ZENworks 2020 Update 1

Inicialização Rápida da Administração

Junho de 2020

Informações legais

Para saber mais sobre informações legais, marcas registradas, isenções de responsabilidade, garantias, exportação e outras restrições de uso, direitos restritos do Governo dos EUA, política de patente e conformidade com FIPS, consulte https://www.novell.com/company/legal/.

As garantias exclusivas para os produtos e serviços da Micro Focus e de suas afiliadas e licenciantes (“Micro Focus”) estão descritas nas declarações de garantia que acompanham esses produtos e serviços. Nenhuma informação nos termos deste documento deve ser interpretada como garantia adicional. A Micro Focus não será responsável por erros técnicos ou editoriais contidos neste documento. As informações constantes neste documento estão sujeitas à mudança sem aviso prévio.

Índice

Sobre este guia

Esta *Inicialização Rápida da Administração do ZENworks*ajuda você a dominar rapidamente os conceitos básicos da administração do seu sistema ZENworks Management. Você já deve ter instalado o sistema ZENworks. Do contrário, consulte a *Instalação do Servidor ZENworks*.

As informações deste guia estão organizadas da seguinte maneira:

- Configuração do sistema (página 9): Apresenta instruções sobre a configuração da Zona de Gerenciamento do ZENworks antes de usar os produtos do ZENworks
- Administração de produtos (página 59): Apresenta instruções sobre o uso dos produtos do ZENworks (Gerenciamento de Bens, Gerenciamento de Configurações, Gerenciamento de Segurança de Endpoint, Criptografia de Disco Cheio e Gerenciamento de Patch).

Público

Este guia destina-se a qualquer pessoa responsável por configurar o sistema ZENworks, monitorar o sistema ZENworks ou executar alguma tarefa do ZENworks relacionada ao gerenciamento de dispositivos ou usuários.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o link *comment on this topic* (comentar sobre este tópico) na parte inferior de cada página da documentação online.

Documentação adicional

O ZENworks é suportado por documentação adicional (nos formatos PDF e HTML), que pode ser utilizada para que você conheça e implemente o produto. Para acessar a documentação adicional, visite o site de documentação do ZENworks na Web (http://www.novell.com/documentation/zenworks-2020).

Configuração do sistema

As seções a seguir apresentam informações sobre como configurar o sistema ZENworks. As tarefas de configuração são aplicadas independentemente do produto do ZENworks que você está usando (Gerenciamento de Configurações, Gerenciamento de Patch, Gerenciamento de Bens e Gerenciamento de Segurança de Endpoint).

1 Lista rápida

Você instalou o Servidor ZENworks (ou até dois servidores) e não vê a hora de começar a usar todas as funcionalidades práticas do ZENworks.

Antes de começar a usar qualquer um dos produtos do ZENworks (Gerenciamento de Configurações, Gerenciamento de Patch, Gerenciamento de Bens, Gerenciamento de Segurança de Endpoint e Criptografia de Disco Cheio) que você adquiriu por meio de licença ou que está avaliando, convém revisar os conceitos e as tarefas das seções a seguir. Estas seções apresentam uma breve introdução sobre o que você precisa saber e fazer para configurar sua Zona de Gerenciamento:

Ferramentas de gerenciamento

O ZENworks dispõe de um console baseado na Web (ZENworks Control Center) e um utilitário de linha de comando (zman) que podem ser usados para gerenciar seus sistema ZENworks. Você deve se familiarizar pelo menos com o ZENworks Control Center.

Tarefa		Detalhes
	Inicie o ZENworks Control Center	Para obter instruções, consulte "ZENworks Control Center" na página 17.
	Descobrir como executar o utilitário zman	O utilitário zman é uma interface de linha de comando que permite realizar muitas das mesmas tarefas do ZENworks Control Center. Para obter instruções, consulte "Utilitário de Linha de Comando zman" na página 19.
	Descobrir como executar o utilitário zac	O utilitário zac é uma interface de linha de comando do Agente do ZENworks. Para obter instruções, consulte "Utilitário de Linha de Comando zac" na página 20.

Configuração de zona

Antes de começar a aproveitar todas as vantagens dos recursos de gerenciamento oferecidos pelos produtos do ZENworks ativados durante a instalação da sua Zona de Gerenciamento, há algumas tarefas de configuração que devem ser concluídas para garantir a configuração correta da Zona de Gerenciamento.

Tarefa		Detalhes
	Criar pastas e grupos para organizar dispositivos	Organize os dispositivos em pastas e grupos para reduzir o overhead envolvido na aplicação das definições de configuração do ZENworks e na execução de tarefas em dispositivos semelhantes. Em vez de fazer atribuições ou executar tarefas em dispositivos individuais, você pode gerenciar as pastas e grupos, com cada dispositivo de uma pasta ou grupo que esteja herdando a atribuição ou a tarefa. Para obter instruções, consulte "Organizando dispositivos: pastas e grupos" na página 23.
	Criar regras ou chaves de registro	O Agente do ZENworks deve ser implantado em cada dispositivo que você deseja gerenciar. Quando você implanta o Agente do ZENworks em um dispositivo, o dispositivo é registrado na zona de gerenciamento. É possível usar chaves de registro ou regras para atribuir automaticamente os dispositivos a pastas ou grupos apropriados, permitindo que os dispositivos herdem imediatamente todas as atribuições associadas às pastas e aos grupos. Para obter instruções, consulte "Criando chaves de registros e regras" na página 27.

Tarefa		Detalhes
	Adicionar origens de usuário	Você pode se conectar a um ou mais diretórios LDAP para fornecer origens de usuário autorizadas no ZENworks. A adição de uma origem de usuário permite associar contas de administrador do ZENworks a contas de usuário LDAP, e associar dispositivos aos usuários que os utilizaram primeiro. Além disso, a adição de usuários proporciona uma funcionalidade extra aos seguintes produtos do ZENworks: ◆ **Gerenciamento de Configurações:** Permite atribuir bundles e políticas a usuários e dispositivos. Habilita os relatórios de inventário baseados no usuário. ◆ **Gerenciamento de Bens:** Permite contabilizar as licenças de software por usuário e por dispositivo. ◆ **Gerenciamento de Segurança de Endpoint:** Permite atribuir políticas a usuários e dispositivos. Para obter instruções, consulte "Conectando-se às origens do usuário" na página 29.
	Criar contas de administrador adicionais	Durante a instalação, é criada uma conta de administrador padrão do ZENworks (chamada Administrador). Essa é uma conta de Superadministrador. Ela possui todos os direitos administrativos dentro da Zona de Gerenciamento. É possível criar contas de administrador adicionais e conceder a elas direitos de Superadministrador. Se preferir, você pode criar contas de administrador com direitos restritos para limitar o escopo do administrador em relação a tarefas, dispositivos e usuários acessíveis. Para obter instruções, consulte "Criando uma conta de administrador" na página 31.

Tarefa		Detalhes
	Criar contas de grupo de administradores	Você pode criar grupos de administradores. Se você atribuir direitos e funções a um grupo de administradores, os direitos e as funções atribuídos serão aplicados a todos os membros do grupo. Para obter instruções, consulte "Criando uma conta de grupo de administradores" na página 31.
	Modificar definições de configuração de zona	As configurações da Zona de Gerenciamento são predefinidas para disponibilizar as configurações mais comuns. Não é necessário mudar nenhuma configuração no momento, mas convém navegar pelas configurações para tornar-se mais familiarizado com elas. Para obter instruções, consulte "Modificando definições de configuração" na página 32.
	Atualizar o Software ZENworks	O recurso Atualizações do Sistema permite que você obtenha·atualizações do software do ZENworks em tempo hábil, além de programar downloads automáticos das atualizações. Para obter instruções, consulte o "Atualizar o Software ZENworks" na página 34.
	Criar Locais	As políticas de segurança podem ser globais ou específicas aos locais. Uma política global é aplicada a todos os locais. Uma política baseada em local é aplicada apenas quando o Agente do ZENworks determina que o ambiente de rede do dispositivo corresponde ao ambiente definido para o local. Para obter instruções, consulte "Criando locais" na página 35.

Implantação de agente

O Agente do ZENworks comunica-se com o Servidor ZENworks para executar tarefas de gerenciamento em um dispositivo. Você deve implantar o Agente do ZENworks em todos os dispositivos que deseja gerenciar. A implantação do Agente do ZENworks instala os arquivos do agente e registra o dispositivo na Zona de Gerenciamento. Para obter mais informações sobre o registro de dispositivos móveis na zona, consulte Registrando dispositivos móveis.

Tarefa		Detalhes
	Habilitar os recursos do Agente do ZENworks	O Agente do ZENworks inclui recursos específicos para cada um dos produtos do ZENworks (Gerenciamento de Bens, Gerenciamento de Configurações, Gerenciamento de Segurança de Endpoint, Criptografia de Disco Cheio e Gerenciamento de Patch). Por padrão, os recursos de seus produtos ativados (licenciados ou de avaliação) são habilitados durante a instalação da Zona de Gerenciamento. No entanto, verifique a configuração no ZENworks Control Center. Para obter instruções, consulte "Configurando recursos do Agente do ZENworks" na página 39.
	Proteger o Agente do ZENworks	É possível configurar as definições de desinstalação e autodefesa do Agente do ZENworks. Para obter instruções, consulte o "Configurando a segurança do Agente do ZENworks" na página 41.
	Instalar o Agente do ZENworks	Você pode usar vários métodos para instalar o Agente do ZENworks em um dispositivo: ◆ Use o ZENworks Control Center para distribuir o agente a partir de um Servidor ZENworks para o dispositivo. ◆ No dispositivo, use um browser da Web para fazer download do agente de um Servidor ZENworks e instalá-lo. ◆ Inclua o agente em uma imagem e aplique-a ao dispositivo. Para obter instruções, consulte "Instalando o Agente do ZENworks" na página 42.
	Efetuar login e usar o Agente do ZENworks	Para receber bundles e políticas atribuídos ao usuário em um dispositivo, efetue login na zona de gerenciamento. Para obter instruções, consulte "Usando o Agente do ZENworks" na página 46.

Mensagens do sistema

À medida que você executa tarefas de gerenciamento na sua zona, as informações são registradas de modo que você possa ver o status da zona e as atividades que ocorrem nela.

Tarefa		Detalhes
	Veja as mensagens do sistema	O sistema ZENworks gera mensagens informativas, de aviso e de erro para ajudá-lo a monitorar atividades, como a distribuição de softwares e a aplicação de políticas. Para obter instruções, consulte "Vendo mensagens do sistema" na página 51.
	Crie uma Lista de Vigias	Se você tiver dispositivos, bundles e políticas cujas atividades você deseja monitorar de perto, adicione-as à Lista de Vigias. Para obter instruções, consulte "Criando uma lista de vigias" na página 53.

2 Ferramentas de gerenciamento

O ZENworks dispõe de um console baseado na Web (ZENworks Control Center) e um utilitário de linha de comando (zman) que podem ser usados para gerenciar o sistema ZENworks. As seções a seguir explicam como acessar e usar as ferramentas de gerenciamento:

ZENworks Control Center

O ZENworks Control Center é instalado em todos os Servidores ZENworks na zona de gerenciamento. Você pode executar todas as tarefas de gerenciamento em qualquer Servidor Principal. Como se trata de um console de gerenciamento com base na Web, o ZENworks Control Center pode ser acessado de qualquer estação de trabalho suportada.

Se você usa o iManager para administrar outros produtos da Micro Focus no ambiente de rede, pode habilitar o ZENworks Control Center para ser iniciado do iManager. Para obter mais informações, consulte "Accessing Control Center through Novell iManager" (Acessando o ZENworks Control Center pelo Novell iManager) na *ZENworks Control Center Reference* (Referência do ZENworks Control Center).

Acessando o ZENworks Control Center

1. Digite o seguinte URL no browser da Web:

   `https://ZENworks_Server_Address:port`

   Substitua *Endereço_Servidor_ZENworks* pelo endereço IP ou nome DNS do Servidor ZENworks. Você precisará apenas especificar a *porta* se não estiver usando uma das portas padrão (80 ou 443). O ZENworks Control Center requer uma conexão HTTPS; as solicitações HTTP são direcionadas para HTTPS.

   A caixa de diálogo de login é exibida.

2. No campo **Nome de usuário**, digite `Administrador`.
3. No campo **Senha**, digite a senha do Administrador criada durante a instalação.

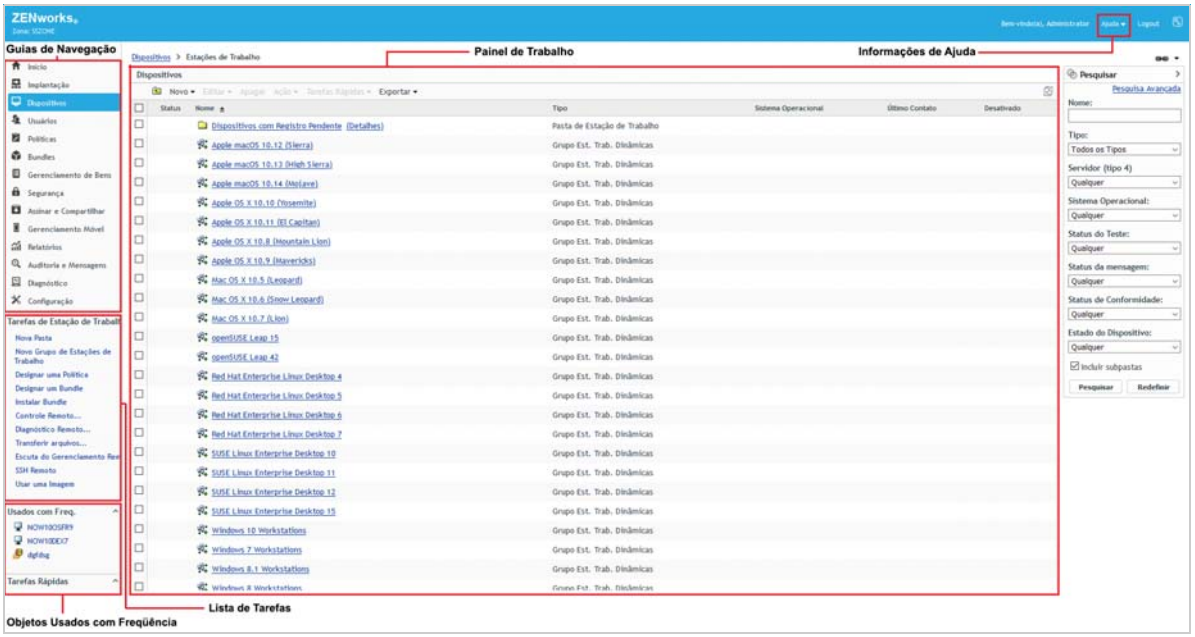
   Para evitar que usuários não autorizados obtenham acesso ao ZENworks Control Center, a conta de administrador é desabilitada após três tentativas de login mal-sucedidas, e um tempo de espera de 60 segundo é aplicado antes de uma nova tentativa de login. Para mudar esses valores padrão, consulte "Changing the Default Login Disable Values" (Mudando os valores de desabilitação de login padrão) na *ZENworks Control Center Reference* (Referência do ZENworks Control Center).

4 Clique em **Login** para exibir o ZENworks Control Center.

Para obter informações mais detalhadas sobre como efetuar login como um administrador diferente, consulte “Accessing ZENworks Control Center” (Acessando o ZENworks Control Center) na *ZENworks Control Center Reference* (Referência do ZENworks Control Center).

Navegando no ZENworks Control Center

A seguinte página Estações de Trabalho representa uma tela padrão no ZENworks Control Center.



Guias de navegação: As guias no painel esquerdo permitem que você navegue pelas áreas funcionais do ZENworks. Por exemplo, a página Estações de Trabalho mostrada acima permite gerenciar tarefas associadas às estações de trabalho.

Lista de Tarefas: A lista de tarefas no painel esquerdo permite um acesso rápido às tarefas executadas com mais frequência referentes à página atual. A lista de tarefas muda a cada página. Por exemplo, a lista de tarefas na página Dispositivos exibe as tarefas relacionadas a dispositivos, enquanto a lista de tarefas na página Configuração exibe as tarefas relacionadas à configuração.

Objetos usados com frequência: A lista Usados com Freq. no painel esquerdo exibe os 10 objetos acessados com mais frequência, do mais ao menos usado. Ao clicar em um objeto, você é levado diretamente para sua página de detalhes.

Painel de trabalho: Os painéis de trabalho são onde você monitora e gerencia seu sistema ZENworks. Eles mudam de acordo com a página atual. No exemplo acima, há dois painéis de trabalho: **Dispositivos** e **Pesquisar**. O painel **Dispositivos** lista as estações de trabalho, as pastas de estação de trabalho, os grupos de estações de trabalho e os grupos dinâmicos de estações de trabalho que foram criados. Esse painel é usado para gerenciar estações de trabalho. O painel **Pesquisar** permite filtrar o painel Dispositivos com base em critérios como nome, sistema operacional ou status da estação de trabalho.

Informações de ajuda: O botão Ajuda é vinculado aos tópicos da Ajuda que fornecem informações sobre a página atual. Os links do botão Ajuda mudam de acordo com a página atual.

Utilitário de Linha de Comando zman

O utilitário zman fornece uma interface de gerenciamento de linha de comando que permite realizar muitas das tarefas disponíveis no ZENworks Control Center. Por exemplo, você pode adicionar conteúdo a bundles, designar políticas a dispositivos e registrar dispositivos. A principal vantagem de usar o utilitário de linha de comando é a capacidade de criar scripts para tratar as operações repetitivas ou em massa. Assim como o ZCC, o utilitário zman é instalado em todos os Servidores Principais, mas só pode ser executado a partir da linha de comando do servidor.

O objetivo principal do utilitário zman é permitir a execução de operações através de um script. Entretanto, você também pode executar as operações manualmente em uma linha de comando.

Localização

O utilitário é instalado na seguinte localização nos Servidores ZENworks:

`%ZENWORKS_HOME%\bin`

onde %ZENWORKS_HOME% representa o caminho de instalação do ZENworks. No Windows, o caminho padrão é `C:\Arquivos de Programas (x86)\Novell\Zenworks\bin`. No Linux, o caminho padrão é `opt/novell/zenworks/bin`.

Sintaxe

O utilitário zman usa a seguinte sintaxe básica:

`zman` *`ação_da_categoria`* `[`*`opções`*`]`

Por exemplo, para atribuir um bundle de software a um dispositivo, use o seguinte comando:

```
zman bundle-assign workstation bundle1 wks1
```

onde`bundle-assign` é a ação da categoria e `workstation bundle1 wks1` são as opções. Nesse exemplo, as opções são o tipo de dispositivo (estação de trabalho), o nome do bundle (bundle1) e o dispositivo de destino (wks1).

Por exemplo, para iniciar uma exploração de inventário de um dispositivo, use o seguinte comando:

```
zman inventory-scan-now dispositivo/servidores/servidor1
```

onde`inventory-scan-now` é a categoria-ação e `dispositivo/servidores/servidor1` é uma opção que especifica o caminho da pasta do dispositivo a ser verificado.

Ajuda com comandos

A melhor maneira de entender os comandos é usando a Ajuda online ou consultando o "zman(1)" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Para usar a ajuda online:

1 No Servidor ZENworks, digite `zman --help` em um prompt de comando.

Esse comando exibe o uso (sintaxe) básico e uma lista das categorias de comando disponíveis. Você também pode usar o seguinte para obter ajuda:

Comando	Descrição
`zman --help | more`	Exibe uma lista completa de comandos por categoria.
`zman categoria --help | more`	Exibe uma lista completa de comandos de uma categoria.
`zman comando --help | more`	Exibe a ajuda de um comando

Utilitário de Linha de Comando zac

O utilitário zac fornece uma interface de gerenciamento em linha de comando que permite executar as tarefas disponíveis no Agente do ZENworks.

- "Localização" na página 20
- "Sintaxe" na página 20
- "Ajuda com comandos" na página 21

Localização

O utilitário é instalado na seguinte localização em todos os dispositivos gerenciados do Windows:

`%ZENWORKS_HOME%\bin`

onde %ZENWORKS_HOME% representa o caminho de instalação do ZENworks. O caminho padrão é `c:\arquivos de programas\novell\zenworks\bin` em um dispositivo Windows de 32 bits e `c:\arquivos de programas (x86)\novell\zenworks\bin` em um dispositivo Windows de 64 bits.

Sintaxe

O utilitário zac usa a seguinte sintaxe básica:

`zac opções de comando`

Por exemplo, para iniciar um bundle em um dispositivo, use o seguinte comando:

```
zac bundle-launch "bundle 1"
```

ondebundle-launch é o comando, e bundle 1é a opção de comando. Nesse exemplo, a opção é o nome de exibição do bundle a ser iniciado. O uso do nome entre aspas somente será necessário se o nome de exibição do bundle incluir espaços.

Por exemplo, para iniciar uma exploração de inventário em um dispositivo, use o seguinte comando:

```
zac inv scannow
```

ondeinv é o comando e scannowé a opção do comando.

Ajuda com comandos

A melhor maneira de entender os comandos é usando a Ajuda online ou consultando o "zac for Windows(1)" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Para usar a ajuda online:

1 No dispositivo gerenciado, digite um dos seguintes comandos em um prompt de comando.

Comando	Descrição
`zac --help`	Exibe uma lista completa de comandos.
`zac` *`comando`* `--help`	Exibe a ajuda detalhada de um comando.

3 Configuração da zona de gerenciamento

O ZENworks foi projetado para possibilitar o gerenciamento eficiente de um número grande de dispositivos e usuários com o menor esforço possível. A primeira etapa para aliviar a carga de gerenciamento consiste em verificar se você configurou a zona de gerenciamento, para poder aproveitar ao máximo os recursos do ZENworks.

As seções a seguir apresentam os conceitos básicos necessários para configurar uma zona de gerenciamento que suporte melhor as tarefas de gerenciamento ininterruptas executadas. Cada seção explica um conceito de gerenciamento e fornece etapas gerais para executar as tarefas associadas ao conceito.

Organizando dispositivos: pastas e grupos

Com o ZENworks Control Center, é possível gerenciar dispositivos, executando tarefas diretamente em objetos Dispositivo individuais. No entanto, essa abordagem não é muito eficiente, a não ser que você tenha poucos dispositivos para gerenciar. Para otimizar o gerenciamento de um grande número de dispositivos, o ZENworks permite que você organize os dispositivos em pastas e grupos; em seguida, você poderá executar as tarefas em uma pasta ou em um grupo para gerenciar seus dispositivos.

Você pode criar pastas e grupos a qualquer momento. No entanto, a melhor prática é criar as pastas e os grupos antes de registrar os dispositivos na sua zona. Isso permitirá usar regras e chaves de registro que adicionem dispositivos automaticamente às pastas e aos grupos adequados quando eles forem registrados (consulte “Criando chaves de registros e regras” na página 27).

Pastas

As pastas são uma excelente ferramenta para ajudá-lo a organizar dispositivos e simplificar seu gerenciamento. Você pode aplicar definições de configuração, atribuir conteúdo e executar tarefas em qualquer pasta. Ao fazê-lo, os dispositivos da pasta herdam essas configurações, atribuições e tarefas.

Para obter melhores resultados, coloque os dispositivos com requisitos de definição de configuração semelhantes na mesma pasta. Se todos os dispositivos da pasta necessitarem do mesmo conteúdo ou das mesmas tarefas, você também poderá criar atribuições de conteúdo ou tarefa na pasta. Contudo, talvez nem todos os dispositivos da pasta tenham os mesmos requisitos de conteúdo e tarefa. Portanto, você pode organizar os dispositivos em grupos e atribuir o conteúdo e as tarefas apropriados a cada grupo (consulte “Grupos” na página 25 abaixo).

Por exemplo, suponha que você tenha estações de trabalho em três sites diferentes. Você deseja aplicar diferentes definições de configuração às estações de trabalho nos três locais e, portanto, cria três pastas (`/Estações de Trabalho/Local1`, `/Estações de Trabalho/Local2` e `/Estações de Trabalho/Local3`) e insere as estações de trabalho adequadas em cada pasta. Você decide que a maioria das definições de configuração deverá ser aplicada a todas as estações de trabalho e define essas configurações na zona de gerenciamento. Entretanto, você deseja efetuar uma coleta de inventário de software e hardware semanal no Site1 e no Site2 e uma coleta de inventário mensal no Site3. Você configura uma coleta de inventário semanal na Zona de Gerenciamento e, em seguida, anula a configuração na pasta Site3 para aplicar uma programação mensal. O Site1 e o Site2 coletam o inventário semanalmente, e o Site3 coleta o inventário mensalmente.

Criando uma pasta

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Clique na pasta **Estações de Trabalho**, **Servidores** ou **Dispositivos Móveis**.
3. Clique em **Novo** > **Pasta** para exibir a caixa de diálogo Nova Pasta.
4. No campo **Nome**, digite um nome para a nova pasta.

   Ao nomear um objeto no ZENworks Control Center (pastas, grupos, bundles, políticas etc.), verifique se o nome segue as seguintes convenções:

   - O nome deve ser exclusivo na pasta.
   - Dependendo do software que está sendo usado para o banco de dados do ZENworks, letras maiúsculas e minúsculas podem não criar exclusividade para o mesmo nome. O banco de dados embutido que está incluído no ZENworks não faz distinção entre maiúsculas e minúsculas, portanto, Pasta 1 e PASTA 1 representam o mesmo nome e não podem ser usados na mesma pasta. Se você usar um banco de dados externo que faça essa distinção, Pasta 1 e PASTA 1 serão nomes exclusivos.
   - Se usar espaços, coloque o nome entre aspas ao digitá-lo na linha de comando. Por exemplo, coloque Pasta 1 entre aspas (“Pasta 1”) ao digitá-la no utilitário zman.
   - Os caracteres a seguir são inválidos e não podem ser usados: / \ * ? : " ' < > | ` % ~
5. Clique em **OK** para criar a pasta.

Você também pode usar os comandos `workstation-folder-create` e `server-folder-create` no utilitário zman para criar pastas de dispositivo. Para obter mais informações, consulte "Comandos da estação de trabalho" e "Comandos do servidor" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Grupos

Como acontece com as pastas, você também pode atribuir conteúdo e executar tarefas em grupos de dispositivos. Ao fazê-lo, os dispositivos do grupo herdam essas atribuições e tarefas. Diferentemente do que acontece com as pastas, não é possível aplicar definições de configuração aos grupos.

Os grupos fornecem uma camada adicional de flexibilidade para atribuições de conteúdo e tarefas. Em alguns casos, convém não atribuir o mesmo conteúdo e e executar a mesma tarefa em todos os dispositivos de uma pasta. Ou convém atribuir o mesmo conteúdo e executar tarefas em um ou mais dispositivos de pastas distintas. Para isso, você pode adicionar os dispositivos a um grupo (independentemente das pastas que os contêm) e atribuir o conteúdo e executar as tarefas no grupo.

Por exemplo, vamos voltar ao exemplo das estações de trabalho localizadas em três diferentes sites (consulte a "Pastas" na página 24). Suponha que algumas estações de trabalho em cada site precisem do mesmo software contábil. Como é possível atribuir software a grupos, você pode criar um grupo Contabilidade, adicionar as estações de trabalho de destino a ele e atribuir o software contábil adequado ao grupo. Da mesma forma, é possível usar os grupos para atribuir políticas de segurança e configuração do Windows.

