não estiver configurado, o dispositivo pode ser descoberto como computador. Você poderá, então, acrescentar o dispositivo à lista de dispositivos gerenciados e executar o utilitário Configurar Serviços para configurar a senha BMC. A funcionalidade do IPMI do dispositivo será, então, reconhecida por este produto.

**Acrescentei uma unidade S.M.A.R.T. em um servidor, mas não vejo a monitoração da unidade S.M.A.R.T. na lista de inventário para aquele servidor.**
A monitoração de hardware depende das capacidades do hardware instalado em um dispositivo, assim como da correta configuração do hardware. Se um disco rígido com capacidades de monitoração S.M.A.R.T. for instalado em um dispositivo mas a detecção S.M.A.R.T. não for habilitada nas configurações do BIOS do dispositivo, ou se o BIOS do dispositivo não suportar unidades S.M.A.R.T., os dados de monitoração não estarão disponíveis e não serão gerados alertas resultantes.

**Dispositivos disco USB não são incluídos na lista de inventário até que a análise seja executada.**
Quando o dispositivo de disco é conectado com um cabo USB a um dispositivo gerenciado, ele não é incluído imediatamente sob os Discos rígidos no inventário do dispositivo. Ele é incluído sob as unidades lógicas após serem conectados ao dispositivo. Entretanto, ele não aparece em Disco rígidos até que seja feita uma análise de inventário no dispositivo.

Nos dispositivos Linux gerenciados, os discos USB devem ser montados par poderem aparecer no inventário. Se ele for montado e não for feita uma análise de inventário, ele aparecerá sob os Unidade lógicas; após a análise de inventário eles serão incluídos também na lista de Discos rígidos. Quando o dispositivo é desconhecido ele deve ser desmontado do sistema. Em alguns sistemas Linux com kernel antigo, o dispositivo pode também ficar na lista de inventário mesmo após ter sido desconectado ou desmontado. Nesse caso o dispositivo gerenciado precisa ser reinicializado antes de ser removido da lista de inventário.

**O índice da Ajuda do Web console está em branco.**
A ajuda online HTML do Web console tem um recurso de busca de texto completo que depende do Serviço de índices do Windows. Normalmente esse recurso está habilitado por padrão. Se for necessário habilitar índices no servidor Web, faça o seguinte:

1. Clique em **Iniciar | Programas | Ferramentas Administrativas | Serviços**.
2. Clique duas vezes em **Serviço de índices** e clique em **Iniciar**.
3. Clique em **OK** para sair das caixas de diálogo.

A indexação do seu servidor pelo serviço de índices pode demorar (até várias horas).