A vantagem de fazer uma atribuição a um grupo é que todos os dispositivos contidos nesse grupo recebem a atribuição, mas você só precisa fazê-la uma vez. Além disso, um dispositivo pode pertencer a qualquer número de grupos exclusivos, e as atribuições de vários grupos se somam. Por exemplo, se você atribuir um dispositivo aos grupos A e B, ele herdará o software atribuído a ambos os grupos.

O ZENworks fornece ambos os grupos e grupos dinâmicos. Do ponto de vista das atribuições de conteúdo ou da execução de tarefas, os grupos e os grupos dinâmicos funcionam exatamente da mesma forma. A única diferença entre os dois tipos de grupos é a maneira como esses dispositivos são adicionados ao grupo. No caso de um grupo, você deve adicionar os dispositivos manualmente. No caso de um grupo dinâmico, defina critérios a serem atendidos por um dispositivo para se tornar membro do grupo. Em seguida, os dispositivos que atenderem aos critérios serão automaticamente adicionados.

O ZENworks inclui vários grupos de servidores dinâmicos predefinidos, por exemplo, Windows 2012 Servers, Windows 2003 Servers e SUSE Linux Enterprise Server.

O ZENworks também inclui grupos de estações de trabalho dinâmicas, por exemplo, Estação de Trabalho Windows XP, Estação de Trabalho Windows 8, Estações de Trabalho Windows Vista e SUSE Linux Enterprise Desktop. Os dispositivos com esses sistemas operacionais são automaticamente adicionados ao grupo dinâmico apropriado.

Criando um grupo

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Para criar um grupo para servidores, clique na pasta **Servidores**.

ou

Se quiser criar um grupo para estações de trabalho, clique na pasta **Estações de Trabalho**.

ou

Para criar um grupo para os dispositivos móveis, clique na pasta **Dispositivos Móveis**.

3 Clique em **Novo** > **Grupo de Servidores** (**Novo** > **Grupo de Estações de Trabalho** para estações de trabalho ou **Novo** > **Grupo de Dispositivos Móveis** para dispositivos móveis.) para iniciar o Assistente de Criação de Novo Grupo.

4 Na página Informações Básicas, digite um nome para o novo grupo no campo **Nome do Grupo** e clique em **Avançar**.

O nome de grupo deve seguir as convenções de nomeação.

5 Na página Resumo, clique em **Concluir** para criar o grupo sem adicionar membros.

ou

Clique em **Avançar** se quiser adicionar membros ao grupo e continue com a Etapa 6.

6 Na página Adicionar Membros do Grupo, clique em **Adicionar** para adicionar dispositivos ao grupo e, em seguida, clique em **Avançar** ao terminar de adicionar dispositivos.

7 Na página Resumo, clique em **Concluir** para criar o grupo.

Você também pode usar os comandos `workstation-group-create` e `server-group-create` no utilitário zman para criar grupos de dispositivos. Para obter mais informações, consulte "Comandos da estação de trabalho" e "Comandos do servidor" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Criando um grupo dinâmico

1 No ZENworks Control Center, clique na guia **Dispositivos**.

2 Para criar um grupo para servidores, clique na pasta **Servidores**.

ou

Se quiser criar um grupo para estações de trabalho, clique na pasta **Estações de Trabalho**.

ou

Para criar um grupo para os dispositivos móveis, clique na pasta **Dispositivo Móvel**.

3 Clique em **Novo** > **Grupo de Servidores Dinâmicos** (**Novo** > **Grupo de Estações de Trabalho Dinâmicas** para estações de trabalho ou **Novo** > **Grupo de Dispositivos Móveis Dinâmicos** para dispositivos móveis) para iniciar o Assistente de Criação de Novo Grupo.

4 Na página Informações Básicas, digite um nome para o novo grupo no campo **Nome do Grupo** e clique em **Avançar**.

O nome de grupo deve seguir as convenções de nomeação.

5 Na página Definir Filtro para Membros do Grupo, defina os critérios a serem atendidos por um dispositivo para se tornar membro do grupo e clique em **Avançar**.

Clique no botão **Ajuda** para obter detalhes sobre a criação dos critérios.

6 Na página Resumo, clique em **Concluir** para criar o grupo.

Herança de atribuições para pastas e grupos

Quando você atribui um conteúdo uma pasta, todos os objetos (usuários, dispositivos, subpastas), exceto os grupos localizados na pasta, herdam a atribuição. Por exemplo, se você atribuir BundleA e PolíticaB a PastadeDispositivos1, todos os dispositivos na pasta (incluindo todos os dispositivos nas subpastas) herdarão as duas atribuições. No entanto, nenhum dos grupos de dispositivos localizados na PastadeDispositivos1 herdará as atribuições. Basicamente, as atribuições de pasta não são propagadas para os grupos localizados na pasta.

Criando chaves de registros e regras

Quando você implanta o Agente do ZENworks em um dispositivo, o dispositivo é registrado na sua zona de gerenciamento e passa a ser um dispositivo gerenciado. Como parte do registro, você pode especificar o nome e a pasta do dispositivo no ZENworks e os grupos aos quais deseja adicionar o dispositivo.

Por padrão, o nome de host de um dispositivo é usado como seu nome no ZENworks, é adicionado à pasta `/Servidores` ou `/Estações de Trabalho` e não obtém participação em nenhum grupo. Você pode mover manualmente dispositivos para outras pastas e adicioná-los a grupos, mas isso talvez seja uma tarefa incômoda no caso de um grande número de dispositivos ou se estiver adicionando novos dispositivos de forma consistente. A melhor maneira de gerenciar um grande número de dispositivos é fazer com que sejam adicionados automaticamente às pastas e aos grupos corretos durante o registro.

Para adicionar dispositivos a pastas e grupos durante o registro, você pode usar chaves de registro, regras de registro ou ambos. As chaves de registro e as regras de registro permitem atribuir participações em pastas e grupos a um dispositivo. No entanto, há diferenças entre chaves e regras que você deve conhecer antes de decidir se deseja usar um ou ambos os métodos para registro.

Esse recurso não é aplicável a Dispositivos Móveis.

- “Chaves de registro” na página 27
- “Regras de Registro” na página 28
- “Gabarito de Nomeação de Dispositivos” na página 29
- “Onde encontrar mais informações” na página 29

Chaves de registro

uma chave de registro é uma string alfanumérica que você define manualmente ou gera aleatoriamente. Durante a implantação do Agente do ZENworks em um dispositivo, a chave de registro deverá ser fornecida. Quando o dispositivo se conecta a um Servidor ZENworks pela primeira vez, ele é adicionado à pasta e aos grupos definidos na chave.

É possível criar uma ou mais chaves de registro para garantir que os dispositivos sejam colocados nas pastas e nos grupos desejados. Por exemplo, você talvez queira garantir que todas as estações de trabalho do Departamento de Vendas sejam adicionadas à pasta `/Estações de Trabalho/Vendas`, mas sejam divididas em três grupos diferentes (EquipeVendas1, EquipeVendas2, EquipeVendas3) dependendo das atribuições de sua equipe. É possível criar três chaves de registro

diferentes e configurar cada uma para adicionar as estações de trabalho Vendas à pasta `/Estações de Trabalho/Vendas` e ao grupo de equipe apropriado. Se cada estação de trabalho usar a chave de registro correta, ela será adicionada à pasta e ao grupo adequados.

Para criar uma chave de registro:

1. No ZENworks Control Center, clique na guia **Configuração** e, em seguida, clique na guia **Registro**.
2. No painel Chaves de Registro, clique em **Novo** > **Chave de Registro** para iniciar o Assistente de Criação de Nova Chave de Registro.
3. Siga os prompts para criar a chave.

   Para obter informações sobre o que você precisa fornecer em cada etapa do assistente, clique no botão **Ajuda**.

Você também pode usar o comando `registration-create-key` no utilitário zman para criar uma chave de registro. Para obter mais informações, consulte "Comandos de registro" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Regras de Registro

Se não desejar digitar uma chave de registro durante a implantação ou se desejar que os dispositivos sejam automaticamente adicionados a pastas e grupos diferentes com base em critérios predefinidos (por exemplo, tipo de sistema operacional, CPU ou endereço IP), você poderá usar regras de registro.

O ZENworks tem duas regras de registro padrão: uma para servidores e uma para estações de trabalho. Se um dispositivo for registrado sem chave e você não tiver criado regras de registro, as regras de registro padrão serão aplicadas para determinar as atribuições de pasta. As duas regras padrão determinam que todos os servidores sejam adicionados à pasta `/Servidores` e todas as estações de trabalho sejam adicionadas à pasta `/Estações de Trabalho`.

As duas regras padrão são atribuídas para garantir que não haja falha de registro em nenhum servidor ou estação de trabalho. Portanto, você não pode apagar nem modificar essas duas regras padrão. É possível, entretanto, definir regras adicionais que permitam filtrar dispositivos à medida que eles forem registrados e adicioná-los a pastas e grupos diferentes. Se, conforme recomendado na "Organizando dispositivos: pastas e grupos" na página 23, você tiver estabelecido pastas para dispositivos com definições de configuração semelhantes e grupos para dispositivos com atribuições semelhantes, novos dispositivos registrados receberão automaticamente as definições de configuração e as atribuições adequadas.

Para criar uma regra de registro:

1. No ZENworks Control Center, clique na guia **Configuração** e, em seguida, clique na guia **Registro**.
2. No painel Regras de Registro, clique em **Novo** para iniciar o Assistente de Criação de Nova Regra de Registro.
3. Siga os prompts para criar a regra.

   Para obter informações sobre o que você precisa fornecer em cada etapa do assistente, clique no botão **Ajuda**.

Você também pode usar o comando `ruleset-create` no utilitário zman para criar uma regra de registro. Para obter mais informações, consulte "Comandos de conjuntos de regras" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Gabarito de Nomeação de Dispositivos

O gabarito de nomeação de dispositivos determina o modo de nomeação dos dispositivos durante seu registro. Por padrão, o nome de host de um dispositivo é usado. Você pode mudá-lo para usar qualquer combinação das seguintes variáveis de máquina: ${HostName}, ${GUID}, ${OS}, ${CPU}, ${DNS}, ${IPAddress} e ${MACAddress}.

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da Zona de Gerenciamento, clique em **Gerenciamento de Dispositivo**.
3. Clique em **Registro** para exibir a página Registro.
4. No painel Gabarito de Nomeação de Dispositivos, clique em  e selecione a variável de máquina desejada da lista.

   Você pode usar qualquer combinação de uma ou mais variáveis. Por exemplo:

   ```
   ${HostName}${GUID}
   ```
5. Clique em **OK** para gravar as mudanças.

Onde encontrar mais informações

Para obter mais informações sobre o registro de dispositivos, consulte a *Referência de Descoberta, Implantação e Desativação do ZENworks*.

Conectando-se às origens do usuário

Você pode se conectar a um ou mais diretórios LDAP para fornecer origens de usuário autorizadas no ZENworks.

A adição de uma origem de usuário permite associar contas de administrador do ZENworks a contas de usuário LDAP, e associar dispositivos aos usuários que os utilizaram primeiro. Além disso, a adição de usuários proporciona uma funcionalidade extra aos seguintes produtos do ZENworks:

- **Gerenciamento de Configurações:** Permite atribuir bundles e políticas a usuários e dispositivos. Habilita os relatórios de inventário baseados no usuário.
- **Gerenciamento de Bens:** Permite contabilizar as licenças de software por usuário e por dispositivo.
- **Gerenciamento de Segurança de Endpoint:** Permite atribuir políticas a usuários e dispositivos.

Quando você define um diretório LDAP como origem de usuário, o diretório não é afetado; o ZENworks exige apenas acesso de leitura ao diretório LDAP e armazena todas as informações de atribuição no banco de dados do ZENworks. Para obter informações mais detalhadas sobre os direitos de leitura específicos necessários para conexão com uma origem de usuário, consulte "Creating User Source Connections" (Criando conexões com origem de usuário) na *ZENworks User Source and Authentication Reference* (Referência de Autenticação e Origem de Usuário do ZENworks 11 SP4).

Você pode se conectar ao Novell eDirectory e ao Microsoft Active Directory como origens de usuário. Os requisitos mínimos são o Novell eDirectory 8.7.3 e o Microsoft Active Directory no Windows 2000 SP4. O requisito mínimo de LDAP é a versão 3.

Após se conectar a um diretório LDAP, defina os containers no diretório que deseja expor. Por exemplo, suponha que você possua uma árvore de domínio do Microsoft Active Directory chamada MinhaEmpresa. Todos os usuários residem em dois containers da árvore MinhaEmpresa: MinhaEmpresa/Usuários e MinhaEmpresa/Temp/Usuários. Você pode fazer referência à árvore MinhaEmpresa como a origem e MinhaEmpresa/Usuários e MinhaEmpresa/Temp/Usuários como containers de usuário separados. Isso limita o acesso dentro do diretório somente aos containers que incluem usuários.

Além dos usuários que residem nos containers adicionados, o ZENworks Control Center também exibe quaisquer grupos de usuários localizados nos containers. Isso possibilita o gerenciamento tanto de um usuário individual quanto de grupos de usuários.

Para se conectar a uma origem de usuário:

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Origens do Usuário, clique em **Novo** para iniciar o Assistente de Criação de Nova Origem de Usuário.
3. Siga os prompts para criar a origem do usuário.

   Para obter informações sobre o que você precisa fornecer em cada etapa do assistente, clique no botão **Ajuda**.

Você também pode usar o comando `user-source-create` no utilitário zman para criar uma conexão com uma origem de usuário. Para obter mais informações, consulte "Comandos do usuário" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Para obter mais informações sobre como habilitar origens de usuário para registro de dispositivo móvel, consulte Configuring User Sources (Configurando origens de usuário) na ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).

Criando contas de administrador do ZENworks

Durante a instalação, é criada uma conta de administrador padrão do ZENworks (chamada Administrador). Essa conta, chamada de conta de Superadministrador, fornece direitos administrativos plenos à Zona de Gerenciamento.

Em geral, você deve criar contas de administrador para cada pessoa que executará tarefas administrativas. Você pode definir essas contas como de superadministrador ou de administrador com direitos restritos. Por exemplo, você pode conceder uma conta de administrador ao usuário que somente lhe permita descobrir e registrar dispositivos na Zona de Gerenciamento. Se preferir, a conta poderá permitir apenas que o usuário atribua bundles a dispositivos. Pode também se limitar à execução de tarefas de gerenciamento de bens, como gerenciamento de contratos, licenças e documentos.

Em alguns casos, você pode ter várias contas de administrador que requerem os mesmos direitos administrativos. Em vez de atribuir direitos a cada conta individualmente, você pode criar uma função de administrador, atribuir os direitos administrativos à função e depois adicionar as contas à função. Por exemplo, você pode ter uma função de Suporte Técnico que fornece direitos administrativos necessários a diversos dos seus administradores.

Você pode criar grupos de administradores. Se você atribuir direitos e funções a um grupo de administradores, os direitos e as funções atribuídos serão aplicados a todos os membros do grupo.

Criando uma conta de administrador

1. No ZENworks Control Center, clique na guia **Administradores**.
2. No painel Administradores, clique em **Novo > Administrador** para exibir a caixa de diálogo Adicionar novo Administrador.
3. Preencha os campos.

   Essa caixa de diálogo permite criar uma nova conta de administrador por meio de um nome e uma senha, ou você pode criar um novo administrador com base em um usuário existente na origem do usuário. Opcionalmente, você pode conceder ao novo administrador os mesmos direitos detidos pelo administrador que efetuou login.

   Crie um novo Administrador, fornecendo nome, senha: Selecione essa opção para criar uma nova conta de administrador especificando manualmente o nome e a senha.

   Com base no(s) usuário(s) de uma origem de usuário: Selecione essa opção para criar uma nova conta de administrador com base nas informações de usuário de sua origem de usuário. Para isso, clique em **Adicionar**, procure e selecione o usuário desejado.

   Atribua a esse Administrador os mesmos direitos que possuo: Selecione essa opção para atribuir ao novo administrador os mesmos direitos que você tem como o administrador atual que efetuou login. Se você tem direitos de Superadministrador, o novo administrador é criado como Superadministrador.
4. Clique em **OK** para adicionar o novo administrador ao painel Administradores.
5. Se precisar mudar os direitos ou as funções do novo administrador, clique na conta do administrador e, em seguida, na guia **Direitos** para exibir os detalhes da conta.
6. Se a opção **Superadministrador** estiver selecionada, desmarque-a.

   Não é possível modificar os direitos de Superadministrador.
7. No painel Direitos Designados, modifique os direitos atribuídos.
8. Usando o painel Funções Designadas, modifique as funções atribuídas.
9. Clique em **Aplicar** para gravar as mudanças.

Para obter mais informações sobre como criar contas de administrador, direitos de administrador ou funções de administrador do ZENworks, consulte a ZENworks Administrator Accounts and Rights Reference (Referência de Contas e Direitos de Administrador do ZENworks).

Você também pode usar o comando `admin-create` no utilitário zman para criar uma conta de administrador do ZENworks. Para obter mais informações, consulte “Comandos do administrador” na *Referência de Utilitários de Linha de Comando do ZENworks*.

Criando uma conta de grupo de administradores

1. No ZENworks Control Center, clique na guia **Administradores**.
2. No painel Administradores, clique em **Novo** > **Grupo de Administradores** para exibir a caixa de diálogo Adicionar novo Grupo de Administradores.
3. Preencha os campos.

A caixa de diálogo Adicionar novo Grupo de Administradores permite criar uma nova conta de grupo de administradores especificando o nome do grupo e adicionando membros ao grupo. É possível também criar um novo grupo de administradores com base no grupo de usuários existente na origem de usuário. Cada nome de grupo de administradores deve ser exclusivo.

Crie um novo Grupo de Administradores fornecendo o nome, a descrição e os membros:

Selecione essa opção para criar uma nova conta de grupo de administradores especificando manualmente o nome e adicionando os membros. Para adicionar membros, clique em **Adicionar**, depois procure e selecione os administradores necessários. É possível adicionar qualquer número de administradores ao grupo. Não é possível adicionar outros grupos de administradores ao grupo.

Com base no(s) grupo(s) de usuários de uma origem de usuário: Selecione essa opção para criar uma nova conta de grupo de administradores baseada nas informações do grupo de usuários da sua origem de usuário. Para isso, clique em **Adicionar**, procure e selecione o grupo de usuários necessário.

Importe os membros usuários de cada grupo de usuários como administradores imediatamente: Selecione essa opção para habilitar os membros usuários dos grupos de usuários selecionados a serem adicionados imediatamente como administradores.

4. Clique em **OK** para adicionar o novo grupo de administradores ao painel Administradores.
5. Se precisar mudar os direitos ou as funções do novo grupo de administradores, clique na conta do grupo de administradores e depois na guia **Direitos** para exibir os detalhes da conta.
6. No painel Direitos Designados, modifique os direitos atribuídos.
7. Usando o painel Funções Designadas, modifique as funções atribuídas.
8. Clique em **Aplicar** para gravar as mudanças.

Para obter mais informações sobre como criar contas de grupo de administradores, direitos de administrador ou funções de administrador do ZENworks, consulte a *ZENworks Administrator Accounts and Rights Reference* (Referência de Contas e Direitos de Administrador do ZENworks).

Você também pode usar o comando `admin-create` no utilitário zman para criar uma conta de administrador do ZENworks. Para obter mais informações, consulte "Comandos do administrador" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Modificando definições de configuração

As definições de configuração da Zona de Gerenciamento permitem controlar uma grande variedade de comportamentos de funcionalidades da sua zona. Existem configurações de Gerenciamento de Dispositivos que permitem controlar a frequência com que os dispositivos acessam um Servidor ZENworks para obter informações atualizadas, a frequência com que os grupos dinâmicos são atualizados e os níveis de mensagens (informativas, de aviso ou de erro) que são registrados pelo Agente do ZENworks. Há configurações de Evento e Mensagens, configurações de Descoberta e Implantação etc.

As configurações da zona de gerenciamento aplicáveis aos dispositivos são herdadas por todos os dispositivos da zona. Conforme mencionado na "Organizando dispositivos: pastas e grupos" na página 23, você pode anular as configurações de zona definindo-as nas pastas de dispositivos ou em dispositivos individuais. Isso permite que você estabeleça configurações de zona aplicáveis ao maior número de dispositivos e, conforme necessário, anule as configurações nas pastas e nos dispositivos.

Por padrão, suas configurações de zona são predefinidas com valores que oferecem uma funcionalidade comum. No entanto, você pode mudar as configurações para adaptá-las melhor ao comportamento necessário ao seu ambiente.

Modificando as definições de configuração na zona

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da Zona de Gerenciamento, clique na categoria de configurações (por exemplo, **Gerenciamento de Dispositivo**, **Descoberta e Implantação** e **Evento e Mensagens**) que tem as configurações que deseja modificar.
3. Clique na configuração para exibir sua página de detalhes.
4. Modifique a configuração conforme necessário.

   Para obter informações sobre a configuração, consulte a *ZENworks Management Zone Settings Reference* (Referência de Configurações da Zona de Gerenciamento do ZENworks).
5. Clique em **OK** ou **Aplicar**.

   Se a definição de configuração for aplicável a dispositivos, a configuração será herdada por todos os dispositivos da zona, a menos que a configuração seja anulada em um nível de pasta ou de dispositivo.

Modificando as definições de configuração em uma pasta

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. No painel Dispositivos (na guia **Gerenciado**), procure a pasta cujas configurações você deseja modificar.
3. Clique em **Detalhes** ao lado do nome da pasta para exibir os detalhes.
4. Clique na guia **Configurações**.
5. No painel Configurações, clique na categoria de configurações (**Gerenciamento de Dispositivo**, **Gerenciamento da Infraestrutura**, etc.) que tem as configurações que deseja modificar.
6. Clique na configuração para exibir a página de detalhes.
7. Modifique a configuração conforme necessário.

   Para obter informações sobre a configuração, consulte a *ZENworks Management Zone Settings Reference* (Referência de Configurações da Zona de Gerenciamento do ZENworks).
8. Clique em **OK** ou **Aplicar**.

   A definição de configuração é herdada por todos os dispositivos na pasta, incluindo os dispositivos contidos em subpastas, a menos que a configuração seja anulada em uma subpasta ou um dispositivo individual.

Modificando as definições de configuração em um dispositivo

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. No painel Dispositivos (na guia **Gerenciado**), procure o dispositivo cujas configurações você deseja modificar.
3. Quando você encontrar o dispositivo, clique no nome dele para exibir seus detalhes.
4. Clique na guia **Configurações**.
5. No painel Configurações, clique na categoria de configurações (**Gerenciamento de Dispositivo**, **Gerenciamento da Infraestrutura**, etc.) que tem as configurações que deseja modificar.
6. Clique na configuração para exibir sua página de detalhes.
7. Modifique a configuração conforme desejado.

   Para obter informações sobre a configuração, clique no botão **Ajuda** no ZENworks Control Center.
8. Quando tiver acabado de modificar a configuração, clique em **OK** (ou **Aplicar**) para gravar as mudanças.

Compartilhamento e assinatura na zona

O recurso Assinar e Compartilhar no ZENworks permite compartilhar objetos de conteúdo (por exemplo, bundles e políticas) que podem ser atribuídos a várias zonas do ZENworks:

- **Zona de Compartilhamento:** Compartilha conteúdo.
- **Zona de Assinante:** Faz a assinatura na zona de compartilhamento e replica o conteúdo compartilhado em sua própria zona.

No ZENworks Control Center, você pode usar o link Configurações de Compartilhamento da Zona, no painel Gerenciamento da Infraestrutura, para gerenciar as atividades de compartilhamento da zona.

Na zona de Compartilhamento, um Servidor Principal é identificado como o servidor de Compartilhamento. Todas as atividades de compartilhamento de conteúdo são realizadas nesse servidor. O registro na zona de Assinante é feito por meio de uma chave do assinante na zona de compartilhamento. A chave do assinante não concede ao assinante nenhum direito sobre o conteúdo. A chave do Assinante é usada para o registro do Assinante.

Em seguida, o conteúdo necessário é compartilhado da zona de Compartilhamento e replicado na zona de Assinante. Você será notificado se houver qualquer problema de replicação, dessa forma, poderá realizar as ações corretivas.

Para obter mais detalhes, consulte a *ZENworks Subscribe and Share Reference* (Referência de Assinatura e Compartilhamento do ZENworks).

Atualizar o Software ZENworks

É possível atualizar o software do ZENworks em todos os dispositivos na Zona de Gerenciamento na qual o software está instalado. Os downloads de atualização podem ser programados. As atualizações de software são fornecidas no nível da versão do Support Pack. Você pode escolher se deseja aplicar cada atualização após ver seu conteúdo (as versões de Support Pack são cumulativas).

Você também pode fazer download da última PRU (Product Recognition Update – Atualização de Reconhecimento do Produto) para atualizar sua base de dados de conhecimento, de forma que o ZENworks Inventory reconheça o software mais recente.

Para obter mais informações, consulte a *ZENworks System Updates Reference* (Referência de Atualizações de Sistema do ZENworks).

Criando locais

Os requisitos de segurança de um dispositivo podem variar de local para local. Por exemplo, você pode ter restrições de firewall pessoais para um dispositivo localizado no terminal de um aeroporto diferentes das restrições de um dispositivo localizado no escritório protegido pelo firewall da sua empresa.

Para assegurar que os requisitos de segurança de um dispositivo sejam apropriados ao seu local, o ZENworks suporta ambas políticas globais e baseadas em local. Uma política global é aplicada independentemente do local do dispositivo. Uma política baseada em local é aplicada apenas quando o local atual do dispositivo atende aos critérios de um local associado à política. Por exemplo, se você criar uma política baseada em local para o seu escritório corporativo e atribuí-la a um laptop, ela só será aplicada quando o local do laptop for o escritório corporativo.

Para usar as políticas baseadas em local, defina primeiro os locais adequados à sua organização. O local é um tipo de lugar para o qual você tem requisitos de segurança específicos. Por exemplo, você pode ter requisitos de segurança diferentes para quando um dispositivo é usado no escritório, em casa ou no aeroporto.

Os locais são definidos por ambientes de rede. Suponha que você tenha um escritório em Nova York e um em Tóquio. Os dois escritórios têm os mesmos requisitos de segurança. Portanto, você cria um local Escritório e o associa a dois ambientes de rede: Rede do Escritório de Nova York e Rede do Escritório de Tóquio. Cada um desses ambientes é definido explicitamente definido por um conjunto de serviços de gateway, servidor DNS e ponto de acesso wireless. Sempre que o Agente do ZENworks determinar a correspondência de seu ambiente atual com a Rede do Escritório de Nova York ou a Rede do Escritório de Tóquio, o agente definirá seu local como Escritório e aplicará as políticas de segurança associadas ao local Escritório.

As seções a seguir explicam como criar locais:

- “Definindo um ambiente de rede” na página 35
- “Criando locais” na página 36
- “Seleção de local e ambiente de rede em um dispositivo gerenciado” na página 37

Definindo um ambiente de rede

As definições de ambiente de rede são os blocos estruturais dos locais. É possível definir os ambientes de rede durante a criação de um local. Porém, é recomendado definir primeiro os ambientes de rede e, depois, adicioná-los durante a criação dos locais.

Para criar um ambiente de rede:

1 No ZENworks Control Center, clique em **Configuração** > **Locais**.

2 No painel Ambientes de Rede, clique em **Novo** para iniciar o Assistente Criar Novo Ambiente de Rede.

3 Na página Definir Detalhes, especifique o nome do ambiente de rede e clique em **Próximo**.

4 Na página Detalhes do Ambiente de Rede, especifique o seguinte:

Limite para o Tipo de Adaptador: Por padrão, os serviços de rede definidos nessa página são avaliados para saber se são adaptadores de rede do dispositivo com fio, wireless e por discagem. Para limitar a avaliação a determinado tipo de adaptador, selecione **Com Fio**, **Wireless** ou **Por Discagem**.

Correspondência Mínima: Especifique o número mínimo de serviços de rede definidos que devem ser correspondidos para que este ambiente de rede seja selecionado.

Especifique o número mínimo de serviços de rede definidos que devem ser correspondidos para que este ambiente de rede seja selecionado.

Por exemplo, se você definir um endereço de gateway, três servidores DNS e um servidor DHCP, terá um total de cinco serviços. É possível especificar que pelo menos três desses serviços sejam correspondidos para que este ambiente de rede seja selecionado.

Ao especificar um número mínimo de correspondências, verifique o seguinte:

- O número não pode ser menor que o número de serviços marcados como Correspondência Obrigatória.
- O número não deve exceder o número total de serviços definidos. Se ele exceder, a correspondência mínima nunca será atingida, e o ambiente de rede nunca será selecionado.

Serviços de rede: Permite definir os serviços de rede que o Agente do ZENworks avalia para saber se o seu ambiente de rede atual corresponde a este ambiente de rede. Selecione a guia referente ao serviço de rede que deseja definir. Clique em **Adicionar** e especifique as informações necessárias.

5 Clique em **Avançar** para exibir a página Resumo e clique em **Concluir**.

Criando locais

Ao criar um local, você especifica um nome e associa os ambientes de rede necessários a ele.

1 No ZENworks Control Center, clique em **Configuração** > **Locais**.

2 No painel Locais, clique em **Novo** para iniciar o assistente Criar Novo Local.

3 Na página Definir Detalhes, especifique um nome ao local e depois clique em **Próximo**.

4 Na página Atribuir Ambientes de Rede:

4a Selecione **Atribuir Ambientes de Rede existentes ao Local**.

4b Clique em **Adicionar**, selecione os ambientes de rede nos quais deseja definir o local e clique em **OK** para adicioná-los à lista.

4c Clique em **Próximo** ao terminar de adicionar os ambientes de rede.

5 Na página Resumo, clique em **Concluir** para criar o local e adicioná-lo à lista Locais.

Quando vários locais incluem o ambiente de rede identificado pelo Agente do ZENworks, a ordem da lista determina o local que será usado. Por padrão, o local que aparecer em primeiro lugar na lista será selecionado. Para reordenar a lista, use as opções **Para Cima** e **Para Baixo**.

É possível usar também os comandos `network-environment-create` e `location-create` no utilitário zman para criar um ambiente de rede e o local relacionado usando o ambiente de rede criado. Para obter mais informações, consulte "Comandos de registro" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Seleção de local e ambiente de rede em um dispositivo gerenciado

Se você tem vários locais e ambientes de rede definidos no ZENworks Control Center, o Agente do ZENworks no dispositivo gerenciado explora todos os ambientes de rede definidos para identificar os ambientes correspondentes. Com base nos ambientes identificados, o Agente do ZENworks seleciona os ambientes de rede que têm o maior número de serviços de rede correspondentes (como Endereço IP do Cliente e Servidores DNS). Em seguida, o Agente do ZENworks explora a lista ordenada de locais, identifica o primeiro local que inclui qualquer um dos ambientes de rede selecionados e escolhe o local e o primeiro ambiente de rede correspondente desse local.

Por exemplo:

- Os locais definidos no ZENworks Control Center são listados na seguinte ordem: L1 e L2.
- Os ambientes de rede dentro de L1 são listados na seguinte ordem: NE1, NE2 e NE4.
- Os ambientes de rede dentro de L2 são listados na seguinte ordem: NE2, NE3 e NE4.
- O Agente do ZENworks no dispositivo gerenciado detecta que NE2, NE3 e NE4 são todos correspondentes no dispositivo gerenciado.

Se NE2 e NE4 tiverem duas correspondências de serviço de rede cada um, e NE3 tiver apenas uma correspondência de serviço de rede, o Agente do ZENworks selecionará NE2 e NE4 por causa do maior número de correspondências de serviço de rede. Como NE2 é o primeiro ambiente de rede da lista em L1, L1 e NE2 são selecionados como o local e o ambiente de rede.

Observação: Para que um ambiente de rede seja correspondente no dispositivo gerenciado, ele deve atender a todas as restrições definidas no ambiente de rede. Essas restrições incluem o atributo **Correspondência Mínima** especificado para o ambiente de rede e também o atributo **Correspondência Obrigatória** especificado para os serviços de rede dentro do ambiente de rede.

Painel

O recurso do painel de controle oferece um instantâneo completo dos indicadores-chave para que você possa avaliar rapidamente a saúde e a conformidade gerais dos dispositivos na zona. Usando os painéis de controle, você pode detalhar outras áreas de interesse.

Os painéis de controle do ZENworks permitem ver informações relacionadas ao status de dispositivos e patches na zona e executar as ações necessárias.

Para obter mais informações, consulte a ZENworks Dashboard Reference (Referência de Painel de Controle do ZENworks).

4 Implantação do Agente do ZENworks

O Agente do ZENworks deve ser implantado nos dispositivos que você deseja gerenciar. As seções a seguir apresentam instruções que o ajudam a entender o processo de implantação do agente:

Observação: Se um dispositivo não atender aos requisitos de instalação do Agente do ZENworks (consulte "Requisitos de dispositivo gerenciado" nos *Requisitos do Sistema do ZENworks 2020 Update 1*), você poderá instalar o Módulo Apenas Inventário nele para suportar o inventário do dispositivo. Para obter mais informações, consulte a *Referência de Descoberta, Implantação e Desativação do ZENworks*.

Configurando recursos do Agente do ZENworks

O Agente do ZENworks utiliza vários módulos para realizar funções em um dispositivo. Esses módulos são chamados de recursos do Agente do ZENworks. Cada produto do ZENworks possui recursos específicos associados, conforme mostrado na tabela a seguir. Os produtos do ZENworks são listados na coluna esquerda; as outras colunas representam os recursos do Agente do ZENworks.

	Gerenciamento de Bens	Gerenciamento de bundles	Segurança de endpoint	Criptografia de Disco Cheio	Gerenciamento de Imagem	Gerenciamento de Patch	Gerenciamento de políticas	Gerenciamento remoto	Gerenciamento de usuários
ZENworks Asset Management	✓								✓
ZENworks Configuration Management		✓			✓		✓	✓	✓
ZENworks Endpoint Security Management			✓						✓
ZENworks Full Disk Encryption				✓					
ZENworks Patch Management						✓			

Por padrão, quando você ativa um produto do ZENworks, todos os recursos do Agente do ZENworks são instalados e habilitados. A única exceção é o ZENworks Asset Management, que não habilita automaticamente o recurso Gerenciamento de Usuários.

O recurso Gerenciamento de Usuários só é suportado nos dispositivos gerenciados pelo Windows em todos os produtos do ZENworks.

Se não quiser algum recurso instalado ou habilitado no dispositivo, você poderá desinstalá-lo ou desabilitá-lo na Zona de Gerenciamento, na pasta de dispositivos ou no dispositivo individual.

Por exemplo, se estiver usando o ZENworks Configuration Management e não quiser usar o Gerenciamento Remoto com nenhum dispositivo, você poderá desabilitá-lo na Zona de Gerenciamento. Se preferir, caso tenha o ZENworks Configuration Management e o ZENworks Asset Management, mas não queira usar o Gerenciamento de Bens em todos os dispositivos, você poderá habilitar o recurso Gerenciamento de Bens na Zona de Gerenciamento e depois desabilitá-lo (ou desinstalá-lo) nas pastas de dispositivos ou nos dispositivos individuais.

Para personalizar os recursos do Agente do ZENworks, antes ou após a implantação do agente, consulte as seguintes seções:

- "Personalizando os recursos do Agente do ZENworks" na página 40
- "Coexistindo com o ZENworks Desktop Management Agent" na página 41

Personalizando os recursos do Agente do ZENworks

Durante a implantação inicial, o Agente do ZENworks instala e habilita os recursos selecionados no nível da Zona de Gerenciamento. Após o registro do agente, ele utiliza as configurações definidas no nível da pasta de dispositivos ou do dispositivo (se forem diferentes das configurações da zona).

Observação: A personalização de recursos do Agente do ZENworks não se aplica a dispositivos Macintosh.

As etapas a seguir explicam como personalizar as configurações no nível da Zona de Gerenciamento. Para obter informações sobre como personalizar as configurações na pasta de dispositivos ou no dispositivo individual, consulte "Personalizando os recursos do agente" na *Referência de Descoberta, Implantação e Desativação do ZENworks*.

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da Zona de Gerenciamento, clique em **Gerenciamento de Dispositivo** > **Agente do ZENworks**.
3. No painel Recursos do Agent:
   - Se não quiser instalar um recurso, anule a seleção de **Instalado** ao lado de um recurso. O recurso selecionado não será instalado no dispositivo. Se você optar por anular a seleção de todos os recursos, apenas o agente central será instalado.
   - Para instalar, mas desabilitar um recurso, selecione **Instalado** e **Desabilitado** ao lado do recurso. O recurso será instalado no dispositivo, mas não estará funcional.

   A instalação dos recursos Gerenciamento de Bundles, Gerenciamento Remoto ou Gerenciamento de Usuários requer a reinicialização do dispositivo. A instalação do recurso Gerenciamento de Imagem somente requer reinicialização no Windows 2008 e no Windows Vista. Você receberá uma solicitação para reinicializar o dispositivo com base na opção de reinicialização selecionada.
4. Para gravar as mudanças, clique em **OK**.

Coexistindo com o ZENworks Desktop Management Agent

É possível implantar o Agente do ZENworks em dispositivos que tenham o ZENworks Desktop Agent instalado.

O Agente do ZENworks e o ZENworks Desktop Agent coexistem no mesmo dispositivo para suportar o uso do ZENworks Asset Management com o ZENworks Desktop Management. Nesse caso, quando você implanta o Agente do ZENworks em um dispositivo que tenha o Agente de Desktop do ZENworks instalado, convém usar apenas os recursos do Agente do ZENworks que não estão associados ao ZENworks Configuration Management. Não use os recursos Gerenciamento de Bundles, Gerenciamento de Imagem, Gerenciamento de Políticas, Gerenciamento Remoto ou Gerenciamento de Usuários. Se você selecionar qualquer um desses recursos, o Agente de Desktop do ZENworks será desinstalado antes da instalação do Agente do ZENworks.

Para obter mais informações sobre a coexistência do Agente do ZENworks e do Agente de Desktop do ZENworks, consulte "Implantação do Agente do ZENworks" na *Referência de Descoberta, Implantação e Desativação do ZENworks*.

Configurando a segurança do Agente do ZENworks

Para garantir a segurança do Agente do ZENworks nos dispositivos, é possível configurar as definições de desinstalação e de autodefesa para o agente.

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da zona de gerenciamento, clique em **Gerenciamento de Dispositivo** e, em seguida, clique em **Agente do ZENworks**.
3. No painel Segurança do Agente, defina as seguintes configurações:
   - **Permitir usuários a desinstalar o Agente do ZENworks:** Selecione essa opção para desinstalar o Agente do ZENworks.
   - **Exigir senha de desinstalação para o Agente do ZENworks:** Selecione essa opção para especificar uma senha que será obrigatória para desinstalar o Agente do ZENworks. Clique em **Mudar** para definir a senha.

     Para que a senha de desinstalação não seja distribuída aos usuários, é recomendável usar o utilitário Gerador de Chaves de Senha para gerar uma chave de senha. A chave, que é baseada na senha de desinstalação, funciona da mesma forma que a senha de desinstalação, mas pode ser associada a um único dispositivo ou usuário para limitar o seu uso.

     O utilitário Gerador de Chaves de Senha pode ser acessado na lista Tarefas de Configuração no painel de navegação esquerdo.
   - **Habilitar senha de substituição para o Agente do ZENworks:** Selecione essa opção para especificar uma senha de substituição que poderá ser usada no Agente do ZENworks para:
     - Acessar informações sobre o local atual do dispositivo e como o local foi atribuído.
     - Acessar as opções Administrativas no Agente de Segurança de Endpoint. Essas opções permitem desabilitar as políticas de segurança que estão aplicadas (com exceção da política de Criptografia de Dados), ver as informações detalhadas sobre a política e as informações de status do agente.

- Acessar as opções Administrativas no Agente de Criptografia de Disco Cheio. Essas opções permitem exibir informações detalhadas de políticas, exibir informações de status do agente e executar funções, como habilitar captura de usuários e decodificar volumes.
- Desinstalar o Agente do ZENworks.

- **Habilitar autodefesa para o Agente do ZENworks:** Selecione essa opção para habilitar a autodefesa. A funcionalidade de autodefesa protege apenas o ZENworks Endpoint Security Agent. Ela não protege os outros módulos do Agente do ZENworks.

  A autodefesa protege o Agente de Segurança de Endpoint contra encerramento, desabilitação ou adulteração de qualquer tipo. Se um usuário realiza qualquer uma das atividades a seguir, o dispositivo é reinicializado automaticamente para restaurar a configuração correta do sistema:

  - Uso do Gerenciador de Tarefas do Windows para terminar qualquer processo do Agente de Segurança de Endpoint.
  - Parada ou pausa de qualquer serviço do Agente de Segurança de Endpoint.
  - Remoção de arquivos essenciais e entradas do registro. Se uma mudança for feita em qualquer chave de registro ou valor associado ao Agente de Segurança de Endpoint, a chave de registro ou o valor será redefinido imediatamente.
  - Desabilitação da vinculação do driver de filtro NDIS aos adaptadores.

4 Para gravar as mudanças, clique em **OK**.

Instalando o Agente do ZENworks

As seguintes seções apresentam instruções sobre a instalação manual do Agente do ZENworks em dispositivos.

- “Instalação manual no Windows” na página 42
- “Instalação manual no Linux” na página 44
- “Instalação manual no Macintosh” na página 45

Observação: Além da instalação manual do Agente do ZENworks, você pode automatizar a instalação usando a descoberta e implantação de dispositivo de rede. O processo de descoberta e implantação não faz parte do escopo desta Inicialização Rápida. Para aprender como usar esse processo, consulte a *Referência de Descoberta, Implantação e Desativação do ZENworks*.

Instalação manual no Windows

1 Verifique se o dispositivo atende aos requisitos necessários (consulte “Requisitos de dispositivo gerenciado.”.

2 No dispositivo de destino, abra um browser da Web e navegue para o seguinte endereço:

`https://server:port/zenworks-setup`

Substitua *servidor* pelo nome DNS ou endereço IP de um servidor ZENworks e substitua a *porta* apenas se o servidor ZENworks não estiver usando a porta padrão (80 ou 443).

O browser da Web exibe uma lista dos pacotes de implantação para o Agente do ZENworks. Para cada arquitetura (32 e 64 bits), há os seguintes tipos de pacotes:

- **Rede (requer .NET):** O pacote de rede (requer .NET) instala apenas o pré-agente no dispositivo de destino; em seguida, o pré-agente faz download e instala o Agente do ZENworks a partir do Servidor ZENworks. O pacote de rede (requer .NET) requer o Microsoft .NET 4.0 ou posterior instalado no dispositivo antes da implantação do agente no dispositivo.
- **Independente (com .NET):** O pacote de rede independente (requer .NET) requer o Microsoft .NET Framework 4.0 ou posterior instalado no dispositivo antes da implantação do agente no dispositivo. Esse pacote contém todos os arquivos executáveis necessários para a instalação do Agente do ZENworks, exceto o instalador do Microsoft .NET.
- **Independente:** O pacote independente instala o pré-agente e extrai todos os arquivos executáveis necessários para a instalação do Agente do ZENworks, incluindo o instalador do Microsoft .NET no dispositivo de destino. O pré-agente instala o Agente do ZENworks do dispositivo local. O pacote independente é útil quando você precisa instalar o Agente do ZENworks em um dispositivo que, no momento, está desconectado da rede. Você pode gravar o pacote em uma mídia removível (CD, unidade flash USB, etc) e fazer com que o dispositivo independente execute o pacote a partir da mídia. O Agente do ZENworks é instalado no dispositivo, mas não ocorre nenhum registro ou gerenciamento até o dispositivo se conectar à rede.
- **Personalizada:** O nome do pacote, Agente Padrão, refere-se aos pacotes de implantação predefinidos. Os pacotes de implantação personalizados criados por meio de **Implantação** > **Editar Pacote de Implantação** são mostrados com o nome especificado durante a criação do pacote.

3 Clique no nome do pacote de implantação a ser usado e grave o pacote na unidade local do dispositivo ou execute-o no Servidor ZENworks.

4 Se tiver feito download do pacote, inicie-o no dispositivo.

Para obter informações sobre as opções que podem ser usadas com o pacote ao iniciá-lo de uma linha de comando, consulte "Opções de pacote para Windows, Linux e Macintosh" na *Referência de Descoberta, Implantação e Desativação do ZENworks*.

Importante: Se você instalar um pacote completo, a instalação do Windows Installer ou do .NET Framework poderá exigir reinicialização após iniciar o pacote. É exibida uma mensagem com várias opções na reinicialização. Selecione uma das seguintes opções:

- Não faça nada, e a reinicialização ocorrerá automaticamente após 5 minutos.
- Clique em **Cancelar**. Será necessário reinicializar posteriormente.
- Clique em **OK** para reinicializar imediatamente.

Quando o dispositivo é reinicializado, a instalação continua automaticamente.

---

5 Ao término da instalação, o dispositivo será reinicializado automaticamente se você tiver reinicializado o dispositivo na instalação do Windows Installer ou do .NET Framework.

Quando o dispositivo for reinicializado, ele será registrado na Zona de Gerenciamento e o ícone do ZENworks será inserido na área de notificação (bandeja do sistema).

No ZENworks Control Center, o dispositivo aparece na pasta `\Servidores` ou `\Estação de Trabalho` na página Dispositivos.

Para obter informações sobre como efetuar login e usar o Agente do ZENworks em um dispositivo, consulte “Usando o Agente do ZENworks” na página 46.

Instalação manual no Linux

Em vez de o Servidor ZENworks transferir o Agente do ZENworks para um dispositivo, você pode fazer download manualmente do pacote de implantação do Agente do ZENworks do servidor e instalar o agente.

Importante: Você poderá instalar o Agente do ZENworks no Linux se tiver permissões de root ou de administrador.

---

1. Verifique se o dispositivo atende aos requisitos necessários (consulte “Requisitos de dispositivo gerenciado” nos *Requisitos do Sistema do ZENworks 2020Update 1*).
2. No dispositivo de destino, abra um browser da Web e navegue para o seguinte endereço:

   `http://server:port/zenworks-setup`

   Substitua *servidor* pelo nome DNS ou endereço IP de um Servidor ZENworks e substitua a *porta* apenas se o Servidor ZENworks não estiver usando a porta padrão (80 ou 443).

   O browser da Web exibe uma lista de pacotes de implantação. Para cada arquitetura (32 e 64 bits), há os seguintes tipos de pacotes:

   - **Rede:** Esse pacote instala apenas o pré-agente no dispositivo de destino; em seguida, o pré-agente faz download e instala o Agente do ZENworks do Servidor ZENworks.
   - **Independente:** O pacote independente instala o pré-agente e extrai todos os arquivos executáveis necessários para a instalação do Agente do ZENworks, incluindo o instalador do JRE no dispositivo de destino. O pré-agente instala o Agente do ZENworks do dispositivo local. O pacote independente é útil quando você precisa instalar o Agente do ZENworks em um dispositivo que esteja desconectado da rede. Você pode gravar o pacote em uma mídia removível (por exemplo, CD ou unidade flash USB) e fazer com que o dispositivo independente execute o pacote da mídia. O Agente do ZENworks é instalado no dispositivo, mas não ocorre nenhum registro ou gerenciamento até o dispositivo se conectar à rede.
   - **Personalizada:** O nome do pacote, Agente Padrão, refere-se aos pacotes de implantação predefinidos. Os pacotes de implantação personalizados criados por meio de **Implantação** > **Editar Pacote de Implantação** são mostrados com o nome especificado durante a criação do pacote.
3. Clique no nome do pacote de implantação que deseja usar, grave o pacote na unidade local do dispositivo e conceda permissões de executável ao arquivo executando o comando `chmod 755 nome_do_arquivo`.

   Para obter informações sobre as opções que podem ser usadas com o pacote ao iniciá-lo de uma linha de comando, consulte “Opções de pacote para Windows, Linux e Macintosh” na *Referência de Descoberta, Implantação e Desativação do ZENworks*.
4. (Opcional) Em um dispositivo RHEL, execute o seguinte comando:

   `chcon -u system_u -t rpm_exec_t nome_do_arquivo`

5 Na janela de terminal, vá para o diretório no qual você fez download do pacote e inicie-o no dispositivo executando o comando `./nome_do_arquivo`, em que **nome_do_arquivo** é o nome do pacote do qual você fez o download na Etapa 3.

6 (Condicional) Para ver o ícone de notificação do ZENworks na área de notificação após a instalação do agente para o dispositivo Linux, efetue logout e login no dispositivo.

No ZENworks Control Center, o dispositivo aparece na pasta `\Servidores` ou `\Estação de Trabalho` na página Dispositivos.

Instalação manual no Macintosh

É possível implantar o Agente do ZENworks em um dispositivo Macintosh fazendo download do pacote de implantação pela página de download do ZENworks.

Importante

- Você poderá instalar o Agente do ZENworks em um dispositivo Macintosh se tiver permissões de root ou de administrador.

---

1 No dispositivo Macintosh de destino, abra um browser da Web e digite o seguinte endereço:

http://<servidor>/zenworks-setup

Substitua *<servidor>* pelo nome DNS ou endereço IP de um Servidor ZENworks.

2 Clique no pacote apropriado do Macintosh para fazer download.

Observação: Existem dois tipos de pacotes:

- **Rede:** Este pacote requer acesso por rede ao Servidor ZENworks para fazer download dos arquivos PKG necessários.
- **Independente:** O acesso ao Servidor ZENworks não é necessário para instalar o agente.

---

3 No prompt de comando, especifique as permissões executáveis nos arquivos `.bin` descarregados executando o comando `chmod +x<nome_do_arquivo>`.

Para obter mais informações sobre as opções que você pode usar com o pacote, consulte "Opções de pacote para Windows, Linux e Macintosh" na *Referência de Descoberta, Implantação e Desativação do ZENworks*.

4 No prompt de comando, vá para o diretório no qual você fez download do pacote e inicie-o no dispositivo executando o seguinte comando:

```
sudo ./filename
```

O `filename`é o nome do pacote que você fez download na Etapa 2 na página 45.

5 Efetue logout e login no dispositivo para ver o ícone de notificação do ZENworks na área de notificação após a instalação do agente no dispositivo Macintosh.

No ZENworks Control Center, o dispositivo aparece na pasta `\Servidores` ou `\Estação de Trabalho` na página Dispositivos.

Observação: Após implantar o Agente do ZENworks no dispositivo Macintosh, `/opt/novell/zenworks/bin` não será adicionado à variável PATH e, portanto, os comandos nesse diretório não poderão ser usados diretamente. Siga um dos procedimentos abaixo no dispositivo Macintosh para executar os comandos de `/opt/novell/zenworks/bin`:

- Efetue login novamente no dispositivo.
- Especifique o caminho completo para acessar o comando.

  Por exemplo: `/opt/novell/zenworks/bin/zac`.

Usando o Agente do ZENworks

As seções a seguir fornecem informações que o ajudarão a efetuar login e usar o Agente do ZENworks:

- "Efetuando login na zona de gerenciamento" na página 46
- "Navegando nas telas do Agente do ZENworks" na página 46
- "Promovendo um dispositivo gerenciado a satélite" na página 48

Efetuando login na zona de gerenciamento

Quando um dispositivo gerenciado pelo Windows inicializa o sistema operacional, o Agente do ZENworks é iniciado, e todos os bundles e políticas atribuídos ao dispositivo ficam disponíveis. Para que as políticas e os bundles atribuídos a um usuário estejam disponíveis, é necessário que o usuário efetue login na zona de gerenciamento.

O·Agente do ZENworks é integrado ao cliente de login do Windows ou da Novell para oferecer·uma única experiência de login aos usuários. Quando os usuários inserem suas credenciais do eDirectory ou do Active Directory no cliente do Windows ou da Novell, eles serão conectados à Zona de Gerenciamento se as credenciais corresponderem às existentes em uma origem de usuário do ZENworks. Do contrário, uma tela de login separada do Agente do ZENworks solicitará as credenciais corretas ao usuário.

Por exemplo, suponha que um usuário tenha contas em duas árvores do eDirectory: Árvore1 e Árvore2. A Árvore1 é definida como uma origem de usuário na zona de gerenciamento, mas a Árvore2 não. Se o usuário efetuar login na Árvore 1, ele será automaticamente conectado à Zona de Gerenciamento. Entretanto, se ele efetuar login na Árvore2, a tela de login do Agente do ZENworks será exibida e solicitará as credenciais da Árvore1 ao usuário.

Navegando nas telas do Agente do ZENworks

O Agente do ZENworks inclui as seguintes telas:

- "ZENworks Application" na página 47
- "ZENworks Explorer" na página 47
- "Ícone do ZENworks" na página 47

ZENworks Application

ZENworks Application é uma janela independente que permite o acesso aos bundles. Inicie a janela pelo menu Iniciar (menu **Iniciar** > **Programas** > **Novell ZENworks** > **ZENworks Application**).

O painel esquerdo do ZENworks Application exibe o seguinte:

- **Pasta [All]:** Contém todos os bundles distribuídos a você, independentemente da pasta em que estejam localizados.
- **Pasta do ZENworks:** Contém todos os bundles não atribuídos a uma pasta diferente. A pasta do ZENworks é a pasta padrão dos bundles; entretanto, os administradores podem criar pastas adicionais para a organização dos bundles e podem até renomear a pasta do ZENworks.
- **Pasta Favoritos:** Contém todos os bundles marcados como favoritos.

Quando você seleciona uma pasta no painel esquerdo, os bundles que estão na pasta aparecem no painel direito. Você pode:

- Instalar um bundle ou iniciar um aplicativo já instalado.
- Exibir as propriedades de um bundle. As propriedades incluem a descrição do bundle, as informações sobre quem deve ser contatado para obter ajuda com o bundle, quando o bundle estará disponível para uso e os requisitos do sistema estabelecidos para o bundle.
- Consertar um aplicativo instalado.
- Desinstalar um aplicativo. Esse é um recurso controlado pelo administrador que talvez não esteja habilitado.

ZENworks Explorer

O ZENworks Explorer é uma extensão do Windows Explorer e permite a exibição de bundles no Windows Explorer, na área de trabalho, no menu Iniciar, na barra de ferramentas Início Rápido e na área de notificação (bandeja do sistema). O gráfico a seguir mostra os bundles exibidos no Windows Explorer.

O gráfico a seguir mostra os bundles exibidos na área de trabalho.

As tarefas executadas nos bundles no ZENworks Window também podem ser executadas no ZENworks Explorer.

Ícone do ZENworks

O ícone do ZENworks está localizado na área de notificação (bandeja do sistema) do Windows. Você pode clicar no ícone para exibir a janela do Agente do ZENworks.

Para exibir as propriedades do agente, clique o botão direito do mouse no ícone do ZENworks e selecione Aplicativo Técnico. A janela Propriedades do Agente do ZENworks é exibida.

O painel de navegação esquerdo da janela de propriedades contém links para o status do Agente do ZENworks e os recursos:

- **Status:** Exibe informações como a última vez em que o agente contatou um Servidor ZENworks e se os recursos do Agente estão sendo executados.

- **Políticas:** Exibe as políticas atribuídas ao dispositivo e ao usuário que efetuou login, além de mostrar se a política está em vigor. Essa opção apenas será incluída se o ZENworks Configuration Management ou o ZENworks Endpoint Security Management estiver habilitado.
- **Bundles:** Exibe os bundles atribuídos ao dispositivo e o usuário conectado. Essa opção também exibe o status da instalação atual de cada bundle (disponível, fazendo download, instalando, etc.) e se o bundle está em vigor (o dispositivo atende aos requisitos de distribuição). Essa opção apenas será incluída se o ZENworks Configuration Management ou o ZENworks Patch Management estiver habilitado.
- **Inventário:** Exibe informações de inventário para o dispositivo. Você poderá ver detalhes do hardware, como o fabricante e o modelo de seus discos rígidos, de suas unidades de disco e de sua placa de vídeo. Você também pode ver detalhes do software, como os hotfixes e os patches instalados do Windows, e também números de versão e locais dos produtos de software instalados. Essa opção apenas será incluída se o ZENworks Configuration Management ou o ZENworks Asset Management estiver habilitado.
- **Segurança de endpoint:** Exibe as informações sobre o Agente de Segurança de Endpoint e o local que está sendo usado para determinar quais políticas de segurança serão aplicadas. Essa opção apenas será incluída se o ZENworks Endpoint Security Management estiver habilitado.
- **Gerenciamento remoto:** Exibe informações sobre os operadores remotos conectados no momento e as configurações de política de Gerenciamento Remoto em vigor para o dispositivo. Essa opção também permite iniciar uma sessão de gerenciamento e controlar as configurações de segurança da sessão. Essa opção apenas será incluída se o ZENworks Configuration Management estiver habilitado.
- **Satélite:** Exibe as informações da função de satélite de um dispositivo que é usado como Servidor Satélite. As funções de satélite incluem Coleção, Conteúdo, Autenticação, Criação de Imagens e Proxy de Junção.

  Esse recurso será exibido apenas se seu administrador do ZENworks tiver usado seu dispositivo como satélite.
- **Registro:** Exibe informações sobre o arquivo de registro do Agente do ZENworks, como a localização do arquivo de registro, o Servidor ZENworks para o qual será feito o upload do arquivo de registro do agente e o próximo horário programado para upload do registro. Essa opção também permite determinar o nível de gravidade das mensagens registradas.
- **Proxy do Windows** Exibe os resultados das atividades de descoberta e implantação executadas no dispositivo quando ele atua como Proxy do Windows no Servidor Principal do ZENworks.

Promovendo um dispositivo gerenciado a satélite

Satélite é um dispositivo gerenciado capaz de desempenhar algumas das funções que o Servidor Principal do ZENworks normalmente desempenha, incluindo autenticação, coleta de informações, distribuição de conteúdo e criação de imagens. Um Satélite pode ser qualquer dispositivo gerenciado pelo Windows, pelo Linux ou pelo Macintosh, mas não um Servidor Principal. Ao configurar um Satélite, você especifica quais funções ele vai desempenhar (Autenticação, Coleção, Conteúdo ou Criação de Imagens). Um Satélite também é capaz de desempenhar funções que podem ser adicionadas por produtos de terceiros que sejam snap-ins à estrutura do ZENworks

---

Observação: O ZENworks não permite mais promover um dispositivo de 32 bits à função de Servidor Satélite nem adicionar uma nova função a um Servidor Satélite de 32 bits existente.

Para obter informações detalhadas sobre Satélites e como promover um dispositivo gerenciado a Satélite, consulte “Satellites” (Satélites) na *ZENworks Primary Server and Satellite Reference* (Referência de Servidor Principal e Satélite do ZENworks).

5 Mensagens do sistema

O ZENworks permite monitorar a atividade na Zona de Gerenciamento por meio de mensagens do sistema.

Vendo mensagens do sistema

O sistema ZENworks gera mensagens normais (informativas), de aviso e de erro para ajudá-lo a monitorar as atividades, como a distribuição de softwares e a aplicação de políticas.

Cada Servidor ZENworks e Agente do ZENworks cria um registro das atividades associadas. Essas mensagens são exibidas no ZENworks Control Center em diversas áreas:

- **Registro das Mensagens do Sistema:** O registro de mensagens do sistema, que pode ser acessado ao selecionar **Painel > Mensagens do Sistema**, mostra as mensagens de todos os Servidores e Agentes do ZENworks na zona.
- **Registro de Mensagens de Dispositivo:** Um registro de mensagens do dispositivo, localizado na página Resumo referente a um servidor ou a uma estação de trabalho, exibe as mensagens geradas pelo Servidor ou Agente do ZENworks. Por exemplo, o registro de mensagens da Estação de Trabalho1 inclui todas as mensagens geradas pelo Agente do ZENworks nessa estação de trabalho.
- **Registro de Mensagem de Conteúdo:** Um registro de mensagens de conteúdo, localizado na página Resumo referente a um bundle ou a uma política, exibe apenas as mensagens do Servidor ou Agente do ZENworks associadas ao bundle ou à política. Por exemplo, o registro de mensagens do Bundle1 pode ter mensagens geradas por três Servidores ZENworks diferentes e 100 Agentes do ZENworks diferentes.

Vendo um resumo das mensagens

Você pode ver um resumo que mostra o número de mensagens geradas para os servidores, as estações de trabalho, os bundles e as políticas na zona.

1 No ZENworks Control Center, clique na guia **Início**.

O painel Resumo da Mensagem exibe o status de todos os servidores, as estações de trabalho, as políticas e os bundles na Zona de Gerenciamento. Por exemplo, se dois servidores tiverem mensagens críticas não confirmadas (mensagens que você ou outro administrador ainda não tenha confirmado como visualizadas), a coluna  exibirá o número 2. Ou se você tiver três bundles com mensagens de aviso e cinco bundles apenas com mensagens normais, a coluna  exibirá o número 3 e a coluna  exibirá o número 5. É possível fazer o seguinte com o resumo:

- Clique em um tipo de objeto para exibir sua pasta raiz. Por exemplo, clique em **Servidores** para exibir a pasta raiz Servidores (`/Servidores`).

- Para qualquer tipo de objeto, clique no número em uma de suas colunas de status ( ) para exibir uma listagem de todos os objetos que têm esse status no momento. Por exemplo, para ver a lista de servidores com status normal, clique no número na coluna .
- Para qualquer tipo de objeto, clique no número na coluna **Total** para exibir todos os objetos com mensagens críticas, de aviso ou normais. Por exemplo, clique em **Contagem** Total de **Servidores** para exibir uma lista de todos os servidores que têm algum tipo de mensagem.

Confirmando mensagens

Uma mensagem permanece em um registro de mensagens até que seja confirmada. Você pode confirmar mensagens individuais ou todas as mensagens no registro de mensagens de uma só vez.

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue na pasta `Servidores` até localizar um Servidor ZENworks.
3. Clique no servidor para exibir seus detalhes.
4. Na guia **Resumo**, localize o painel Registro de Mensagens.

   Esse painel lista todas as mensagens (informativas, de aviso e de erro) geradas pelo Servidor ZENworks. A tabela a seguir explica as várias maneiras de confirmar e apagar mensagens.

Tarefa	Etapas	Detalhes Adicionais
Confirmar uma mensagem	1. Clique na mensagem para exibir a caixa de diálogo Informações Detalhadas da Mensagem. 2. Clique em **Confirmar**.	Para não confirmar a mensagem, clique em **Concluído** para fechar a caixa de diálogo. Isso faz com que a mensagem permaneça na lista **Registro de Mensagens**.
Confirmar todas as mensagens	1. Na lista **Tarefas** localizada no painel de navegação esquerdo, clique em **Confirmar Todas as Mensagens**.	
Ver todas as mensagens confirmadas ou não confirmadas	1. Clique no botão **Avançado** para exibir a página Editar Registro de Mensagens.	Além de ver todas as mensagens confirmadas e não confirmadas, você também pode ver somente as mensagens com status ou data específica, ver mais detalhes das mensagens e confirmar mensagens. Clique no botão **Ajuda** na página Editar Registro de Mensagens para obter informações específicas sobre como executar tarefas nessa página.
Apagar uma mensagem	1. Clique na mensagem para exibir a caixa de diálogo Registro Detalhado da Mensagem. 2. Clique em **Apagar**.	Quando você apaga uma mensagem, ela é removida completamente do sistema do ZENworks.

Você também pode usar o comando `messages-acknowledge` no utilitário zman para confirmar as mensagens associadas a dispositivos, bundles e políticas. Para obter mais informações, consulte "Comandos de mensagem" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Onde encontrar mais informações

Para obter mais informações sobre mensagens do sistema, consulte "Using Message Logging" (Usando o registro de mensagens) na *ZENworks Control Center Reference* (Referência do ZENworks Control Center).

Criando uma lista de vigias

Se houver dispositivos, bundles ou políticas cujo status você deseja monitorar de perto, poderá adicioná-los à Lista de Vigias. Essa lista fornece as seguintes informações:

- **Agente:** Para servidores e estações de trabalho, mostra se o Agente do ZENworks do dispositivo está conectado no momento ( ) ou desconectado ( ).
- : Mostra se o objeto tem quaisquer mensagens críticas.

- **Tipo:** Exibe um ícone que representa o tipo do objeto. Por exemplo, um bundle pode ter um ícone  para mostrar que se trata de um bundle do Windows. Ou um dispositivo pode ter um ícone  para mostrar que se trata de um servidor. Você pode passar o mouse sobre o ícone para ver uma descrição.
- **Nome:** Exibe o nome do objeto. Você pode clicar no nome para ir para o registro de mensagens do objeto.

Para adicionar um dispositivo, um bundle ou uma política à Lista de Vigias.

1. No ZENworks Control Center, clique na guia **Início**.
2. No painel Lista de Avisos, clique em **Adicionar**, depois selecione o tipo de objeto (dispositivo, bundle ou política) que deseja adicionar à lista.
3. Na caixa de diálogo de seleção, selecione o objeto desejado e clique em **OK** para adicioná-lo à Lista de Avisos.

   Por exemplo, se você estiver adicionando servidores, procure e selecione um servidor.

Os objetos permanecem na Lista de Vigias até que sejam removidos.

6 Gerenciamento de Auditoria

O ZENworks permite registrar e ver as atividades executadas no sistema do ZENworks, usando o recurso Gerenciamento de Auditoria. O recurso Gerenciamento de Auditoria permite capturar vários eventos que ocorrem na zona. Os detalhes de um evento capturado podem ser usados para fins de segurança e conformidade, permitindo identificar quem fez o que e em qual sistema, quando algum evento importante acontece no ambiente. Usando esse recurso, é possível monitorar centralmente as atividades relacionadas a Servidores Principais, Servidores Satélites e dispositivos gerenciados.

Tipos de eventos de auditoria

Há dois tipos de eventos de auditoria do ZENworks:

- **Eventos de mudança:** Esses eventos capturam mudanças na configuração feitas na zona por meio do ZENworks Control Center ou dos utilitários de linha de comando zman. É possível capturar uma variedade de mudanças, desde modificações no bundle a modificações no sistema do ZENworks. Por exemplo, você pode configurar um evento de auditoria que registra a atividade do administrador atribuindo um bundle a determinado dispositivo.
- **Eventos do Agente** Esses eventos capturam ações que ocorrem nos dispositivos gerenciados pelo ZENworks. Eles também são chamados de eventos de Dispositivo.

Tanto os eventos de mudança quanto os de agente podem ser habilitados em todos os dispositivos na zona ou em dispositivos individuais.

Habilitando um evento

Para fazer a auditoria de um evento, você deve primeiro habilitá-lo no ZENworks Control Center. É possível habilitar o evento no nível da zona ou do dispositivo. Um evento que é habilitado no nível da zona é aplicado a todos os dispositivos na zona, e um evento que é habilitado no nível do dispositivo é aplicado apenas ao dispositivo selecionado.

1. Efetue login no ZENworks Control Center.
2. (Zona) Para habilitar eventos na zona, clique em **Configuração > Configurações da Zona de Gerenciamento > Gerenciamento de Auditoria**.

   ou

   (Dispositivos) Para habilitar eventos no dispositivo, clique em **Dispositivos > Dispositivos Gerenciados**. Localize o dispositivo nas pastas Servidores ou Estações de Trabalho, clique no objeto Dispositivo para exibir suas propriedades e clique em **Configurações > Gerenciamento de Auditoria**.

3 Clique em **Configuração de Eventos** para exibir a página da caixa de diálogo Configuração de Eventos.

4 Na guia **Eventos de Mudança** ou **Eventos do Agente**, clique em **Adicionar** para exibir a caixa de diálogo Adicionar Eventos de Mudança ou Adicionar Eventos de Agente.

   Para obter informações sobre as categorias de evento de mudança e de agente, consulte a *ZENworks Audit Management Reference* (Referência de Gerenciamento de Auditoria do ZENworks).

5 Expanda a árvore **Eventos de Mudança** ou **Eventos do Agente** e selecione o evento necessário.

6 Especifique as seguintes informações em **Configurações de Evento**:

   - **Classificação do Evento:** Com base na importância do evento, selecione **Crítico**, **Principal** ou **Informativo**.
   - **Dias para Manter:** Indique por quantos dias o evento deve ser mantido antes de ser purgado.
   - **Notification Types (Tipos de Notificação):** Especifique se a notificação deve ser enviada por e-mail, Detecção de SNMP, UDP ou para um arquivo local quando acontecer o evento. Se você selecionar **Registrar mensagem em um arquivo local**, defina as configurações de arquivo de registro local.

     É possível também selecionar todos os tipos de notificação. Para obter mais informações, consulte "Using Message Logging" (Usando o registro de mensagens).
   - (Eventos de Agente) Especifique a taxa de **Frequência de Amostra** em que os dados devem ser coletados para gerar os eventos de auditoria. Esse campo é exibido apenas quando um evento do ZENworks Endpoint Security Management ou um evento do Agente do ZENworks é selecionado.

7 Clique em **OK** para adicionar o evento.

É possível editar ou apagar um evento selecionando-o na página Configuração de Eventos e clicando em **Editar** ou **Apagar** na barra de menus. Para selecionar vários eventos de uma vez, pressione **Ctrl** e clique para selecioná-los.

Vendo um evento gerado

Quando ocorre um evento habilitado, um evento de auditoria é gerado.

Após a geração de um evento de auditoria, você poderá acessar os detalhes do evento nos seguintes locais:

- **Painel:** É possível ver os dados de auditoria no Painel do ZENworks Control Center. O Painel tem as seguintes guias:
  - **Painel:** Nessa guia, você vê um resumo dos eventos de auditoria ocorridos na zona. É possível ver os principais indicadores referentes aos eventos mais importantes e objetos afetados e analisar a tela do registro de eventos aplicando filtros. Por padrão, esse painel mostra uma visão geral dos eventos nas últimas 4 horas. Para ver mais dados, é possível mudar o período de tempo.
  - **Eventos (Registro de Auditoria):** Essa guia permite ver todos os eventos ocorridos na zona. As informações são exibidas em um formato parecido com o da página Configuração de Eventos. O total de eventos gerados em determinada categoria é exibido. Por exemplo, se

um evento **Gerenciamento de Atribuição de Bundle** tiver sido gerado, **1** será exibido na categoria Gerenciamento de Atribuição de Bundle na estrutura da árvore. Quando você clica no evento, os detalhes são exibidos no painel direito.

- **(Eventos de Mudança) Pastas de Objetos:** A guia **Auditoria** nas pastas de objetos (**Dispositivos**, **Bundles**, **Políticas** e **Usuários**) permite ver os eventos de auditoria gerados para todos os objetos na pasta selecionada. Por exemplo, você pode ver os eventos gerados para todos os bundles de uma pasta de bundles. Portanto, é possível ver todos os eventos relacionados a bundles na pasta de Bundles. As informações são classificadas de forma parecida que na página **Configuração de Eventos.** Você pode procurar os eventos ocorridos e, se precisar de mais informações, poderá clicar no evento para ver seus detalhes.
- **(Eventos de Mudança) Objetos:** É possível também ver os eventos de auditoria de um objeto na pasta de objetos. Por exemplo, se você selecionar determinado bundle em uma pasta de bundles, poderá ver os eventos gerados para esse bundle específico.
- **(Eventos do Agente) Pasta de Dispositivos:** A guia **Auditoria** na pasta **Dispositivos** permite ver os eventos que são gerados para determinado dispositivo (servidor ou estação de trabalho).

Para ver os detalhes dos eventos gerados:

1. Efetue login no ZENworks Control Center.
2. (Painel) Para ver os eventos no Painel, clique em **Painel** > **Eventos**.

   ou

   (Pasta de Objetos) Para ver os eventos de todos os objetos em uma pasta (por exemplo, uma pasta de dispositivos, de bundles ou de políticas), clique no link **Detalhes** da pasta e clique na guia **Auditoria**.

   ou

   (Objeto) Para ver os eventos de determinado objeto (por exemplo, dispositivo, bundle ou política), clique no objeto e, em seguida clique na guia **Auditoria**.

   (Pasta de Dispositivos) Para ver os eventos na pasta de Dispositivos, no painel esquerdo, clique em **Dispositivos**. Se o evento tiver sido executado em um servidor na zona, clique em **Detalhes** do servidor ou, se o evento tiver sido executado em um dispositivo gerenciado, clique em **Detalhes** da estação de trabalho. Em seguida, clique na guia **Auditoria** para ver a tela Eventos.
3. Clique na guia **Eventos de Mudança** ou **Eventos do Agente**.
4. Expanda a estrutura da árvore e navegue até a categoria relevante.

   Dependendo do número de eventos de auditoria configurados, o total relevante será exibido para a categoria.
5. Clique no evento.

   Os detalhes do evento gerado são exibidos no painel direito.

Observação: Para ver os detalhes do evento em uma nova janela, clique em 

II Administração de produtos

As seções a seguir apresentam informações que o ajudam a usar os produtos do ZENworks Antes de tentar qualquer uma das seções, você já deve ter concluído as tarefas de configuração na Parte I, “Configuração do sistema” na página 9.

7 Lista rápida

Após configurar sua Zona de Gerenciamento (consulte a Parte I, “Configuração do sistema” na página 9), convém revisar os conceitos e as tarefas das seções a seguir referentes a todos os produtos ZENworks que você tem, licenciados ou em avaliação:

Gerenciamento de Bens

O ZENworks Asset Management permite monitorar a conformidade com a licença de software, o uso do software e a propriedade do software por meio da alocação de licenças a dispositivos, sites, departamentos e centros de custo.

Tarefa	Detalhes
Ativar o Gerenciamento de Bens	Se você não ativou o Gerenciamento de Bens durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, faça isso antes de usar o produto. Para obter instruções, consulte “Ativando o Gerenciamento de Bens” na página 67.
Habilitar o Agente do ZENworks para executar as operações de Gerenciamento de Bens	O recurso Gerenciamento de Bens do agente é habilitado por padrão quando o ZENworks Asset Management é ativado (licença completa ou de avaliação). Verifique se o recurso Gerenciamento de Bens do agente ainda está habilitado. Além disso, para monitorar as licenças de software dos usuários (e não somente dos dispositivos), você precisará habilitar o recurso Gerenciamento de Usuários que, por padrão, fica desabilitado. Para obter instruções, consulte “Habilitando o Gerenciamento de Bens no Agente do ZENworks” na página 67.

Tarefa	Detalhes
Explorar dispositivos para coletar o inventário de software e hardware	Explore dispositivos para coletar inventários de software e hardware para os dispositivos. As informações de inventário podem ajudá-lo a tomar decisões sobre distribuição de software e upgrades de hardware. Essa tarefa deve ser feita antes de executar qualquer outra tarefa restante. Para obter instruções, consulte "Coletando inventário de software e hardware" na página 68.
Monitorar o uso do software	Gere esse relatório para analisar o volume e a frequência de uso dos produtos de software. Para obter instruções, consulte "Monitorando o uso do software" na página 69.
Monitorar a conformidade das licenças de software	Veja se os produtos de software instalados estão licenciados apropriadamente, sublicenciados ou superlicenciados. Para obter instruções, consulte "Monitorando a conformidade da licença" na página 70.
Alocar licenças	Aloque as licenças da sua organização para monitorar a propriedade e a distribuição das licenças. Você pode alocar licenças a dispositivos ou demográficos (sites, departamentos e centros de custo). Para obter instruções, consulte "Alocando licenças" na página 77.

Gerenciamento de Configurações

O ZENworks Configuration Management permite gerenciar a configuração de um dispositivo, incluindo a distribuição de software ao dispositivo, a aplicação das políticas de configuração do Windows, a criação e aplicação de imagens. Além disso, você pode coletar inventário de hardware e software de dispositivo para informar suas decisões de upgrade e compra e acessar os dispositivos remotamente para resolver problemas.

As tarefas a seguir podem ser realizadas conforme o necessário e em qualquer ordem.

Tarefa	Detalhes
Ativar o Gerenciamento de Configurações	Se você não ativou o Gerenciamento de Configurações durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, faça isso antes de usar o produto. Para obter instruções, consulte "Ativando o Gerenciamento de Configurações" na página 79.

Tarefa	Detalhes
Habilitar o Agente do ZENworks para executar as operações de Gerenciamento de Configurações	Para que o Agente do ZENworks execute as operações de Gerenciamento de Configurações no dispositivo, os recursos apropriados do agente devem ser habilitados. Esses recursos (Gerenciamento de Bundles, Gerenciamento de Imagem, Gerenciamento de Políticas, Gerenciamento Remoto e Gerenciamento de Usuários) são habilitados por padrão quando o ZENworks Configuration Management é ativado (licença completa ou de avaliação). Verifique se os recursos estão habilitados. Se preferir, caso não queira usar determinados recursos, você pode desabilitá-los. Para obter instruções, consulte "Habilitando o Gerenciamento de Configurações no Agente do ZENworks" na página 80.
Registrar Dispositivos Móveis	Para permitir as operações de Gerenciamento de Configurações em dispositivos móveis, como implantar bundles, aplicar políticas de segurança e várias operações de gerenciamento de dispositivo, você precisa registrar os dispositivos móveis na Zona de Gerenciamento do ZENworks. Para obter instruções, consulte a ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).
Distribuir softwares	Distribua o software por meio de bundles. Os bundles contêm as instruções e os arquivos necessários para instalar, iniciar e desinstalar o software (quando necessário). Você pode criar bundles para distribuir aplicativos do Windows Installer (MSI e MSP), aplicativos que não são do Windows Installer, links da Web, aplicativos thin client, aplicativos Linux e Macintosh. Para obter instruções, consulte "Distribuindo software" na página 80.
Aplicar políticas	Controle o comportamento do dispositivo por meio da aplicação de políticas. O ZENworks permite criar e aplicar políticas de Grupo do Windows, políticas de perfil de roaming, políticas de marcador de browser, políticas de impressora e outras. Para obter instruções, consulte "Aplicando políticas" na página 82.
Obter imagens de dispositivos e aplicar imagens a eles	Crie imagens de dispositivos, aplique imagens a dispositivos e execute neles scripts de criação de imagem. O ZENworks Configuration Management usa sua funcionalidade Preboot Services para executar essas tarefas de criação de imagem em dispositivos na inicialização. Para obter instruções, consulte "Dispositivos de criação de imagens" na página 85.
Explorar dispositivos para coletar o inventário de software e hardware	Explore dispositivos para coletar inventários de software e hardware para os dispositivos. As informações de inventário podem ajudá-lo a tomar decisões sobre distribuição de software e upgrades de hardware. Para obter instruções, consulte "Coletando inventário de software e hardware" na página 104.

Gerenciamento de Segurança de Endpoint

O ZENworks Endpoint Security Management permite proteger os dispositivos impondo configurações de segurança por meio de políticas. É possível controlar o acesso de um dispositivo a dispositivos de armazenamento removível, redes wireless e aplicativos. Além disso, é possível proteger os dados por criptografia e a comunicação de rede por imposição de firewall (portas, protocolos e listas de controle de acesso). Você também pode mudar a segurança de um dispositivo de endpoint com base em seu local.

As seguintes tarefas devem ser executadas na ordem listada.

Tarefa	Detalhes
Ativar o Gerenciamento de Segurança de Endpoint	Se você não ativou o Gerenciamento de Segurança de Endpoint durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, faça isso antes de usar o produto. Para obter instruções, consulte “Ativando o Gerenciamento de Segurança de Endpoint” na página 115.
Habilitar o Agente de Segurança de Endpoint	O Endpoint Security Agent assegura o uso obrigatório das políticas de segurança nos dispositivos. Ele deve ser instalado e habilitado em cada dispositivo ao qual deseja distribuir as políticas de segurança. Para obter instruções, consulte “Habilitando o Agente de Segurança de Endpoint” na página 116.
Criar locais	As políticas de segurança podem ser globais ou específicas aos locais. Uma política global é aplicada a todos os locais. Uma política baseada em local é aplicada apenas quando o Agente de Segurança de Endpoint determina que o ambiente de rede do dispositivo corresponde ao ambiente definido para o local. Para usar políticas baseadas em local, é necessário criar os locais. Para obter instruções, consulte “Criando locais” na página 116.
Criar políticas de segurança	As configurações de segurança de um dispositivo são definidas por meio de políticas de segurança. Há 11 tipos de políticas de segurança que você pode criar. Para obter instruções, consulte “Criar uma diretiva de segurança” na página 117.
Atribuir políticas a usuários e dispositivos	Políticas de segurança podem ser atribuídas a usuários ou dispositivos. Para obter instruções, consulte “Atribuindo uma política a usuários e dispositivos” na página 119.

Tarefa	Detalhes
Atribuir políticas a zonas	Para garantir que um dispositivo esteja sempre protegido, é possível definir políticas de segurança padrão para cada tipo de política, atribuindo políticas à zona. Uma política atribuída por zona é aplicada quando o dispositivo não é coberto por uma política atribuída por usuário ou dispositivo. Para obter instruções, consulte “Atribuindo uma política à zona” na página 120.

Criptografia de Disco Cheio

O ZENworks Full Disk Encryption protege os dados do dispositivo contra acesso não autorizado quando o dispositivo é desligado ou entra no modo de hibernação. Para fornecer proteção de dados, todo o disco ou partição é criptografado, incluindo arquivos temporários, arquivos de troca e o sistema operacional. É possível acessar os dados somente quando um usuário autorizado efetua login, e os dados nunca podem ser acessados inicializando o dispositivo a partir de mídia, como CD/DVD, disquete ou unidade USB. Para o usuário autorizado, o acesso aos dados em disco criptografado é igual ao acesso aos dados em um disco não criptografado.

As seguintes tarefas devem ser executadas na ordem listada.

Tarefa	Detalhes
Ativar Criptografia de Disco Cheio	Se você não ativou a Criptografia de Disco Cheio durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, faça isso antes de usar o produto. Para obter instruções, consulte “Ativando a criptografia de disco cheio” na página 123.
Habilitar o Agente de Criptografia de Disco Cheio	O Agente de Criptografia de Disco Cheio realiza a criptografia do disco. Ele deve estar instalado e habilitado em cada dispositivo no qual os discos serão criptografados. Para obter instruções, consulte “Habilitando o agente de criptografia de disco cheio” na página 124.
Criar uma política de Criptografia de Disco	As informações necessárias para criptografar discos dos dispositivos são passadas para o Agente de Criptografia de Disco Cheio pela política de Criptografia de Disco. Você deve criar pelo menos uma política. Para obter instruções, consulte “Criando uma política de criptografia de disco” na página 124.
Atribuir a política aos dispositivos	Políticas de Criptografia de Disco podem ser atribuídas somente a dispositivos, grupos de dispositivos ou pastas de dispositivos. Para obter instruções, consulte “Atribuindo a política aos dispositivos” na página 125.

Gerenciamento de Patch

O ZENworks Patch Management permite automatizar o processo de avaliação das vulnerabilidades do software e aplicação de patches para eliminá-las.

As seguintes tarefas devem ser executadas na ordem listada.

Tarefa	Detalhes
Ativar o Gerenciamento de Patch	Se o Gerenciamento de Patch não foi ativado durante a instalação da Zona de Gerenciamento do ZENworks, seja por meio da licença de assinatura ou ativando a avaliação, você precisará ativar o produto. Para obter instruções, consulte “Ativando o gerenciamento de patch” na página 132.
Habilitar o Agente do ZENworks para executar as operações de Gerenciamento de Patch	Para que o Agente do ZENworks execute as operações de Gerenciamento de Patch no dispositivo, o recurso Gerenciamento de Patch do agente deve ser habilitado. O recurso Gerenciamento de Patch é habilitado por padrão quando o ZENworks Patch Management é ativado (licença completa ou de avaliação). Verifique se o recurso Gerenciamento de Patch do agente está habilitado. Para obter instruções, consulte “Habilitando o gerenciamento de patch no Agente do ZENworks” na página 132.
Iniciar o serviço de assinatura	Inicie o serviço de assinatura no Servidor ZENworks. Esse servidor faz download de patches e os replica para os outros Servidores ZENworks (se tiver mais de um). Para obter instruções, consulte “Iniciando o serviço de assinatura de patch” na página 133.
Criar políticas de patch	Depois que o serviço de assinatura fizer download dos patches, aplique os patches desejados. Para obter instruções, consulte “Criando políticas de patch” na página 133.

8 Gerenciamento de Bens

As seções a seguir apresentam explicações e instruções para uso do ZENworks Asset Management para coletar inventário de software e hardware dos dispositivos, monitorar o uso do software nos dispositivos e a conformidade com a licença do software.

Ativando o Gerenciamento de Bens

Caso não tenha ativado o Gerenciamento de Bens durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, execute as seguintes etapas:

1. No ZENworks Control Center, clique em **Configuração**.
2. No painel Licenças, clique em **ZENworks 2020 Asset Management**.
3. Selecione Avaliar/Ativar o produto e preencha os seguintes campos:

   Avaliação de Uso: Selecione essa opção para habilitar um período de avaliação de 60 dias. Após esse período, você deve inserir a chave de licença para continuar usando o produto.

   Chave de Licença do Produto: Especifique a chave de licença que você adquiriu para o Gerenciamento de Bens. Para comprar a licença de um produto, consulte o site do produto ZENworks Asset Management (http://www.novell.com/products/zenworks/assetmanagement).
4. Clique em **OK**.

Habilitando o Gerenciamento de Bens no Agente do ZENworks

Para que o Agente do ZENworks execute as operações de Gerenciamento de Bens no dispositivo, o recurso Gerenciamento de Bens do agente deve ser habilitado. O recurso Gerenciamento de Bens é habilitado por padrão quando o ZENworks Asset Management é ativado (licença completa ou de avaliação).

Verifique se o recurso Gerenciamento de Bens do agente está habilitado. Além disso, para monitorar as licenças de software dos usuários (e não somente dos dispositivos), você precisará habilitar o recurso Gerenciamento de Usuários que, por padrão, fica desabilitado. Para obter instruções, consulte "Configurando recursos do Agente do ZENworks" na página 39.

Observação: Após habilitar o módulo ZENworks Asset Management, imponha uma exploração completa em todos os dispositivos executando o comando `zac inv -f scannow`. Até você executar a exploração, o relatório de Gerenciamento de Bens não será preciso.

Coletando inventário de software e hardware

Quando você faz o inventário de um dispositivo, o ZENworks Asset Management coleta informações de software e hardware do dispositivo. Usando o ZENworks Control Center, você pode ver o inventário de um dispositivo individual ou gerar relatórios de vários dispositivos com base em critérios específicos.

É possível usar o inventário de software para várias finalidades, incluindo monitorar o uso de aplicativos específicos e garantir que haja licenças suficientes para todas as cópias do aplicativo em uso. Por exemplo, suponha que sua empresa possua 50 licenças de um software de processamento de texto. Você faz um inventário de software e descobre que ele está instalado em 60 dispositivos, o que significa que você não está em conformidade com seu contrato de licença. Porém, após examinar o uso do software nos últimos 6 meses, você verá que ele está realmente sendo usado em apenas 45 dispositivos. Para ficar em conformidade com o contrato de licença, você desinstala o software dos 15 dispositivos que não o estão usando.

Também é possível usar o inventário de hardware para várias finalidades, incluindo garantir que seu hardware cumpra os requisitos para executar um software específico. Por exemplo, suponha que seu departamento de Contabilidade deseja implantar uma nova versão de seu software contábil. O novo software tem requisitos maiores de processador, memória e espaço em disco. Usando o inventário de hardware coletado de seus dispositivos, você pode criar dois relatórios: um com todos os dispositivos que cumprem os requisitos e um com os dispositivos que não cumprem os requisitos. Com base nos relatórios, distribua o software para os dispositivos compatíveis e crie um plano de upgrade para os dispositivos não compatíveis.

Por padrão, os dispositivos são automaticamente explorados à 1 h no primeiro dia do mês. Você pode modificar a programação, bem como muitas outras definições de configuração de **Inventário**, na guia **Configuração** do ZENworks Control Center.

As seções a seguir fornecem instruções para iniciar a exploração de um dispositivo e usar o inventário coletado:

- “Iniciando a exploração de um dispositivo” na página 68
- “Vendo um inventário de dispositivo” na página 69
- “Gerando um relatório de inventário” na página 69
- “Onde encontrar mais informações” na página 69

Iniciando a exploração de um dispositivo

Você pode iniciar a exploração de um dispositivo a qualquer momento.

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue até a pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo que você deseja explorar.
3. Clique no dispositivo para exibir seus detalhes.

4 Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Exploração de Inventário do Servidor** ou **Exploração de Inventário da Estação de Trabalho** para iniciar a exploração.

   A caixa de diálogo Status da Tarefa Rápida exibe o status da tarefa. Quando a tarefa é concluída, você pode clicar na guia **Inventário** para ver os resultados da exploração.

Para explorar vários dispositivos ao mesmo tempo, abra a pasta em que estão localizados os dispositivos, marque as caixas de seleção ao lado dos dispositivos e clique em **Tarefas Rápidas** > **Exploração de Inventário**.

Você também pode usar o comando `inventory-scan-now` no utilitário zman para explorar um dispositivo. Para obter mais informações, consulte "Comandos de inventário" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Vendo um inventário de dispositivo

1 No ZENworks Control Center, clique na guia **Dispositivos**.
2 Navegue na pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo cujo inventário você deseja ver.
3 Clique no dispositivo para exibir seus detalhes.
4 Clique na guia **Inventário**.

   A página Inventário fornece um resumo do inventário de hardware. Para ver informações detalhadas do inventário, clique em **Inventário Detalhado de Hardware/Software**.

Gerando um relatório de inventário

O ZENworks Asset Management contém vários relatórios padrão. Além disso, você pode criar relatórios personalizados para fornecer diferentes exibições das informações de inventário.

1 No ZENworks Control Center, clique na guia **Relatórios**.
2 No painel Relatórios de Inventário Padrão, clique em **Aplicativos de Software**.
3 Clique no relatório **Sistema Operacional** para gerar o relatório.

   Usando as opções localizadas na parte inferior do relatório, você pode gravar o relatório gerado como uma planilha do Microsoft Excel, um arquivo CSV (comma-separated values - valores separados por vírgula), um arquivo PDF ou um arquivo gráfico PDF.

Onde encontrar mais informações

Para obter mais informações sobre inventário, consulte a *Referência do Asset Inventory do ZENworks*.

Monitorando o uso do software

Depois de fazer o inventário dos dispositivos, você poderá executar relatórios para ver com que frequência os aplicativos dos dispositivos são usados. O ZENworks Asset Management inclui relatórios padrão para o uso do aplicativo por produto, usuário e dispositivo. Também é possível

personalizar os relatórios para fornecer informações mais detalhadas ou com um foco específico. Por exemplo, o Gerenciamento de Bens inclui um relatório personalizado predefinido que mostra aplicativos não usados nos últimos 90 dias.

Para executar um relatório que mostra a frequência de uso de um aplicativo específico:

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Uso do Software**.
2. No painel do Padrão de Uso de Software, clique em **Uso do Aplicativo** para exibir a lista dos relatórios de uso dos aplicativos.
3. No painel, clique em **Uso Local do Aplicativo por Produto**.

   O relatório mostra todos os produtos que estão instalados no dispositivo, agrupados por fabricante.
4. Encontre um fabricante cujos produtos você queira ver e clique no número da coluna Instalações para exibir os produtos instalados.

   O relatório resultante mostra o número atual de instalações para cada produto, quantas instalações foram usadas, quando foram usadas pela última vez e outras informações de uso.
5. Se desejar mudar o período do relatório ou a lista de produtos exibidos (todos os produtos, produtos usados ou produtos não usados), clique em **Mudar Período/Filtros** na parte inferior do relatório.

Há muitos outros relatórios padrão e personalizados predefinidos que você pode usar. Para obter informações adicionais sobre o uso do aplicativo, consulte “Relatórios” na *Referência do ZENworks Asset Management*.

Monitorando a conformidade da licença

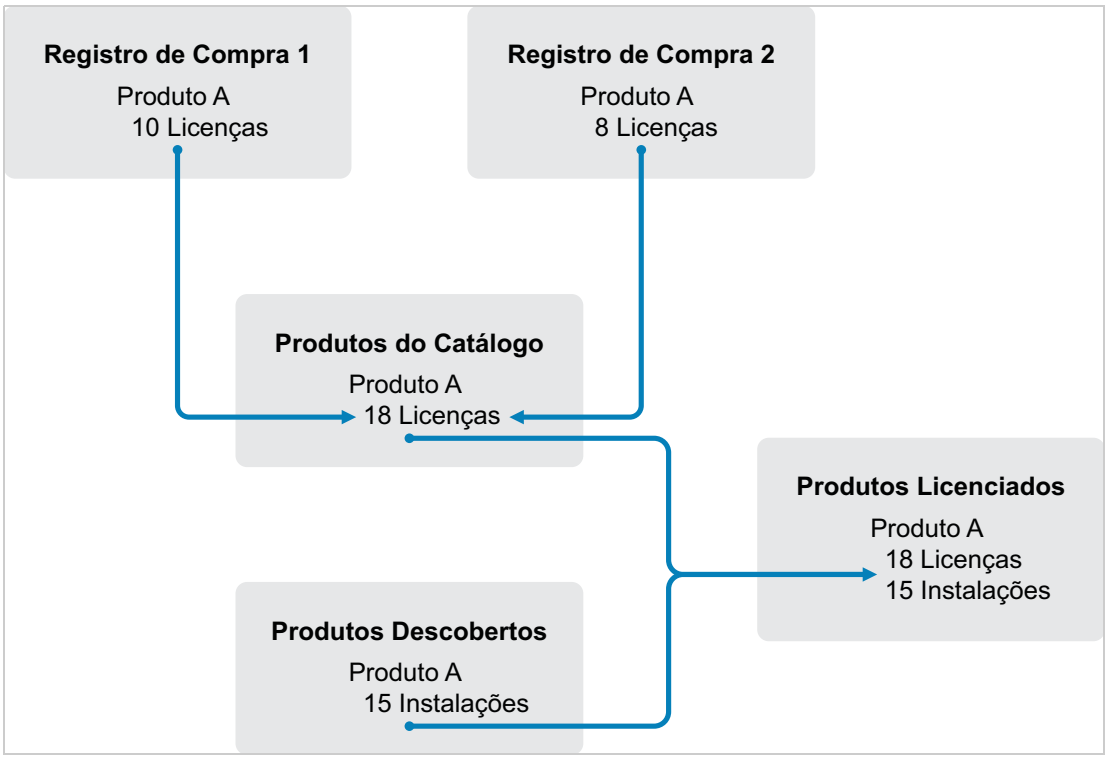
O ZENworks Asset Management permite monitorar a conformidade da sua organização com os contratos de licença de software, comparando as licenças de software adquiridas com as instalações de software reais que foram descobertas durante as explorações de inventário.

A conformidade de licença do Gerenciamento de Bens é uma ferramenta eficiente e flexível. Por isso, você pode usar várias abordagens e métodos ao configurar a conformidade de licença. As seções a seguir fornecem instruções básicas em breves explicações para ajudá-lo a configurar rapidamente um único produto para a monitoração de conformidade de licença. Após concluir esse cenário básico, consulte “Conformidade de licença” na *Referência do ZENworks Asset Management* para obter informações e instruções mais detalhadas.

Componentes de conformidade da licença

Antes de começar a implementar o monitoramento da conformidade, é necessário compreender os componentes envolvidos e como eles funcionam juntos, conforme está explicado na ilustração a seguir e no texto subsequente.

Figura 8-1 *Componentes de conformidade da licença*



- Explore os dispositivos da sua Zona de Gerenciamento para coletar a lista de produtos de software instalados. Eles são chamados de *produtos descobertos*. Na ilustração acima, a exploração de inventário descobriu que o Produto A está instalado em 15 dispositivos.
- Crie *produtos do catálogo* para representar os produtos de software adquiridos pela sua organização. Em geral, cada produto do catálogo corresponde a um número de peça específico do fabricante. Na ilustração acima, o Produto A é o único produto do catálogo. Entretanto, você pode ter produtos do catálogo para o Produto A, o Upgrade do Produto A e o Produto B.
- Crie *registros de compra* para representar as ordens de compra ou faturas dos produtos de software. Cada item de linha do registro de compra lista um produto do catálogo, juntamente com a quantidade de compra de licença. Se um produto do catálogo estiver listado em vários registros de compra, o total de licenças do produto do catálogo será igual à quantidade de compra de todos os registros. Na ilustração acima, um registro de compra inclui 10 licenças do Produto A, e outro registro de compra inclui oito licenças. A quantidade total de licenças do Produto A é de 18 unidades.
- Crie *produtos licenciados* e associe os produtos descobertos e produtos do catálogo correspondentes a eles. Isso compõe um único produto licenciado que inclui o número de licenças e de instalações desse produto. O resultado é uma visão rápida da conformidade ou

não do uso do produto com o contrato de licença. Na ilustração acima, o Produto A tem 18 licenças e está instalado em 15 dispositivos, portanto está em conformidade com seu contrato de licença.

Descobrindo produtos instalados

Se você ainda não tiver explorado os dispositivos da sua Zona de Gerenciamento para coletar informações sobre os produtos instalados (chamados de **produtos descobertos**), execute as etapas da "Coletando inventário de software e hardware" na página 68.

Depois que tiver os produtos descobertos, escolha aquele cuja conformidade deseja monitorar.

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Gerenciamento de Licença**.
2. No painel Gerenciamento de Licença, clique em **Produtos Descobertos** para exibir a lista Produtos Descobertos.
3. Percorra a lista para escolher o produto descoberto a ser usado.

   O produto deve ter pelo menos uma instalação listada na coluna **Quantidade Instalada.** Se possível, escolha um produto para o qual possui uma ordem de compra ou uma fatura prontamente disponível. Isso lhe permitirá concluir o cenário usando informações reais. Caso contrário, você poderá inventar as informações de compra à medida que avançar. Lembre-se do produto escolhido para poder usá-lo posteriormente.
4. Prossiga com a próxima seção, "Criando um produto de catálogo e um registro de compra" na página 72.

Criando um produto de catálogo e um registro de compra

Os produtos descobertos fornecem as informações de instalação dos produtos. Para fornecer informações sobre compras de produtos, crie produtos de catálogo e registros de compra.

Um produto de catálogo representa um produto de software. Um registro de compra preenche o produto de catálogo com o número de licenças de produto adquiridas.

As etapas a seguir explicam como criar um produto de catálogo e um registro de compra para o produto descoberto escolhido na "Descobrindo produtos instalados" na página 72.

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Gerenciamento de Licença**.
2. Crie o produto de catálogo:
   - **2a** No painel Gerenciamento de Licenças, clique em **Produtos do Catálogo**.
   - **2b** Clique em **Novo** > **Produto do Catálogo** para abrir o Assistente de Criação de Novo Produto do Catálogo.
   - **2c** Preencha os campos a seguir:

     Fabricante: Selecione o fabricante de software da lista. Se o fabricante correto não estiver listado, digite o nome dele (por exemplo, Novell, Symantec ou Microsoft).

Produto: Digite o nome do produto. O produto deve representar o SKU (software product package - pacote de produtos de software) adquirido. Por exemplo, o pacote adquirido pode ser Licença Única do Produto A ou Pacote de 10 Licenças do Produto A. Se você tiver um registro de fatura que inclua o produto para o qual está criando o produto de catálogo, use o nome do produto que consta na fatura.

Licenças por Pacote: Especifique o número de licenças incluídas no pacote do produto.

Tipo de Produto - Notas: Esses campos são opcionais. Você pode usá-los para identificar ainda mais o produto.

Excluído: Não marque esta caixa de seleção.

2d Clique em **Avançar** para exibir a página Resumo e clique em **Concluir** para adicionar o produto à lista Produtos do Catálogo.

2e Clique em **Gerenciamento de Licença** (no caminho de navegação localizado na parte superior da página) para retornar à página Gerenciamento de Licença.

3 Crie o registro de compra:

3a No painel Gerenciamento de Licença, clique em **Registros de Compra**.

3b Clique em **Novo** > **Registro de Compra** para abrir o Assistente de Criação de Novo Registro de Compra.

3c Preencha os campos a seguir:

Número de PO: Especifique o número da ordem de compra ou da fatura associado à compra do produto de software. Se você não tiver PO ou fatura para esse produto, use qualquer número.

Data do pedido: Selecione a data em que o software foi comprado.

Destinatário - Revendedor: Esses campos são opcionais. Você pode usá-los para identificar ainda mais o registro de compra.

3d Clique em Próximo para exibir a página Resumo.

3e Marque a caixa **Definir Propriedades Adicionais** e clique em **Concluir** para criar o registro de compra e exibir a página Detalhes de Compra do registro.

3f Clique em **Adicionar** para exibir a caixa de diálogo Adicionar Detalhe de Compra e, em seguida, preencha os seguintes campos:

Produto: Clique em  para procurar e selecionar o produto de catálogo criado na Etapa 2.

Quantidade: Especifique a quantidade do produto comprado. Por exemplo, se o produto do catálogo que você selecionou é Produto A - pacote com 10 unidades e a ordem de compra se referia a 5 pacotes com 10 unidades do Produto A, especifique 5.

Preço Unitário Sugerido - Preço Estendido: Esses campos são necessários. Especifique o preço de varejo sugerido pelo fabricante (MSRP - manufacturer's suggested retail price), o preço pago por unidade e o preço estendido. Se você deixar o campo **Preço Estendido** em branco, o assistente o preencherá multiplicando a **Quantidade da Compra** pelo **Preço Unitário**.

Nº da Fatura - Comentários: Esses campos são opcionais. Você pode usá-los para identificar melhor a compra.

3g Clique em **OK**.

4 Prossiga com a próxima seção, Criando um produto licenciado.

O Gerenciamento de Bens também pode importar informações de compra dos arquivos eletrônicos. Durante o processo, o registro de compra é criado, assim como quaisquer produtos de catálogo referentes aos produtos de software incluídos no registro de compra. Para obter mais informações, consulte "Conformidade de licença" na *Referência do ZENworks Asset Management*.

Criando um produto licenciado

A última etapa da configuração da conformidade para o produto de software é criar um produto licenciado e associar a ele o produto descoberto e o produto de catálogo. Assim, o produto da licença é preenchido com as informações necessárias de instalação e licença a fim de determinar seu status de conformidade de licença.

As seguintes etapas explicam como usar o Assistente de Reconciliação Automática para criar o produto licenciado e associar a ele o produto descoberto e o produto de catálogo.

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Gerenciamento de Licença**.
2. No painel Gerenciamento de Licença, clique em **Produtos Licenciados**.
3. No painel Produtos Licenciados, clique em **Ação > Reconciliação Automática: Criar Produtos Licenciados** para iniciar o Assistente de Reconciliação Automática. Preencha o assistente usando informações da tabela a seguir para preencher os campos.

Página do Assistente	Detalhes
Filtro de Produto Descoberto	O Auto-Reconcile Wizard (Assistente de Reconciliação Automática) cria produtos licenciados a partir dos produtos descobertos existentes. Para localizar seu produto descoberto: 1. Clique na opção **Produtos Especificados Abaixo**. 2. Na lista **Selecionar**, selecione o fabricante do seu produto descoberto. 3. No campo **Produto**, digite o nome do seu produto descoberto.
Selecionar Produtos Licenciados a Serem Criados	De acordo com as informações especificadas na página Filtro de Produtos Descobertos, essa página deverá exibir o seu produto descoberto e o produto licenciado que será criado para ele. O assistente tenta encontrar correspondência entre os produtos de catálogo e o produto descoberto, comparando os campos Fabricante e Produto. Se ele conseguir encontrar correspondência entre o produto de catálogo que você criou e o produto descoberto, o produto de catálogo também será listado. Selecione o produto de catálogo para associá-lo ao produto licenciado. Se o assistente não conseguir encontrar correspondência entre o produto de catálogo e o produto descoberto, será preciso atribuir manualmente o produto de catálogo após a conclusão do assistente.

Página do Assistente	Detalhes
Pasta de Destino	Selecione a pasta em que deseja colocar o novo produto licenciado. O campo assume como padrão a pasta atual (a pasta da qual foi iniciado o Auto-Reconcile Wizard (Assistente de Reconciliação Automática)). Para especificar outra pasta, clique em  para procurar e selecionar a pasta. A pasta já deverá existir; não é possível usar a caixa de diálogo de seleção para criar uma nova pasta.
Direitos de Licença	Todo produto licenciado deve ter pelo menos um modelo de direito e licença. Um direito normalmente representa um contrato de licença. Em muitos casos, um produto licenciado pode ter apenas um direito. Contudo, ao permitir vários direitos, você pode determinar a conformidade de um produto licenciado que tenha vários contratos de licença. Por exemplo, você pode ter um contrato de licença completa e um contrato de licença de upgrade para o mesmo produto. Em vez de criar dois produtos licenciados separados para o mesmo produto, crie um único produto licenciado com dois direitos diferentes. O modelo de licença determina como as licenças são contadas. Elas podem ser contadas por instalação, usuário ou dispositivo. Para esse cenário, especifique **Por Instalação** como descrição e selecione **Por Instalação** como modelo de licença. Isso faz cada instalação do produto consumir uma licença.
Reconciliação Automática - Criar Resumo	Analise seus dados.

4 Se ainda não tiver feito isso, clique em **Concluir** para criar o produto licenciado e adicioná-lo à lista Produtos Licenciados.

5 Se o Auto-Reconcile Wizard (Assistente de Reconciliação Automática) não conseguir associar seu produto de catálogo ao produto licenciado:

5a Clique no produto licenciado.

5b Clique na guia **Direitos da Licença**.

5c No painel Direitos, clique no direito.

5d Clique na guia **Prova de Propriedade**.

5e No painel Produtos do Catálogo, clique em **Adicionar**.

5f Selecione o produto de catálogo e clique em **OK** para adicioná-lo ao painel Produtos do Catálogo.

O painel Produtos do Catálogo exibe a Quantidade da Compra do produto de catálogo, que é o número de unidades do produto de catálogo que você comprou (de acordo com o registro de compra). Ele também exibe a Quantidade de Licenças, que é o número total de licenças incluídas nas unidades adquiridas.

6 Continue na próxima seção, Vendo dados de conformidade, para obter informações sobre como monitorar a conformidade.

Vendo dados de conformidade

É possível usar duas telas para ver o status de conformidade dos seus produtos licenciados. Você pode ver a página Produtos Licenciados para obter um resumo do status da conformidade de todos os produtos ou pode gerar o relatório Conformidade de Software para ver informações mais detalhadas.

- "Vendo o resumo do status da conformidade" na página 76
- "Gerando o relatório de conformidade do software" na página 76

Vendo o resumo do status da conformidade

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Gerenciamento de Licença**.
2. No painel Gerenciamento de Licença, clique em **Produtos Licenciados** para exibir a página Produtos Licenciados.

   A lista Produtos Licenciados exibe todos os produtos licenciados e o status de sua conformidade atual:

   - O produto de software está licenciado apropriadamente. O número de licenças compradas é igual ao número de instalações.
   - O produto de software está superlicenciado. Há mais licenças compradas do que instalações.
   - O produto de software está sublicenciado. Há menos licenças compradas do que instalações.

Gerando o relatório de conformidade do software

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens** e, em seguida, clique na guia **Gerenciamento de Licença**.
2. No painel Gerenciamento de Licença, clique em **Gerenciamento de Licença**.
3. No painel do Padrão de Gerenciamento de Licenças, clique em **Conformidade do Software**.
4. No painel, clique em **Relatório de Conformidade**.

   Um relatório é exibido contendo os dados de conformidade por licença. Os dados podem ser filtrados por status de conformidade, fabricante e valor ou critérios demográficos. Vá para **Quantidade de Licenças** para ver os detalhes de conformidade de um produto licenciado específico. Para obter outras informações, consulte a *Referência do ZENworks Asset Management*.

Onde encontrar mais informações

O cenário descrito nas seções anteriores mostra apenas uma pequena parte da funcionalidade de conformidade de licença disponível no ZENworks Asset Management. Para obter mais informações, consulte "Conformidade de licença" na *Referência do ZENworks Asset Management*.

Alocando licenças

O ZENworks Asset Management permite alocar as licenças da sua organização com o objetivo de monitorar a propriedade e a distribuição das licenças. Você pode alocar licenças a dispositivos ou demográficos (sites, departamentos e centros de custo).

Uma *alocação de dispositivo* é a atribuição de uma licença a um dispositivo específico. O produto pode estar instalado ou não no dispositivo. Por exemplo, suponha que você adquira 10 licenças do ProdutoA. Você pode alocar as licenças aos dispositivos de destino antes mesmo que o ProdutoA seja instalado nos dispositivos.

Uma *alocação demográfica* é a atribuição de uma ou mais licenças a um site, departamento ou centro de custo. Qualquer dispositivo que receber atribuição de demográfico e tiver o produto instalado será exibido como uma instalação associada à alocação. Por exemplo, suponha que você adquira 15 licenças do ProdutoA e aloque-as ao DepartamentoQ. Existem 20 dispositivos atribuídos ao DepartamentoQ. Desses 20 dispositivos, 12 estão com o ProdutoA instalado. O resultado é que a alocação do DepartamentoQ mostra 15 licenças alocadas com 12 instalações.

As etapas a seguir explicam como alocar licenças a dispositivos. Para obter informações sobre alocação de licenças a regiões demográficas, consulte "Alocação de licenças" na *Referência do ZENworks Asset Management*.

1. No ZENworks Control Center, clique na guia **Gerenciamento de Bens**.
2. Na página Gerenciamento de Licença, clique em **Produtos Licenciados**.
3. Na lista Produtos Licenciados, clique no produto licenciado para o qual deseja alocar licenças.
4. Por padrão, apenas a alocação de dispositivo está habilitada para monitorar a propriedade das licenças de produto. Para alocar licenças a demográficos, o usuário deve executar as seguintes etapas para habilitar a alocação demográfica para o produto:
   - **4a** Clique na guia **General**.
   - **4b** No painel Configurações de Alocação de Licenças, preencha os seguintes campos:

     Habilitar alocações demográficas: Selecione essa opção.

     Tipo de alocação demográfica: Todas as alocações demográficas para um único produto licenciado devem ser do mesmo tipo. Selecione o tipo (**Site**, **Departamento**, **Centro de Custo**) que deseja usar para este produto.

     Atualizar alocações de licença com dados demográficos das importações de registros de compra futuros: Selecione essa opção se, ao importar registros de compra futuros para o produto, você quiser atualizar automaticamente a quantidade de licenças alocadas com base nos dados demográficos do registro de compra.

     Por exemplo, suponha que o produto esteja usando alocações de Departamento. Você importa um registro de compra que inclui licenças atribuídas ao Departamento Q. As licenças são adicionadas como uma alocação demográfica do Departamento Q.

     Também cria novas alocações, se necessário. Por exemplo, se um registro de compra incluir licenças do Produto A atribuídas ao Departamento Z (um novo departamento que não aparece na lista de alocações do Produto A), uma nova alocação para o Departamento Z será criada.

     Quantidade Alocada: Exibe o número total de licenças alocadas, seja para dispositivos ou para demográficos.

   - **4c** Clique em **Aplicar** para gravar todas as mudanças.

5 Clique na guia **Alocações de Licença**.

6 (Opcional) Para ver quais dispositivos têm o produto instalado, mas não têm uma licença alocada, clique no número **Instalações sem alocações** no painel Alocações de Dispositivo.

7 Clique em **Adicionar** > **Dispositivos com Produto Instalado** caso o dispositivo para o qual você deseja alocar uma licença tenha o produto instalado.

ou

Clique em **Adicionar** > **Todos os Dispositivos** caso o dispositivo para o qual você deseja alocar uma licença não tenha o produto instalado.

A caixa de diálogo Pesquisar por Dispositivo é exibida.

8 No campo **Tipo de Dispositivo**, selecione a opção desejada para pesquisar **Dispositivos Gerenciados**, **Dispositivos Inventariados**, **Dispositivos Gerenciados ou Inventariados**, **Dispositivos Migrados do ZAM** ou **Todos**.

Se não tiver certeza do tipo de dispositivo, selecione **Todos**.

9 Para limitar a pesquisa, use os filtros para criar os critérios de pesquisa.

Se você não criar filtros, todos os dispositivos (ou todos os dispositivos que têm o produto instalado) serão exibidos, até o número máximo para exibição.

10 Especifique o número máximo de dispositivos a serem exibidos pela pesquisa.

11 Selecione as colunas que deseja exibir na caixa de diálogo de pesquisa resultante. Pressione Control e clique para selecionar vários campos.

12 Clique em **Pesquisar** para exibir uma caixa de diálogo Selecionar Dispositivo com a lista de resultados da pesquisa.

13 Selecione os dispositivos para os quais deseja alocar licenças e, em seguida, clique em **OK**.

As seguintes informações são fornecidas para a alocação:

- **Nome do Computador, Nome de Login e Endereço IP:** Informações padrão sobre o dispositivo, incluindo o nome de login do usuário que estava conectado no momento em que o dispositivo foi inventariado.
- **Site, Departamento, Centro de Custo:** Dados demográficos sobre o dispositivo. Se um ou mais campos estiverem vazios, os dados do inventário do dispositivo não conterão essas informações.
- **Quantidade Instalada:** O número de instalações do produto licenciado no dispositivo. Normalmente é 1.
- **Alocação Duplicada:** Inclui uma marca de seleção se a instalação do dispositivo também estiver incluída em uma alocação demográfica.
- **Instalações sem Alocações:** Exibe o número de instalações sem alocação de licença, seja por uma alocação demográfica ou uma alocação de dispositivo. Clique no número para exibir a lista de instalações.

9 Gerenciamento de Configurações

As seções a seguir apresentam explicações e instruções sobre as tarefas que você pode executar com o ZENworks Configuration Management. Dependendo do seu ambiente e da funcionalidade do que você planeja usar, talvez não seja necessário saber como executar todas as tarefas. Você pode analisar em qualquer ordem as tarefas sobre as quais decida obter mais informações.

Ativando o Gerenciamento de Configurações

Caso não tenha ativado o Gerenciamento de Configurações durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, execute as seguintes etapas:

1. No ZENworks Control Center, clique em **Configuração**.
2. No painel Licenças, clique em **ZENworks 2020 Configuration Management**.
3. Selecione Avaliar/Ativar o produto e preencha os seguintes campos:

   Avaliação de Uso: Selecione essa opção para habilitar um período de avaliação de 60 dias. Após esse período, você deve inserir a chave de licença para continuar usando o produto.

   Chave de Licença do Produto: Especifique a chave de licença que você adquiriu para o Gerenciamento de Configurações. Para comprar a licença de um produto, consulte o site do produto Novell ZENworks Configuration Management (http://www.novell.com/products/zenworks/configurationmanagement).
4. Clique em **OK**.

Habilitando o Gerenciamento de Configurações no Agente do ZENworks

Para que o Agente do ZENworks execute as operações de Gerenciamento de Configurações no dispositivo, os recursos apropriados do agente devem ser habilitados. Esses recursos (Gerenciamento de Bundles, Gerenciamento de Imagem, Gerenciamento de Políticas, Gerenciamento Remoto e Gerenciamento de Usuários) são habilitados por padrão quando o ZENworks Configuration Management é ativado (licença completa ou de avaliação).

Verifique se os recursos estão habilitados. Se preferir, caso não queira usar determinados recursos, você pode desabilitá-los. Para obter instruções, consulte "Configurando recursos do Agente do ZENworks" na página 39.

Distribuindo software

O ZENworks Configuration Management fornece excelente flexibilidade para a distribuição de software. É possível distribuir aplicativos e arquivos individuais; simplesmente fazer modificações nos arquivos existentes em um dispositivo; instalar, remover e voltar aplicativos em seus dispositivos.

O software é distribuído com o uso de bundles. Um bundle consiste em todos os arquivos, definições de configuração, instruções de instalação etc. necessários para distribuir e gerenciar o aplicativo ou os arquivos em um dispositivo. Ao atribuir um bundle a um dispositivo, você pode instalá-lo e iniciá-lo no dispositivo de acordo com as programações (distribuição, inicialização e disponibilidade) definidas.

Você também pode ver o resumo do status de atribuição, distribuição, instalação e inicialização do bundle usando o painel de controle Bundle. Para obter mais informações, consulte a Referência de Distribuição de Software do ZENworks.

Há quatro tipos de bundles que você pode criar:

- **Bundle Corporativo:** Permite configurar e gerenciar recursos corporativos em dispositivos móveis.
- **Bundle do iOS/iPadOS:** Permite implantar aplicativos e perfis de instalação em dispositivos iOS e iPadOS cliente.
- **Bundle do Linux:** Permite configurar e gerenciar aplicativos em dispositivos Linux.
- **Bundle de Dependência do Linux:** Permite a disponibilização dos pacotes de software nos dispositivos Linux para resolver as dependências dos pacotes.
- **Bundle do Macintosh:** Permite configurar e gerenciar aplicativos em dispositivos Macintosh.
- **Bundle de pré-inicialização:** Permite executar um conjunto de tarefas em um dispositivo gerenciado ou não gerenciado antes da inicialização do sistema operacional no dispositivo.
- **Bundle do Windows:** Permite configurar e gerenciar aplicativos em dispositivos Windows.

Os bundles Android (aplicativos de trabalho associados ao Android na empresa) e os bundles Apple VPP são criados automaticamente logo após a sincronização do ZENworks com os respectivos servidores Google e Apple. No entanto, você pode criar mais bundles Android ou Apple VPP. Para obter mais informações, consulte Aplicativos de aprovisionamento.

O software incluído em um bundle é carregado para o repositório do Servidor ZENworks. Isso permite que o Servidor ZENworks distribua o software sem ter que acessar outros locais de rede.

Assista aos seguintes vídeos para saber como distribuir o software para dispositivos Windows, Linux e Macintosh:

- Deploying Windows Software with ZENworks (Implantando software do Windows com o ZENworks)
- Deploying Linux Software with ZENworks (Implantando software do Linux com o ZENworks)
- Mac Management with ZENworks: Agent Deployment (Gerenciamento do Mac com ZENworks: Implantação do Agente)
- Mac Management with ZENworks: Standardized Application Deployment (Gerenciamento de Mac com o ZENworks: implantação de aplicativos padronizados)

Criando um bundle

Para criar um bundle de software, use o Assistente de Criação de Novo Bundle. Além de ajudá-lo a criar o bundle, o assistente também permite que você o designe a dispositivos e usuários e crie programações de distribuição, inicialização e disponibilidade.

1. No ZENworks Control Center, clique na guia **Bundles**.
2. No painel Bundles, clique em **Novo** > **Bundle** para iniciar o Assistente de Criação de Novo Bundle.
3. Siga os prompts para criar o bundle.

   Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

   Quando você concluir o assistente, o bundle será adicionado ao painel Bundles. É possível clicar no bundle para ver e modificar seus detalhes.
4. Prossiga com a próxima seção, Atribuindo um bundle.

Você também pode usar o comando `bundle-create` no utilitário zman para criar um bundle de software. Para obter mais informações, consulte "Comandos de bundles" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Atribuindo um bundle

Após criar um bundle, você precisa atribuí-lo aos dispositivos nos quais deseja instalá-lo. Você pode fazer atribuições a dispositivos ou usuários.

1. No painel Bundles, selecione o bundle que deseja atribuir marcando a caixa de seleção ao lado dele.
2. Clique em **Ação** > **Designar o ao Dispositivo**.

   ou

   Clique em **Ação** > **Designar ao Usuário.**
3. Siga os prompts para atribuir o bundle.

Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

Ao concluir o assistente, os dispositivos ou usuários atribuídos são adicionados à página Relacionamentos do bundle. É possível clicar no bundle para ver as atribuições.

Você também pode usar o comando `bundle-assign` no utilitário zman para atribuir um bundle. Para obter mais informações, consulte "Comandos de bundles" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Onde encontrar mais informações

Para obter mais informações sobre distribuição de software, consulte a *Referência de Distribuição de Software do ZENworks*.

Para obter mais informações sobre como distribuir aplicativos a dispositivos móveis, consulte a *ZENworks Mobile Management Reference* (Referência de Gerenciamento Móvel do ZENworks).

Aplicando políticas

O ZENworks Configuration Management permite o uso de políticas para criar um conjunto de configurações que podem ser atribuídas a qualquer número de dispositivos gerenciados. Ele ajuda a fornecer os dispositivos com uma configuração uniforme e dispensa a configuração separada de cada dispositivo.

As políticas do ZENworks Configuration Management ajudam no gerenciamento de serviços externos, configurações relacionadas à política puppet, favoritos do Internet Explorer, políticas de Grupo do Windows, direitos Arquivo Local, configurações de Gerenciamento de Energia CA, impressoras, configurações de serviço SNMP, perfis de roaming, na configuração e no gerenciamento de contas de usuário local dinâmico nos dispositivos gerenciados. Você também pode configurar o comportamento ou a execução de uma sessão de Gerenciamento Remoto no dispositivo gerenciado, bem como administrar e gerenciar de forma centralizada o comportamento e os recursos do ZENworks Explorer.

A seção a seguir inclui a lista de políticas de Configuração do Windows que podem ser criadas e atribuídas a um usuário ou dispositivo gerenciado.

- **Política de Marcadores do Browser:** Configura os favoritos do Internet Explorer para os dispositivos e usuários do Windows.
- **Política de Usuário Local Dinâmico:** Configura os usuários criados nas estações de trabalho Windows XP, Windows Vista, Windows 7; e nos Servidores de Terminal Windows 2003, Windows 2008, Windows 2008 R2 após a autenticação bem-sucedida dos usuários no Novell eDirectory.
- **Política de Direitos Arquivo Local:** Configura direitos para arquivos ou pastas existentes nos sistemas de arquivos NTFS.

  É possível usar a política para configurar permissões básicas e avançadas para usuários e grupos locais e de domínio. Desse modo, um administrador pode criar grupos personalizados em dispositivos gerenciados.
- **Política de Gerenciamento de Energia:** Define configurações de Gerenciamento de Energia nos dispositivos gerenciados.

Assista a um vídeo que demonstra como configurar uma política de Gerenciamento de Energia.

- **Política de Impressora:** Configura impressoras Locais, SMB, HTTP, TCP/IP, CUPS e iPrint para dispositivos e usuários do Windows.
- **Política de Gerenciamento Remoto:** Configura o comportamento ou a execução de uma sessão de Gerenciamento Remoto em um dispositivo gerenciado. A política inclui propriedades, como operações de Gerenciamento Remoto, segurança etc. É possível atribuir uma política de Gerenciamento Remoto a usuários e a dispositivos gerenciados.
- **Política de Perfil de Roaming:** Permite que o usuário configure o caminho em que seu perfil de usuário deve ser armazenado.

  Um perfil de usuário contém informações sobre as configurações de área de trabalho e as preferências pessoais de um usuário, que são retidas a cada sessão.

  Qualquer perfil de usuário armazenado em um caminho de rede é conhecido como perfil de roaming. Toda vez que o usuário efetua login em uma máquina, seu perfil é carregado no caminho da rede. Desse modo, o usuário pode utilizar várias máquinas e ainda reter configurações pessoais consistentes.
- **Política de SNMP:** Configura parâmetros de SNMP nos dispositivos gerenciados.
- **Política de Grupo do Windows:** Configura a Política de Grupo para dispositivos e usuários Windows.
- **Política de Configuração do ZENworks Explorer:** Permite administrar e gerenciar centralmente o comportamento e os recursos do ZENworks Explorer.

A seção a seguir inclui a lista de políticas de Configuração do Linux que podem ser criadas e atribuídas a um usuário ou dispositivo gerenciado.

- **Política de Serviços Externos:** Configura os serviços externos em um dispositivo gerenciado pelo Linux para os repositórios YUM, ZYPP ou MOUNT. Oferece ao administrador a capacidade de fazer download e instalar pacotes ou atualizações de software desses repositórios nos dispositivos gerenciados.
- **Política Puppet:** Especifica como executar declarações e módulos puppet no dispositivo gerenciado, fazer upload dos arquivos de script, além de especificar se um dry run do script deve ser executado no dispositivo.

A seção a seguir lista as políticas aplicáveis aos dispositivos móveis registrados na zona.

- **Política de Controle de Dispositivo Móvel:** Você pode permitir ou restringir o acesso dos usuários aos diversos recursos de um dispositivo móvel.
- **Política de E-mail Móvel:** Permite gerenciar a conta de e-mail corporativo em dispositivos móveis.
- **Política de Registro Móvel:** Impõe os usuários que podem registrar dispositivos móveis, quais dispositivos móveis os usuários podem registrar, o modo a ser usado para o registro de dispositivos móveis, o local e a nomeação do dispositivo.
- **Política de Segurança Móvel:** Configura as restrições de senha e as definições de criptografia e inatividade nos dispositivos.
- **Política de Conformidade Móvel:** Garante que os dispositivos estejam em conformidade com as regras aplicadas a esses dispositivos.

- **Política de Registro do Android Empresa:** Permite que os usuários registrem seus dispositivos Android no modo de perfil de trabalho ou no modo de dispositivo gerenciado pela empresa como parte do programa Android Empresa.
- **Política de Proteção de Aplicativo do Intune:** Assegura o uso obrigatório das restrições nos aplicativos do Microsoft Intune, como restrição das ações recortar, copiar e colar no aplicativo e imposição do uso de um PIN para acessar um aplicativo do Intune. Aplicável a dispositivos iOS, iPadOS e Android.

Criando uma política

Para criar uma política, use o Assistente de Criação de Nova Política. Além de ajudá-lo a criar a política, o assistente também permitirá que você a designe a dispositivos e usuários, e decida se deve assegurar o uso obrigatório da política imediatamente ou esperar até que o dispositivo atualize suas informações.

1. No ZENworks Control Center, clique na guia **Políticas**.
2. No painel Políticas, clique em **Novo** > **Política** para exibir a página Selecionar Plataforma.
3. Selecione a categoria da política e clique em **Avançar** para exibir a página Selecionar Categoria de Política.
4. Selecione a categoria de política que deseja criar e clique em **Avançar**.
5. Selecione um Tipo de Política na lista de políticas exibida. Siga os prompts na tela para criar a política.

   Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

   Quando você conclui o assistente, a política é adicionada ao painel Políticas. Você pode clicar na política para ver seus detalhes e modificar as atribuições.

Você também pode usar o comando `policy-create` no utilitário zman para criar uma política. Para obter mais informações, consulte “Comandos de políticas” na *Referência de Utilitários de Linha de Comando do ZENworks*.

Designar uma política

Após criar uma política, você precisa atribuí-la aos dispositivos aos quais deseja aplicá-la. Você pode fazer atribuições a dispositivos ou usuários.

1. No painel Políticas, selecione a política que deseja atribuir marcando a caixa de seleção ao lado dela.
2. Clique em **Ação** > **Designar o ao Dispositivo**.

   ou

   Clique em **Ação** > **Designar ao Usuário.**
3. Siga os prompts para atribuir a política.

   Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

   Ao concluir o assistente, os dispositivos ou usuários atribuídos são adicionados à página Relacionamentos da política. É possível clicar na política para ver as atribuições.

Você também pode usar o comando `policy-assign` no utilitário zman para atribuir uma política. Para obter mais informações, consulte "Comandos de políticas" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Onde encontrar mais informações

Para obter mais informações sobre como aplicar políticas, consulte a *ZENworks Configuration Policies Reference (Referência de Políticas de Configuração do ZENworks)*.

Para obter mais informações sobre como aplicar políticas a dispositivos móveis, consulte a *ZENworks Mobile Management Reference* (Referência de Gerenciamento Móvel do ZENworks).

Dispositivos de criação de imagens

O ZENworks Configuratoin Management inclui um serviço chamado Preboot Services, que permite realizar tarefas nos dispositivos antes da inicialização de seus sistemas operacionais. Usando o Preboot Services, você pode fazer o seguinte, automática ou manualmente, para um dispositivo quando ele for inicializado:

- Executar scripts de criação de imagens do ZENworks que contêm comandos que você pode emitir no prompt do bash
- Obter uma imagem das unidades de disco rígido do dispositivo e de outros dispositivos de armazenamento
- Restaurar uma imagem no dispositivo
- Participar de uma sessão em que uma imagem existente é aplicada a vários dispositivos por multicast
- Obter ou restaurar uma imagem WIM usando o ImageX
- Obter ou restaurar uma imagem Ghost usando o Symantec Ghost

Para realizar algumas dessas tarefas automaticamente, basta ter o PXE (Preboot Execution Environment) habilitado nos seus dispositivos e, em seguida, configurar tarefas pré-inicializáveis no ZENworks Control Center e atribuí-las aos dispositivos. Os dispositivos poderão então implementar automaticamente essas tarefas durante a inicialização.

Para implementar as tarefas manualmente, você pode configurar os dispositivos para requerer a intervenção do usuário durante a inicialização.

Usando o ZENworks Control Center, você também pode replicar as mudanças no diretório `tftp` de um Servidor Principal para outros imaging servers (Servidor Principal ou dispositivo Satélite com a função de criação de imagens).

- "Configurando o Preboot Services" na página 86
- "Obtendo uma imagem" na página 89
- "Aplicando uma imagem" na página 91
- "Onde encontrar mais informações" na página 94

Configurando o Preboot Services

Para usar o Preboot Services, execute as tarefas das seções a seguir:

Habilitando o PXE em um dispositivo

O Preboot Services requer que o PXE (Preboot Execution Environment) seja habilitado em qualquer dispositivo gerenciado em que você deseja obter ou aplicar uma imagem.

Para verificar se o PXE está habilitado em um dispositivo, reinicie o dispositivo e selecione a opção de inicialização (F12 na maioria dos dispositivos). O PXE estará habilitado se houver uma opção de inicialização de rede.

Se o PXE não estiver habilitado em um dispositivo, edite o BIOS do dispositivo para habilitá-lo. Para que o ambiente PXE esteja disponível sempre que o dispositivo for iniciado, você também pode mudar a ordem de inicialização, para que a opção NIC (Network Interface Card) seja listada antes das outras opções de inicialização.

Configurando um servidor de criação de imagens

O Imaging Server é o servidor PXE ao qual o mecanismo PXE de um dispositivo é conectado. Para permitir que um Servidor ZENworks funcione como um Imaging Server, simplesmente inicie o Serviço DHCP Proxy da Novell nesse servidor. Ao iniciar o serviço, você também deve mudar o tipo de inicialização de Manual para Automática, de modo que ele seja iniciado sempre que o servidor for reinicializado.

Definindo as configurações de criação de imagens de terceiros

Se você quiser usar as soluções de criação de imagens de terceiros, defina as Configurações da Criação de Imagens de Terceiros no ZENworks Control Center. O ZENworks suporta as seguintes ferramentas de criação de imagens de terceiros:

- Microsoft ImageX, que usa o formato de arquivo de imagem WIM e o WINPE como distro
- Symantec Ghost, que usa o formato de arquivo de imagem Ghost e o WINPE como distro

A criação de imagens de terceiros do ZENworks suporta apenas PXE como o mecanismo de boot.

Para definir as configurações de criação de imagens de terceiros:

1. Instale o ZENworks Configuration Management no Imaging Server.

   Para obter mais informações sobre como instalar o ZENworks 2020, consulte "Instalando um servidor principal do ZENworks em Windows" na *Instalação do Servidor ZENworks 2020*.

2 Defina as configurações da criação de imagens de terceiros no ZENworks Control Center.

2a Verifique se o Kit de Instalação Automatizada do Windows (WAIK) ou o Kit de Avaliação e Implantação do Windows (WADK) da Microsoft está instalado no dispositivo que executa o ZENworks Control Center.

2b No Centro de Controle do ZENworks, clique na guia **Configuração**.

2c No painel **Configurações da Zona de Gerenciamento**, clique em **Gerenciamento de Dispositivo** > **Preboot Services** > painel **Configurações da Criação de Imagens de Terceiros**.

2d Para **Configurações de Upload de 32 Bits**:

Fazer Upload da Distribuição de Base WinPE (Requer o Windows AIK/Windows ADK):

Clique no ícone para fazer upload do arquivo de Criação de Imagens WIM. Na caixa de diálogo Fazer Upload dos Arquivos de Criação de Imagens WIM, faça o seguinte:

1. Para fazer upload de um arquivo `winpe.wim` de 32 bits:

   Do WAIK: Navegue até a pasta `Windows AIK\Tools\PETools\x86` no diretório instalado e selecione o arquivo `winpe.wim`.

   Do WADK: Navegue até a pasta `Windows Kits\<versão>\Assessment and Deployment Kit\Windows Preinstallation Environment\x86\en-us` no diretório instalado e selecione o arquivo `winpe.wim`.

   Em que *<versão>* é a versão do Sistema Operacional Windows.

   Observação: Refazer o upload do arquivo `winpe.wim` sobregrava a instância anterior desse arquivo no servidor.

   ---

2. Clique em **OK**.

   Dessa forma, será feito o download dos arquivos de imagens do servidor para o dispositivo no qual você acessa o ZENworks Control Center, o `winpe.wim` será reconstruído com os arquivos de imagens e, em seguida, será feito o upload dos arquivos do dispositivo para o servidor. O andamento do download e upload de arquivos aparece no campo **Status**.

Fazer Upload de Arquivos ImageX para Suportar a Criação de Imagens WIM (ImageX.exe):

1. Clique no ícone para procurar e selecionar o mecanismo Microsoft Imaging (`imagex.exe`) no dispositivo em que você acessa o ZENworks Control Center.
2. Após a definição das configurações de criação de imagem de terceiros, clique em **Aplicar**.
3. Clique em **Status** para ver o status da replicação de conteúdo em todos os Servidores Principais e Satélites com a função de Criação de Imagens na zona de gerenciamento. Você deve iniciar a operação de criação de imagem somente quando o status é Disponível.

   Observação: Se você fizer upload dos arquivos de imagens ImageX tanto de 32 bits quanto de 64 bits, faça isso em instâncias diferentes.

Fazer Upload dos Arquivos do Ghost 11.5 ou Superior para Suportar a Criação de Imagens do Ghost (Ghost32.exe):

1. Clique no ícone para procurar e selecionar o mecanismo Symantec GHOST (`ghost32.exe`) no dispositivo em que você acessa o ZENworks Control Center.
2. Após a definição das configurações de criação de imagem de terceiros, clique em **Aplicar**.
3. Clique em **Status** para ver o status da replicação de conteúdo em todos os Servidores Principais e Satélites com a função de Criação de Imagens na zona de gerenciamento. Você deve iniciar a operação de criação de imagem somente quando o status é Disponível.

2e Para **Configurações de Upload de 64 Bits**:

Fazer Upload da Distribuição de Base WinPE (Requer o Windows AIK/Windows ADK):

Clique no ícone para fazer upload do arquivo de Criação de Imagens WIM. Na caixa de diálogo Fazer Upload dos Arquivos de Criação de Imagens WIM, faça o seguinte:

1. Para fazer upload de um arquivo `winpe.wim` de 64 bits do WADK, navegue até a pasta `Windows Kits\<versão>\Assessment and Deployment Kit\Windows Preinstallation environment\amd64\en-us` no diretório instalado e selecione o arquivo `winpe.wim`. SETUP.ISS.

   Em que *<versão>* é a versão do Sistema Operacional Windows.
2. Clique em **OK**.

   Dessa forma, será feito o download dos arquivos de imagens do servidor para o dispositivo no qual você acessa o ZENworks Control Center, o `winpe.wim` será reconstruído com os arquivos de imagens e, em seguida, será feito o upload dos arquivos do dispositivo para o servidor. O andamento do download e upload de arquivos aparece no campo **Status**.

Fazer Upload de Arquivos ImageX para Suportar a Criação de Imagens WIM (ImageX.exe):

1. Clique no ícone para procurar e selecionar o mecanismo Microsoft Imaging (`imagex.exe`) no dispositivo em que você acessa o ZENworks Control Center.
2. Após a definição das configurações de criação de imagem de terceiros, clique em **Aplicar**.
3. Clique em **Status** para ver o status da replicação de conteúdo em todos os Servidores Principais e Satélites com a função de Criação de Imagens na zona de gerenciamento. Você deve iniciar a operação de criação de imagem somente quando o status é Disponível.

Observação: Se você fizer upload dos arquivos de imagens ImageX tanto de 32 bits quanto de 64 bits, faça isso em instâncias diferentes.

Fazer Upload dos Arquivos do Ghost 11.5 ou Superior para Suportar a Criação de Imagens do Ghost (Ghost64.exe):

1. Clique no ícone para procurar e selecionar o mecanismo Symantec GHOST (`ghost64.exe`) no dispositivo em que você acessa o ZENworks Control Center.

2. Após a definição das configurações de criação de imagem de terceiros, clique em **Aplicar**.
3. Clique em **Status** para ver o status da replicação de conteúdo em todos os Servidores Principais e Satélites com a função de Criação de Imagens na zona de gerenciamento. Você deve iniciar a operação de criação de imagem somente quando o status é Disponível.

3 Habilite o PXE no dispositivo.

4 Providencie um servidor DHCP padrão no Imaging Server ou em outro servidor de rede.

Definindo as configurações de driver NTFS de terceiros

É possível fazer download do driver NTFS de alto desempenho mais recente e gravá-lo no sistema. É possível ver o status de replicação de conteúdo em todos os Servidores Principais e Satélite com a função Criação de Imagens na zona de gerenciamento. Você poderá iniciar a operação de Criação de Imagens usando o driver NTFS de Terceiros quando o status for Disponível.

Para definir essas configurações, clique em **Configuração** no painel esquerdo para exibir a guia **Configuração**. Se ela não for expandida, clique em **Configurações da Zona de Gerenciamento** e, em seguida, clique em **Gerenciamento de Dispositivo** > **Preboot Services** para exibir a página do Preboot Services.

Obtendo uma imagem

Você pode criar e restaurar imagens do ZENworks em um dispositivo usando o ZENworks Imaging e imagens de terceiros usando o utilitário de Criação de Imagens de Terceiros do ZENworks. Esse utilitário permite criar uma imagem e restaurá-la em um dispositivo ou servidor local usando o formato Windows Imaging (WIM) ou Ghost Imaging.

1 No ZENworks Control Center, clique na guia **Dispositivos**.

2 Navegue na pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo cuja imagem você deseja obter.

3 Clique no dispositivo para exibir seus detalhes.

4 Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Obter uma Imagem** para iniciar o Assistente de Obtenção de Imagem.

5 Na página Informações do Arquivo, preencha os campos a seguir e clique em **Avançar**.

Para criação de imagens do ZENworks, especifique o seguinte:

Formato da Imagem: Selecione o formato da imagem a ser obtida para o dispositivo

Servidor e Caminho do Arquivo: Clique no ícone para exibir a caixa de diálogo Informações de Caminho e Servidor. Configure estas opções.

- **Objeto, IP ou DNS do Servidor:** Clique no ícone para procurar e selecionar o objeto, endereço IP ou nome DNS do Servidor Principal ou do dispositivo que foi elevado para a função Imaging Server.
- **Caminho do Arquivo no Servidor:** Clique no ícone para procurar e selecionar um arquivo de imagem. Esse arquivo de imagem precisar conter a extensão de nome de arquivo `.zmg`, o que significa ser um arquivo de imagem válido do ZENworks.

Observação: Você não poderá ir para o sistema de arquivos especificado se vários domínios de pesquisa com DHCP estiverem configurados para Linux e se o servidor estiver no Windows.

Para Criação de Imagens de Terceiros, especifique o seguinte:

Caminho de Rede Compartilhado do Arquivo de Imagem: Especifique o caminho de rede compartilhado em que você deseja gravar os arquivos.`wim` ou `.gho`. O diretório deve ser um compartilhamento do Windows ou um compartilhamento SMB ou CIFS do Linux.

Para procurar e fazer upload dos arquivos a serem instalados, instale a extensão de Upload de Arquivo da Novell neste dispositivo.

Nome do Arquivo de Imagem: Especifique o nome de arquivo para gravar o arquivo `.wim` ou `.gho`. Essa opção é exibida apenas para o formato de Criação de Imagens do Windows (`.wim`) o Formato de Criação de Imagens do Ghost (`.gho`).

Credencial de Rede: Clique em  para procurar e selecionar as credenciais de rede a serem usadas para acessar o dispositivo que tem os arquivos `.wim`. Essa opção é exibida somente para o formato de imagem do Windows (`.wim`) e o Formato Ghost Image (`.gho`).

Usar Compactação: A compactação é obrigatória. Escolha um dos seguintes itens:

- **Balanceada:** Equilibra automaticamente a compactação de acordo com uma média da velocidade de recriação da imagem e o espaço em disco disponível para o arquivo de imagem. Essa opção é exibida somente para o formato de imagem do ZENworks
- **Nenhuma:** Essa opção é exibida apenas para o formato Windows Image e o formato Ghost Image.
- **Otimizar Velocidade:** Otimiza a compactação para reduzir o tempo de recriação da imagem. Use essa opção se a velocidade da CPU não for satisfatória.
- **Otimizar Espaço:** Otimiza a compactação para diminuir o tamanho do arquivo de imagem, poupando espaço em disco. Isso pode fazer com que a recriação da imagem seja mais demorada.

Balanceadaé a opção padrão para o formato de imagem do ZENworks e **Otimizar para Aumentar a Velocidade** é a opção padrão para o formato de Imagem do Windows e o formato de Imagem Ghost.

Criar um Bundle de Imagem: Anule a seleção desse campo.

6 Analise as informações na página Resumo do Arquivo de Imagem, clique em **Concluído** e clique em **OK**.

Como as tarefas de criação de imagens são concluídas pelo Preboot Services, a imagem do dispositivo é obtida na próxima reinicialização do dispositivo. O painel Trabalho de Criação de Imagem, localizado na página Resumo do dispositivo, mostra que o trabalho está programado. Quando o trabalho é concluído, a tarefa é removida desse painel.

7 Para reinicializar o dispositivo imediatamente e iniciar o trabalho de criação de imagem, clique em **Reinicializar/Encerrar uma Estação de Trabalho** (ou **Reinicializar/Encerrar Servidor**) no painel de navegação esquerdo.

O tempo necessário para obter a imagem depende do tamanho das unidades do dispositivo.

Aplicando uma imagem

Para aplicar uma imagem a um dispositivo, use o Assistente de Criação de Novo Bundle para criar um bundle de criação de imagens. O bundle contém a imagem que você deseja aplicar. Além de ajudá-lo a criar o bundle, o assistente também permite que você o designe a dispositivos. Após criar o bundle de criação de imagens, inicie o trabalho de criação de imagens.

- “Criando o bundle de imagens do ZENworks” na página 91
- “Criando o bundle de imagens de terceiros” na página 92
- “Iniciando o trabalho de criação de imagens” na página 93

Assista aos seguintes vídeos para saber como implantar imagens do Windows 7 e do Linux em dispositivos:

- Deploying Windows 7 Image with ZENworks (Implantando imagem do Windows 7 com o ZENworks)
- Deploying Linux with ZENworks (Implantando Linux com o ZENworks)

Criando o bundle de imagens do ZENworks

Para restaurar as imagens do ZENworks em um dispositivo, crie o bundle de imagens do ZENworks.

1. No ZENworks Control Center, clique na guia **Bundles**.
2. No painel Bundles, clique em **Novo** > **Bundle** para iniciar o Assistente de Criação de Novo Bundle.
3. Na página Selecionar Tipo de Bundle, escolha **Bundle de Pré-inicialização** e clique em **Avançar**.
4. Na página Selecione a Categoria do Bundle, selecione **Imagem do ZENworks** e clique em **Avançar**.
5. Preencha o assistente usando informações da tabela a seguir para preencher os campos.

Página do Assistente	Detalhes
Página Definir Detalhes	Especifique um nome para a tarefa. O nome não pode incluir nenhum destes caracteres inválidos: / \ * ? : " ' < > | ` % ~
Página Selecione o Arquivo de Imagem do ZENworks	Para selecionar o arquivo de imagem: 1. Clique em para exibir a caixa de diálogo Informações de Caminho e Servidor. 2. Preencha os campos a seguir: **Objeto, IP ou DNS do Servidor:** Selecione o Servidor ZENworks em que você armazenou a imagem. **Caminho do Arquivo no Servidor:** Procure e selecione o arquivo de imagem. O diretório de armazenamento padrão dos arquivos de imagem é `\Novell\ZENworks\work\content-repo\images`. 3. Clique em **OK**.
Página Resumo	Clique em **Avançar** para continuar no assistente e atribuir o bundle ao dispositivo de destino.

Página do Assistente	Detalhes
Página Grupos de Bundles	Você não deve atribuir o bundle de imagens a grupos. Clique em **Avançar** para ignorar essa página.
Página Adicionar atribuições	Selecione o dispositivo em que você deseja aplicar a imagem.
Página Programações	Você não deve atribuir uma programação ao bundle de imagens. Clique em **Avançar** para ignorar essa página.
Página Concluir	Clique em **Concluir** para criar o bundle e designá-lo ao dispositivo selecionado.

Criando o bundle de imagens de terceiros

Para restaurar as imagens de terceiros, crie o bundle de imagens de terceiros.

1. No ZENworks Control Center, clique na guia **Bundles**.
2. No painel Bundles, clique em **Novo** > **Bundle** para iniciar o Assistente de Criação de Novo Bundle.
3. Na página Selecionar Tipo de Bundle, escolha **Bundle de Pré-inicialização** e clique em **Avançar**.
4. Na página Selecione a Categoria do Bundle, selecione **Imagem de Terceiros** e clique em **Avançar**.
5. Preencha o assistente usando informações da tabela a seguir para preencher os campos.

Página do Assistente	Detalhes
Página Definir Detalhes	Especifique um nome para a tarefa. O nome não pode incluir nenhum destes caracteres inválidos: / \ * ? : " ' < > | ` % ~

Página do Assistente	Detalhes
Página Selecionar um Arquivo de Imagem de Terceiros	Para selecionar um arquivo de imagem de terceiros: 1. Selecione o tipo da imagem a ser usada no bundle. No ZENworks Configuration Management , , apenas o Formato Windows Image (`.wim`) e o Formato GHOST·Image (`.gho`) estão disponíveis. 2. Especifique o diretório de rede compartilhado que contém os arquivos `.wim` ou `.gho`. O diretório deve ser um compartilhamento do Windows ou um compartilhamento SMB ou CIFS do Linux. 3. Clique em para procurar e selecionar as credenciais de rede a serem usadas para acessar o dispositivo que tem os arquivos `.wim` ou `.gho`. 4. Se desejar usar o bundle WIM como uma imagem de expansão, selecione **Restaurar WIM como Imagem de Expansão** e configure as seguintes opções **Número da Imagem (Apenas WIM):** Selecione o número do índice da imagem a ser restaurada. **Caminho para restaurar a imagem de extensão:** Especifique a localização no dispositivo em que deseja restaurar a imagem de expansão. 5. Clique em **OK**.
Página Resumo	Clique em **Avançar** para continuar no assistente e atribuir o bundle ao dispositivo de destino.
Página Grupos de Bundles	Você não deve atribuir o bundle de imagens a grupos. Clique em **Avançar** para ignorar essa página.
Página Adicionar atribuições	Selecione o dispositivo em que você deseja aplicar a imagem.
Página Programações	Você não deve atribuir uma programação ao bundle de imagens. Clique em **Avançar** para ignorar essa página.
Página Concluir	Clique em **Concluir** para criar o bundle e designá-lo ao dispositivo selecionado.

Iniciando o trabalho de criação de imagens

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue na pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo em que deseja aplicar a imagem.
3. Clique no dispositivo para exibir seus detalhes.
4. Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Aplicar o Bundle de Criação de Imagem Atribuído** para programar o trabalho.

Como as tarefas de criação de imagens são concluídas pelo Preboot Services, a imagem é aplicada ao dispositivo em sua próxima reinicialização. O painel Trabalho de Criação de Imagem, localizado na página Resumo do dispositivo, mostra que o trabalho está programado. Quando o trabalho é concluído, a tarefa é removida desse painel.

5 Para reinicializar o dispositivo imediatamente e iniciar o trabalho de criação de imagem, clique em **Reinicializar/Encerrar uma Estação de Trabalho** (ou **Reinicializar/Encerrar Servidor**) no painel de navegação esquerdo.

Onde encontrar mais informações

Para obter mais informações sobre criação de imagens e Preboot Services, consulte a *Referência para Preboot Services e Criação de Imagens do ZENworks*.

Gerenciando dispositivos remotamente

O Zenworks Configuration Management fornece a funcionalidade de Gerenciamento Remoto que permite gerenciar dispositivos remotamente. O Gerenciamento Remoto suporta as seguintes operações:

Operação Remota	Descrição	Detalhes Adicionais
Controle Remoto	Permite que você controle um dispositivo gerenciado a partir do console de gerenciamento para poder fornecer assistência ao usuário e ajudá-lo a resolver problemas. Você pode executar todas as operações que um usuário pode executar no dispositivo. Para obter mais informações sobre Controle Remoto em um dispositivo do Windows, consulte a "Executando operações de controle remoto, tela remota e execução remota em um dispositivo Windows" na página 98. Para obter mais informações sobre Controle Remoto em um dispositivo do Linux, consulte a "Executando operações de Controle Remoto, Tela Remota e Login Remoto em um dispositivo do Linux" na página 102.	

Operação Remota	Descrição	Detalhes Adicionais
Tela Remota	Permite que você conecte-se a um dispositivo gerenciado para poder vê-lo em vez de controlá-lo. Isto ajuda a solucionar problemas encontrados pelo usuário. Por exemplo, você pode observar como o usuário de uma dispositivo gerenciado executa determinadas tarefas, para garantir que ele as execute corretamente Para obter mais informações sobre Tela Remota em um dispositivo do Windows, consulte a "Executando operações de controle remoto, tela remota e execução remota em um dispositivo Windows" na página 98. Para obter mais informações sobre Tela Remota em um dispositivo do Linux, consulte a "Executando operações de Controle Remoto, Tela Remota e Login Remoto em um dispositivo do Linux" na página 102.	
Execução remota	Permite que você ative qualquer executável em um dispositivo gerenciado a partir do console de gerenciamento. Para executar um aplicativo remotamente, especifique o nome do executável na caixa de diálogo Execução Remota. Se o aplicativo não estiver no caminho de sistema no dispositivo gerenciado, forneça seu caminho completo. Por exemplo, você pode executar o comando `regedit` para abrir o Editor de Registro no dispositivo gerenciado. A caixa de diálogo Execução Remota exibe o status da execução do comando. Para obter mais informações sobre Execução Remota em um dispositivo do Windows, consulte a "Executando operações de controle remoto, tela remota e execução remota em um dispositivo Windows" na página 98.	Essa operação é suportada somente em um dispositivo gerenciado Windows.
Diagnóstico Remoto	Permite diagnosticar e analisar os problemas em um dispositivo gerenciado. Isso ajuda a reduzir o tempo de solução de problemas e dar assistência aos usuários sem que um técnico precise visitar fisicamente o dispositivo com problemas. Isto aumenta a produtividade do usuário, por manter as áreas de trabalho em operação. Para obter mais informações sobre Diagnóstico Remoto de um dispositivo, consulte a "Executando uma operação de Diagnóstico Remoto" na página 100.	Essa operação é suportada somente em um dispositivo gerenciado Windows.

Operação Remota	Descrição	Detalhes Adicionais
Transferência de Arquivos	permite transferir arquivos entre o console de gerenciamento e um dispositivo gerenciado. Para obter mais informações sobre a operação Transferência de Arquivos, consulte a “Executando uma operação de Transferência de Arquivos” na página 101	Essa operação é suportada somente em um dispositivo gerenciado Windows.
Login Remoto	Permite efetuar login em um dispositivo gerenciado a partir do console de gerenciamento e iniciar uma nova sessão gráfica sem incomodar o usuário no dispositivo gerenciado. Contudo, o usuário no dispositivo gerenciado não pode ver a sessão de Login Remoto. Para obter mais informações sobre Registro Remoto em um dispositivo do Linux, consulte a “Executando operações de Controle Remoto, Tela Remota e Login Remoto em um dispositivo do Linux” na página 102.	Essa operação é suportada somente em um dispositivo gerenciado Linux. Efetue login no dispositivo com as credenciais de usuário não `root`.
SSH Remoto	Permite que você se conecte e execute comandos com segurança em um dispositivo Linux remoto. Para obter mais informações sobre Registro Remoto em um dispositivo do Linux, consulte a “Executando a operação de SSH Remoto em um dispositivo do Linux” na página 103.	Essa operação é suportada somente em um dispositivo gerenciado Linux.

As seções a seguir explicam como configurar o Gerenciamento Remoto e executar cada uma das operações:

 Assista a um vídeo para aprender sobre o gerenciamento remoto de dispositivos.

Criando uma política de gerenciamento remoto

Por padrão, uma política segura de Gerenciamento Remoto é criada no dispositivo gerenciado quando o Agente do ZENworks é implantado com o componente de Gerenciamento Remoto no dispositivo. Você pode usar a política padrão para gerenciar um dispositivo remotamente. A política

padrão permite que você execute todas as operações de Gerenciamento Remoto em um dispositivo. Para anular a política padrão, crie uma política de Gerenciamento Remoto explicitamente para o dispositivo.

Você pode atribuir uma política de Gerenciamento Remoto a dispositivos ou usuários.

Para criar uma política de Gerenciamento Remoto:

1. No ZENworks Control Center, clique na guia **Políticas**.
2. No painel Políticas, clique em **Nova** > **Política** para iniciar o Assistente de Criação de Nova Política.
3. Selecione **Políticas de Configuração do Windows** e clique em **Próximo**.
4. Siga os prompts para criar a política de Gerenciamento Remoto.

   Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página. Quando você conclui o assistente, a política é adicionada ao painel Políticas. Você pode clicar na política para ver seus detalhes e modificar atribuições, programações etc.
5. Atribua a política de Gerenciamento Remoto a usuários e dispositivos:
   - **5a** No painel Políticas, marque a caixa de seleção ao lado da política.
   - **5b** Clique em **Ação** > **Designar o ao Dispositivo**.

     ou

     Clique em **Ação** > **Designar ao Usuário.**
   - **5c** Siga os prompts para atribuir a política.

     Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

     Ao concluir o assistente, os dispositivos ou usuários atribuídos são adicionados à página Relacionamentos da política. É possível clicar na política para ver as atribuições.

Definindo as configurações de Gerenciamento Remoto

As definições de configuração de Gerenciamento Remoto, localizadas na página Configuração, permitem especificar configurações, como a porta de Gerenciamento Remoto, o desempenho da sessão e os aplicativos de diagnóstico disponíveis.

As configurações são predefinidas para fornecer a configuração mais comum. Se quiser modificar as configurações:

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da zona de gerenciamento, clique em **Gerenciamento de Dispositivo** > **Gerenciamento Remoto**.
3. Modifique as configurações da forma que desejar.

   Clique no botão **Ajuda** na página para obter informações detalhadas sobre a página.
4. Quando terminar de modificar as configurações, clique em **Aplicar** ou em **OK** para gravar as mudanças.

Executando operações de controle remoto, tela remota e execução remota em um dispositivo Windows

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue pela pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo a ser gerenciado.
3. Selecione o dispositivo, clicando na caixa de seleção ao lado dele.
4. Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Controlar Remotamente uma Estação de Trabalho** ou **Controlar Remotamente um Servidor** para exibir a caixa de diálogo Gerenciamento Remoto.
5. Na caixa de diálogo Gerenciamento Remoto, preencha os seguintes campos:

   Dispositivo: Especifique o nome ou o endereço IP do dispositivo que você deseja gerenciar remotamente.

   Sempre assumir como padrão endereços IP para todos os dispositivos: Selecione para que o sistema exiba o endereço IP em vez do nome DNS.

   Os valores especificados para acessar um dispositivo durante a execução da operação de Controle Remoto são gravados no sistema quando você clica em **OK**. Alguns desses valores são selecionados automaticamente durante as operações de Controle Remoto subsequentes, dependendo do dispositivo ou do operador remoto.

   Operação: Selecione o tipo de operação remota (Controle Remoto, Tela Remota ou Execução Remota) a ser executado no dispositivo gerenciado:

   Autenticação: Selecione o modo que você deseja usar para se autenticar no dispositivo gerenciado. Estas são as duas opções:

   - **Senha:** Fornece autenticação baseada em senha para executar uma operação de Controle Remoto. Você deve inserir a senha correta conforme definida pelo usuário no dispositivo gerenciado ou conforme definida pelo administrador nas configurações de segurança da política de Gerenciamento Remoto. A senha definida pelo usuário têm preferência em relação à senha configurada pelo administrador.
   - **Direitos:** Essa opção está disponível somente quando você seleciona o dispositivo gerenciado em que a operação remota deve ser executada. Se um administrador já designou direitos de Gerenciamento Remoto a você para que execute a operação remota desejada no dispositivo gerenciado selecionado, você obterá acesso automaticamente assim que a sessão for iniciada.

   Porta: Especifique o número da porta em que o Agente de Gerenciamento Remoto está escutando. Por padrão, o número de porta é 5950.

   Modo de Sessão: Selecione um dos modos a seguir para a sessão:

   - **Colaborar:** Permite iniciar uma sessão de Controle Remoto e uma sessão de Tela Remota no modo de colaboração. Entretanto, você não pode iniciar primeiro uma sessão de Tela Remota no dispositivo gerenciado. Se iniciar a sessão de Controle Remoto no dispositivo gerenciado, você obterá todos os privilégios de um Operador Remoto master, que incluem:
     - Convidando outros Operadores Remotos para entrarem na sessão remota.
     - Delegando direitos de Controle Remoto ao Operador Remoto.
     - Retomando o controle do Operador Remoto.
     - Encerrar uma sessão remota.

Depois que a sessão de Controle Remoto tiver sido estabelecida para o dispositivo gerenciado no modo Colaborar, as outras sessões remotas no dispositivo gerenciado serão sessões de Tela Remota.

- **Compartilhada:** Permitir que mais de um Operador Remoto controle o dispositivo gerenciado, de forma simultânea.
- **Exclusivo:** Permite que haja uma sessão remota exclusiva no dispositivo gerenciado. Depois que uma sessão for iniciada no modo Exclusivo, não será possível iniciar nenhuma outra sessão remota no dispositivo gerenciado.

Criptografia de sessão: Garante a proteção da sessão remota usando a criptografia SSL (protocolo TLSv1).

Habilitar Armazenamento em Cache de Memória: Habilita o armazenamento em cache dos dados da sessão de gerenciamento remoto para melhorar o desempenho. Esta opção está disponível apenas para a operação de controle remoto. No momento, essa opção é suportada apenas no Windows.

Habilitar Otimização de Largura de Banda Dinâmica: Habilita a detecção da largura de banda de rede disponível e ajusta as configurações da seção de acordo para melhorar o desempenho. Esta opção está disponível apenas para a operação de controle remoto.

Enable Logging: Registra informações de sessão e depuração no arquivo `novell-zenworks-vncviewer.txt`. Por padrão, o arquivo será gravado na área de trabalho, se você iniciar o ZENworks Control Center por meio do Internet Explorer, e no diretório instalado do Mozilla, se você iniciar o ZENworks Control Center por meio do Mozilla FireFox.

Rotear por Proxy: Permite que a operação de gerenciamento remoto do dispositivo gerenciado seja roteada através de um servidor proxy. Se o dispositivo gerenciado estiver em uma rede privada ou no outro lado de um firewall ou roteador que esteja usando NAT (Network Address Translation - Conversão de Endereço de Rede), a operação de gerenciamento remoto do dispositivo poderá ser roteada através de um servidor proxy. Preencha os campos a seguir:

- **Proxy:** Especifique o nome DNS ou o endereço IP do servidor proxy. Por padrão, o servidor proxy configurado no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um servidor proxy diferente.
- **Porta do Proxy:** Especifique o número da porta em que o servidor proxy está escutando. Por padrão, a porta é 5750.

Use o Seguinte Par de Chave para Identificação: Se uma CA (certificate authority - autoridade de certificação) interna for implantada, as seguintes opções não serão exibidas. Se uma CA externa foi implantada, preencha os campos a seguir:

- **Chave privada:** Clique em **Procurar** para procurar e selecionar a chave privada do operador remoto.
- **Certificado:** Clique em **Procurar** para procurar e selecionar o certificado correspondente à chave privada. Esse certificado deve ser encadeado à autoridade de certificação configurada na zona.

  Os formatos suportados para a chave e o certificado são DER e PEM.

Instalar o Viewer de Gerenciamento Remoto: Clique no link **Instalar Viewer de Gerenciamento Remoto** para instalar o Viewer de Gerenciamento Remoto. Esse link será exibido somente se você estiver executando a sessão de Gerenciamento Remoto no dispositivo gerenciado pela primeira vez ou se o Viewer de Gerenciamento Remoto não estiver instalado no dispositivo gerenciado.

6 Clique em **OK** para iniciar a sessão.

Executando uma operação de Diagnóstico Remoto

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue pela pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo a ser gerenciado.
3. Selecione o dispositivo, clicando na caixa de seleção ao lado dele.
4. Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Diagnóstico Remoto** para exibir a caixa de diálogo Diagnóstico Remoto.
5. Na caixa de diálogo Diagnósticos Remotos, preencha os seguintes campos:

   Dispositivo: Especifique o nome ou o endereço IP do dispositivo a ser diagnosticado remotamente.

   Sempre assumir como padrão endereços IP para todos os dispositivos: Selecione para que o sistema exiba o endereço IP em vez do nome DNS.

   Os valores especificados para acessar um dispositivo durante a execução da operação de Controle Remoto são gravados no sistema quando você clica em **OK**. Alguns desses valores são selecionados automaticamente durante as operações de Controle Remoto subsequentes, dependendo do dispositivo ou do operador remoto

   Aplicativo: Selecione o aplicativo a ser iniciado no dispositivo para diagnóstico remoto.

   Autenticação: Selecione o modo que você deseja usar para se autenticar no dispositivo gerenciado. Estas são as duas opções:

   - **Senha:** Fornece autenticação baseada em senha para executar uma operação de Diagnósticos Remoto. Você deve inserir a senha correta conforme definida pelo usuário no dispositivo gerenciado ou conforme definida pelo administrador nas configurações de segurança da política de Gerenciamento Remoto. A senha definida pelo usuário têm preferência em relação à senha configurada pelo administrador.
   - **Direitos:** Essa opção está disponível somente quando você seleciona o dispositivo gerenciado em que a operação remota deve ser executada. Se um administrador já designou direitos de Gerenciamento Remoto a você para que execute a operação remota desejada no dispositivo gerenciado selecionado, você obterá acesso automaticamente assim que a sessão for iniciada.

   Porta: Especifique o número da porta em que o Agente de Gerenciamento Remoto está escutando. Por padrão, o número de porta é 5950.

   Modo de Sessão: Não se aplica à operação de Diagnósticos Remotos.

   Criptografia de sessão: Garante a proteção da sessão remota usando a criptografia SSL (protocolo TLSv1).

   Habilitar Armazenamento em Cache de Memória: Habilita o armazenamento em cache dos dados da sessão de gerenciamento remoto para melhorar o desempenho. No momento, essa opção é suportada apenas no Windows.

   Habilitar Otimização de Largura de Banda Dinâmica: Habilita a detecção da largura de banda de rede disponível e ajusta as configurações da seção de acordo para melhorar o desempenho.

   Enable Logging: Registra informações de sessão e depuração no arquivo `novell-zenworks-vncviewer.txt`. Por padrão, o arquivo será gravado na área de trabalho, se você iniciar o ZENworks Control Center por meio do Internet Explorer, e no diretório instalado do Mozilla, se você iniciar o ZENworks Control Center por meio do Mozilla FireFox.

Rotear por Proxy: Permite que a operação de gerenciamento remoto do dispositivo gerenciado seja roteada através de um servidor proxy. Se o dispositivo gerenciado estiver em uma rede privada ou no outro lado de um firewall ou roteador que esteja usando NAT (Network Address Translation - Conversão de Endereço de Rede), a operação de gerenciamento remoto do dispositivo poderá ser roteada através de um servidor proxy. Preencha os campos a seguir:

- **Proxy:** Especifique o nome DNS ou o endereço IP do servidor proxy. Por padrão, o servidor proxy configurado no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um servidor proxy diferente.
- **Porta do Proxy:** Especifique o número da porta em que o servidor proxy está escutando. Por padrão, a porta é 5750.

6 Clique em **OK** para iniciar a sessão.

Executando uma operação de Transferência de Arquivos

1 No ZENworks Control Center, clique na guia **Dispositivos**.

2 Navegue pela pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo a ser gerenciado.

3 Selecione o dispositivo, clicando na caixa de seleção ao lado dele.

4 Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Transferir Arquivos** para exibir a caixa de diálogo Transferência de Arquivos.

5 Na caixa de diálogo Transferência de Arquivos, preencha os seguintes campos:

Dispositivo: Especifique o nome ou o endereço IP do dispositivo a ser acessado.

Sempre assumir como padrão endereços IP para todos os dispositivos: Selecione para que o sistema exiba o endereço IP em vez do nome DNS. Os valores especificados para acessar um dispositivo durante a execução da operação de Controle Remoto são gravados no sistema quando você clica em **OK**. Alguns desses valores são selecionados automaticamente durante as operações de Controle Remoto subsequentes, dependendo do dispositivo ou do operador remoto.

Autenticação: Selecione o modo que você deseja usar para se autenticar no dispositivo gerenciado. Estas são as duas opções:

- **Senha:** Fornece uma autenticação baseada em senha para executar uma operação. Você deve inserir a senha correta conforme definida pelo usuário no dispositivo gerenciado ou conforme definida pelo administrador nas configurações de segurança da política de Gerenciamento Remoto. A senha definida pelo usuário têm preferência em relação à senha configurada pelo administrador.
- **Direitos:** Essa opção está disponível somente quando você seleciona o dispositivo gerenciado em que a operação remota deve ser executada. Se um administrador já designou direitos de Gerenciamento Remoto a você para que execute a operação remota desejada no dispositivo gerenciado selecionado, você obterá acesso automaticamente assim que a sessão for iniciada.

Porta: Especifique o número da porta em que o Agente de Gerenciamento Remoto está escutando. Por padrão, o número de porta é 5950.

Modo de Sessão: Não se aplica à operação de Transferência de Arquivos.

Criptografia de sessão: Garante a proteção da sessão remota usando a criptografia SSL (protocolo TLSv1).

Enable Logging: Registra informações de sessão e depuração no arquivo `novell-zenworks-vncviewer.txt`. Por padrão, o arquivo será gravado na área de trabalho, se você iniciar o ZENworks Control Center por meio do Internet Explorer, e no diretório instalado do Mozilla, se você iniciar o ZENworks Control Center por meio do Mozilla FireFox. Em um Console de Gerenciamento do Linux, o arquivo é gravado no diretório Pessoal do usuário conectado.

Rotear por Proxy: Permite que a operação de gerenciamento remoto do dispositivo gerenciado seja roteada através de um servidor proxy. Se o dispositivo gerenciado estiver em uma rede privada ou no outro lado de um firewall ou roteador que esteja usando NAT (Network Address Translation - Conversão de Endereço de Rede), a operação de gerenciamento remoto do dispositivo poderá ser roteada através de um servidor proxy. Preencha os campos a seguir:

- **Proxy:** Especifique o nome DNS ou o endereço IP do servidor proxy. Por padrão, o servidor proxy configurado no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um servidor proxy diferente.
- **Porta do Proxy:** Especifique o número da porta em que o servidor proxy está escutando. Por padrão, a porta é 5750.

6 Clique em **OK** para iniciar a sessão.

Executando operações de Controle Remoto, Tela Remota e Login Remoto em um dispositivo do Linux

1 No ZENworks Control Center, clique na guia **Dispositivos**.

2 Navegue pela pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo a ser gerenciado.

3 Selecione um dispositivo do Linux clicando na caixa de seleção na frente do dispositivo.

4 Clique em **Ação** > **Controle Remoto** para exibir a caixa de diálogo Gerenciamento Remoto.

5 Na caixa de diálogo Gerenciamento Remoto, preencha os seguintes campos:

Dispositivo: Especifique o nome ou o endereço IP do dispositivo que você deseja gerenciar remotamente.

Sempre assumir como padrão endereços IP para todos os dispositivos: Selecione para que o sistema exiba o endereço IP em vez do nome DNS.

Os valores especificados para acessar um dispositivo durante a execução da operação de Controle Remoto são gravados no sistema quando você clica em **OK**. Alguns desses valores são selecionados automaticamente durante as operações de Controle Remoto subsequentes, dependendo do dispositivo ou do operador remoto.

Operação: Selecione o tipo de operação remota (Controle Remoto, Tela Remota ou Login Remoto) que deseja executar no dispositivo gerenciado:

Porta: Especifique o número da porta em que o Agente de Gerenciamento Remoto está escutando. Por padrão, o número da porta é 5950 para as operações de Controle Remoto e Tela Remota; e 5951 para a operação de Login Remoto.

Enable Logging: Registra informações de sessão e depuração no arquivo `novell-zenworks-vncviewer.txt`. Por padrão, o arquivo será gravado na área de trabalho, se você iniciar o ZENworks Control Center por meio do Internet Explorer, e no diretório instalado do Mozilla, se você iniciar o ZENworks Control Center por meio do Mozilla FireFox. Em um Console de Gerenciamento do Linux, o arquivo é gravado no diretório Pessoal do usuário conectado.

Rotear por Proxy: Permite que a operação de gerenciamento remoto do dispositivo gerenciado seja roteada através de um servidor proxy. Se o dispositivo gerenciado estiver em uma rede privada ou no outro lado de um firewall ou roteador que esteja usando NAT (Network Address Translation - Conversão de Endereço de Rede), a operação de gerenciamento remoto do dispositivo poderá ser roteada através de um servidor proxy. Preencha os campos a seguir:

- **Proxy:** Especifique o nome DNS ou o endereço IP do servidor proxy. Por padrão, o servidor proxy configurado no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um servidor proxy diferente.
- **Porta do Proxy:** Especifique o número da porta em que o servidor proxy está escutando. Por padrão, a porta é 5750.

Instalar o Viewer de Gerenciamento Remoto: Clique no link **Instalar Viewer de Gerenciamento Remoto** para instalar o Viewer de Gerenciamento Remoto. Esse link será exibido somente se você estiver executando a sessão de Gerenciamento Remoto no dispositivo gerenciado pela primeira vez ou se o Viewer de Gerenciamento Remoto não estiver instalado no dispositivo gerenciado.

6 Clique em **OK** para iniciar a sessão.

Executando a operação de SSH Remoto em um dispositivo do Linux

1 No ZENworks Control Center, clique na guia **Dispositivos**.

2 Navegue pela pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo a ser gerenciado.

3 Selecione um dispositivo do Linux clicando na caixa de seleção na frente do dispositivo.

4 Clique em **Ação** > **SSH Remoto** para exibir a caixa de diálogo SSH Remoto.

5 Na caixa de diálogo SSH Remoto, preencha os seguintes campos:

Dispositivo: Especifique o nome ou o endereço IP do dispositivo ao qual você deseja conectar-se remotamente. Se o dispositivo não estiver na mesma rede, você deverá especificar o endereço IP do dispositivo.

Nome do Usuário: Especifique o nome de usuário usado para efetuar login no dispositivo remoto. O padrão é `root`.

Porta: Especifique o número de porta do serviço SSH Remoto. Por padrão, o número de porta é 22.

Clicar em **OK** o solicita a iniciar o Disparador Java Web Start de SSH Remoto. Clique em Sim para aceitar o certificado e clique em **Executar**. Para continuar a conexão com o dispositivo, clique em **Sim**. Você será solicitado a digitar a senha para conectar-se ao dispositivo gerenciado.

6 Clique em **OK** para iniciar a sessão.

Onde encontrar mais informações

Para obter mais informações sobre gerenciamento remoto de dispositivos, consulte a *Referência de Gerenciamento Remoto do ZENworks*.

Coletando inventário de software e hardware

O ZENworks Configuration Management permite que você colete informações de software e hardware dos dispositivos. Você pode ver o inventário de um dispositivo individual e gerar inventário com base em critérios específicos.

Por exemplo, você deseja distribuir um aplicativo de software que tem requisitos específicos de processador, memória e espaço em disco. Você cria dois, um que lista todos os dispositivos que atendem aos requisitos e outro que lista os dispositivos que não atendem aos requisitos. Com base nisso, distribua o software para os dispositivos compatíveis e crie um plano de upgrade para os dispositivos não compatíveis.

Por padrão, os dispositivos são automaticamente explorados à 1 h no primeiro dia do mês. Você pode modificar a programação, bem como muitas outras definições de configuração de **Inventário**, na guia **Configuração** do ZENworks Control Center.

Iniciando a exploração de um dispositivo

Você pode iniciar a exploração de um dispositivo a qualquer momento.

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue até a pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo que você deseja explorar.
3. Clique no dispositivo para exibir seus detalhes.
4. Na lista de tarefas localizada no painel de navegação esquerdo, clique em **Exploração de Inventário do Servidor** ou **Exploração de Inventário da Estação de Trabalho** para iniciar a exploração.

   A caixa de diálogo Status da Tarefa Rápida exibe o status da tarefa. Quando a tarefa é concluída, você pode clicar na guia **Inventário** para ver os resultados da exploração.

Você também pode usar o comando `inventory-scan-now` no utilitário zman para explorar um dispositivo. Para obter mais informações, consulte "Comandos de inventário" na *Referência de Utilitários de Linha de Comando do ZENworks*.

Vendo um inventário de dispositivo

1. No ZENworks Control Center, clique na guia **Dispositivos**.
2. Navegue até a pasta `Servidores` ou `Estações de Trabalho` até localizar o dispositivo que você deseja explorar.
3. Clique no dispositivo para exibir seus detalhes.
4. Clique na guia **Inventário**.

Gerando um relatório de inventário

O ZENworks Configuration Management inclui vários padrões. Além disso, você pode criar relatórios personalizados para fornecer diferentes exibições das informações de inventário.

1. No ZENworks Control Center, clique na guia .
2. No painel de Inventário Padrão, clique em **Aplicativos de Software**.
3. Clique no relatório **Sistema Operacional** para gerar o relatório.

   Usando as opções localizadas na parte inferior do relatório, você pode gravar o relatório gerado como uma planilha do Microsoft Excel, um arquivo CSV (comma-separated values - valores separados por vírgula), um arquivo PDF ou um arquivo gráfico PDF.

Onde encontrar mais informações

Para obter mais informações sobre inventário, consulte a *Referência do Asset Inventory do ZENworks*.

Linux Management

O Linux Management facilita a adoção e a extensão do Linux no ambiente existente. Ele usa a automação orientada por políticas para implantar, gerenciar e manter recursos do Linux. As políticas inteligentes e automatizadas permitem fornecer controle centralizado durante o ciclo de vida dos sistemas Linux para bloqueio de área de trabalho, criação de imagens, gerenciamento remoto, gerenciamento de inventário e de software. O resultado é uma abrangente solução de gerenciamento do Linux que elimina os esforços de TI reduzindo grandemente o overhead necessário para gerenciar sistemas Linux.

É possível aplicar patch aos dispositivos do Linux usando um dos seguintes itens:

- Gerenciamento de Patch
- Gerenciamento de Pacote do Linux

Gerenciamento de Patch

O Gerenciamento de Patch é um recurso totalmente integrado do ZENworks que oferece patch baseado no agente, patch de vulnerabilidade e solução de gerenciamento de conformidade.

O Gerenciamento de Patch dispõe dos seguintes recursos:

- Usa assinaturas para determinar os patches necessários e os retorna para fácil geração de relatórios.
- Implementa as linhas de base obrigatórias referentes a determinados patches para que estejam sempre presentes no dispositivo.
- Aplica os patches apenas às distribuições SLES e RHEL.

Para obter mais informações, consulte o Capítulo 12, “Gerenciamento de patch” na página 129.

Gerenciamento de Pacote do Linux

O Gerenciamento de Pacote do Linux foi desenvolvido para trabalhar com a funcionalidade de gerenciamento de pacote do ZENworks Configuration Management para dispositivos do Linux (servidores e áreas de trabalho).

O Gerenciamento de Pacote do Linux oferece os seguintes recursos:

- Dispõe de gerenciamento de ponto único para aplicação de patches, instalação e atualização de pacotes para um grande número de dispositivos do Linux em um nível corporativo.
- Faz o espelhamento de atualizações e pacotes dos repositórios NU, RHN, RCE e YUM para patches e pacotes como bundles do ZENworks. É possível atribuir esses bundles a dispositivos gerenciados pelo Linux para o gerenciamento de pacote.
- Suporta o download de RPMs delta em dispositivos gerenciados sempre que os RPMs delta estiverem disponíveis e forem aplicáveis, reduzindo assim a largura de banda necessária durante a aplicação de patch.
- Permite escolher catálogos, pacotes e bundles que deseja espelhar.
- Permite aplicar patch aos servidores OES.

Gerenciando dispositivos móveis

O ZENworks Control Center inclui uma página **Introdução ao Gerenciamento Móvel** que orienta você a concluir as tarefas necessárias para registrar e gerenciar dispositivos móveis na zona.

Para acessar a página **Introdução ao Gerenciamento Móvel**:

1. No ZENworks Control Center, clique em **Gerenciamento Móvel** (no painel de navegação esquerdo).

   Cada tarefa de configuração nessa página inclui um ícone com uma marca ⛔ ou ✅ que indica o status de conclusão e um ou mais links para a página na qual você realiza a tarefa.

   Você também pode clicar no ícone ⓘ que aparece ao lado de cada tarefa ou no link **Ajuda** exibido no canto superior direito de cada página para obter informações sobre a tarefa.
2. Conclua as tarefas de **Configuração** que são necessárias para registrar os dispositivos na zona. Na sequência, você pode concluir as tarefas listadas na seção **O que vem a seguir?** para gerenciar esses dispositivos.

   Para obter mais informações sobre cada uma dessas tarefas, consulte a ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).

Registrando dispositivos móveis

Registrando um dispositivo DEP iOS/iPadOS

O registro de um dispositivo DEP é simples para um usuário final, pois você pode permitir que o usuário ignore a maioria dos prompts de ativação de dispositivo modificando o Perfil do DEP. Antes de registrar um dispositivo DEP, você deve atender aos seguintes pré-requisitos:

Pré-requisitos

- Adicione um Servidor DEP no ZCC que vincule o Servidor ZENworks MDM e o Servidor MDM virtual no portal da Apple.
- Atribua dispositivos ao Servidor MDM virtual no portal da Apple. Em seguida, esses dispositivos são descobertos pelo ZENworks e preenchidos no ZCC.
- (Opcional) Atribua usuários ao dispositivo para que apenas eles sejam associados ao dispositivo durante o registro no DEP.
- (Opcional) Modifique as configurações de perfil do DEP para aprimorar o processo de registro.
- (Condicional) Se você modificar o perfil do DEP, verifique se ele foi atribuído com êxito ao Portal da Apple.

Além disso:

- Atribua uma Política de Registro Móvel.
- (Condicional) Se você estiver registrando novamente um dispositivo que foi desativado por outro usuário, verifique se o objeto Dispositivo anterior foi apagado do ZCC.
- (Opcional) Atribua uma Política de E-mail Móvel para configurar a conta de e-mail no dispositivo.

Para obter mais informações sobre cada uma dessas tarefas, consulte a ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).

Procedimento

Siga os prompts de configuração para registrar o dispositivo. Depois que o usuário definir as configurações de Wi-Fi, efetue login no dispositivo com as credenciais do usuário. Se o dispositivo for atribuído a um usuário específico, apenas as credenciais desse usuário deverão ser especificadas, do contrário, haverá falha no registro.

Após o registro do dispositivo, você poderá ver o **Status da Implantação** dele no ZCC, que deve ter mudado de **Descoberto** para **Gerenciado**. É possível ver esse status na página de resumo do dispositivo.

Registrando um dispositivo iOS/iPadOS usando o Apple Configurator

O Apple Configurator é uma ferramenta do Mac OS X que ajuda os administradores na implantação de dispositivos iOS e iPadOS em configurações empresariais ou educacionais. O Apple Configurator agiliza e simplifica a reatribuição de dispositivos, possibilitando que o próximo usuário comece com um novo slate de conteúdo.

Pré-requisitos

- Atribua uma Política de Registro Móvel.

- Copie o URL de Registro na Apple, que especifica o Servidor MDM no qual o dispositivo será registrado. Para saber essa informação, no ZCC, navegue até **Configuração** > **Gerenciamento da Infraestrutura** > **Servidores MDM**. Selecione um Servidor MDM e clique em **URL de Registro na Apple**.
- (Opcional) Atribua uma Política de E-mail Móvel para configurar a conta de e-mail no dispositivo.

Para obter mais informações sobre cada uma dessas tarefas, consulte a ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).

Procedimento

1. Conecte o dispositivo ao Mac pela porta USB.
2. Clique o botão direito do mouse e selecione **Preparar**, ou selecione **Preparar** da barra de menus superior no Apple Configurator.
3. Selecione **Manual** no menu suspenso **Configuração**. Clique em **Avançar**.
4. Selecione o Servidor MDM no qual você deseja registrar o dispositivo. Se você não tem o Servidor MDM gravado no menu suspenso, selecione **Novo Servidor**.
5. Especifique um nome para o servidor e cole o URL de Registro na Apple copiado do ZCC. Para saber essa informação, no ZCC, navegue até **Configuração** > **Gerenciamento da Infraestrutura** > **Servidores MDM**. Selecione um Servidor MDM e clique em **URL de Registro na Apple**. Copie o URL e cole-o na página Definir um Servidor MDM no Apple Configurator. Esse Servidor MDM será gravado para uso futuro.
6. Selecione **Supervisionar dispositivos** para definir o dispositivo como supervisionado. A caixa de seleção **Permitir que os dispositivos sejam emparelhados com outros computadores** é automaticamente habilitada.
7. Selecione a organização que supervisionará esses dispositivos.
8. Selecione a opção apropriada no menu suspenso **Assistente de Configuração** para ignorar determinadas etapas de configuração durante o registro do dispositivo. Verifique os itens de configuração que devem ser apresentados durante o registro do dispositivo.
9. Clique em **Preparar** para preparar o dispositivo conectado.

Após a fase de preparação, o dispositivo iOS/iPadOS será redefinido às configurações de fábrica. Depois que o dispositivo for redefinido, siga os prompts que serão exibidos no dispositivo iOS/iPadOS, conforme configurado na página **Assistente de Configuração do iOS** no Apple Configurator. Após inserir a senha do Wi-Fi, será solicitado para o usuário informar as credenciais.

Registrando um dispositivo iOS/iPadOS pelo Portal do Usuário do ZENworks

Este cenário mostra como registrar um dispositivo iOS e iPadOS como totalmente gerenciado na Zona de Gerenciamento do ZENworks. Esse tipo de registro cria um perfil MDM no dispositivo pelo qual você pode aplicar restrições e implantar aplicativos no dispositivo.

Pré-requisitos

- O ZENworks suporta dispositivos com iOS versão 8 e versões mais recentes.

- Uma origem de usuário foi configurada e habilitada para o registro do dispositivo móvel.
- Uma política de registro foi criada e atribuída ao usuário.
- Uma função MDM foi atribuída a um Servidor Principal.
- Notificações por servidor push para dispositivos iOS.
- Para habilitar o ZENworks a sincronizar e-mails para contas do Exchange ActiveSync, um servidor ActiveSync deve ser configurado. Além disso, crie e atribua uma Política de E-mail Móvel com o Servidor ZENworks configurado como proxy para o Servidor ActiveSync. Isso permite que o ZENworks gerencie os e-mails corporativos enviados e recebidos no dispositivo.
- O registro de dispositivos iOS usando o browser Safari em execução no modo particular é suportado apenas no iOS versão 11 ou versões posteriores.

Procedimento

1 Insira *endereço_servidor_ZENworks*/zenworks-eup, em que *endereço_servidor_ZENworks* é o nome DNS ou o endereço IP do Servidor ZENworks MDM, no browser Safari no dispositivo.

   É exibida a tela de login para o Portal do Usuário do ZENworks.

2 Digite o nome de usuário e a senha do usuário. Se a opção **Permitir Registro Simples** for selecionada para a origem de usuário à qual o usuário pertence, o domínio de registro não precisará ser especificado ou, se preferir, especifique o domínio de registro

   Todos os dispositivos associados ao usuário são exibidos no Portal do Usuário do ZENworks.

3 Toque em **Registrar** no canto superior direito para exibir as opções de registro para o dispositivo.

4 Toque em **Apenas Dispositivo Gerenciado** para exibir a tela **Opções de Registro de Dispositivo**. Se você configurou a política de Dispositivo Móvel para permitir que o usuário especifique a propriedade do dispositivo (empresa ou pessoal), essas informações são solicitadas. Selecione a opção de propriedade do dispositivo apropriada e clique em **OK**.

5 Toque em **Fazer Download do Certificado** para exibir a tela **Instalar Perfil**.

   Observação: Se você estiver registrando um dispositivo iOS 12.1.2 ou mais antigo, ao clicar em Fazer Download do Certificado, será levado à tela Instalar Perfil. Clique em Instalar e siga os prompts para instalar o perfil.

   5a Permita que o site na Web faça download do perfil de configuração.

   5b O download do perfil de configuração será feito. Agora você pode avançar para o menu Configurações para fazer download do perfil.

   5c Navegue até o menu Configurações, clique em **Geral** > **Perfis**.

   5d Toque em **Perfil de Confiança do ZENworks**.

   5e Instale o perfil.

6 (Condicional) Habilite o certificado de registro no dispositivo. Esta etapa será exibida nos dispositivos com iOS versão 10.3 ou mais recente. Para habilitar o certificado:

   6a Navegue até o menu **Configurações** no dispositivo e clique em **Geral**.

   6b Clique em **Sobre**.

   6c Clique em **Certificados Confiáveis**.

   6d Habilite o certificado raiz exibido na tela. Retorne à página EUP.

7 Toque em **Fazer Download do Perfil** na tela Registrar como Dispositivo Gerenciado para exibir a tela de instalação do perfil.

Observação: Se o usuário estiver registrando um dispositivo iOS 12.1.2 ou mais antigo, ao clicar em **Fazer Download do Perfil**, ele será levado à tela Instalar Perfil. Toque em **Instalar** e siga os prompts para instalar o perfil.

7a Permita que o site na Web faça download do perfil.

7b O download do perfil de configuração será feito. Agora você pode avançar para o menu Configurações para fazer download do perfil.

7c Navegue até o menu **Configurações** no dispositivo para instalar o perfil e toque em **Geral** > **Perfis**.

7d Toque em **Perfil do Programa de Registro de Dispositivo ZENworks**. O Perfil do Programa de Registro de Dispositivo ZENworks contém o perfil do MDM necessário para o ZENworks gerenciar o dispositivo.

7e Toque em **Instalar** e siga os prompts para instalar o perfil.

8 Retorne à página EUP. O dispositivo é exibido na lista Meus Dispositivos com o status **Registro em andamento**. Você precisa atualizar o browser para mudar o status para Dispositivo é Ativo.

Neste momento, você pode ver o modo de registro na página Informações do Dispositivo no ZCC. Para exibir as informações do dispositivo, no painel de navegação esquerdo do ZCC, clique em **Dispositivos** > **Dispositivos Móveis** (ou navegue até a pasta, conforme configurado na Política de Registro Móvel) e selecione o dispositivo apropriado. O registro será exibido como **iOS MDM**.

9 Uma conta de e-mail é configurada automaticamente no dispositivo de acordo com a Política de E-mail Móvel atribuída ao usuário ou dispositivo.

Registrando dispositivos Android no modo de perfil de trabalho

O modo de perfil de trabalho cria containers dedicados nos dispositivos para aplicativos e dados corporativos, permitindo assim que a organização gerencie apenas os dados corporativos. Esse modo tem como foco o cenário BYOD, em que o usuário leva seu próprio dispositivo ao local de trabalho.

Pré-requisitos

Configurações obrigatórias

- Crie uma Assinatura do Android Empresa.
- Crie e atribua uma Política de Registro Móvel.
- Crie e atribua uma Política de Registro de Perfil do Android.
- Verifique se a versão do Android é 5.0 ou mais recente (para o modo de perfil de trabalho) e 6.0 ou mais recente (para o modo de dispositivo gerenciado pela empresa).

Configurações opcionais

- Convide usuários para registrar os dispositivos deles.

Para obter mais informações sobre cada uma dessas tarefas, consulte a ZENworks Mobile Management Reference (Referência de Gerenciamento Móvel do ZENworks).

Procedimento

O cenário elaborado nesta seção destina-se aos usuários que estão registrando seus dispositivos no ZENworks pela primeira vez. Para os usuários que já registraram os dispositivos no modo básico (apenas Aplicativo Android) e desejam efetuar o registro no modo de perfil de trabalho, consulte Registro de perfil de trabalho para usuários existentes.

Procedimento

1. Instale o Aplicativo do Agente do ZENworks pela Google Play Store. Se preferir, o usuário pode seguir o procedimento descrito na carta de convite para fazer download do aplicativo do Agente do ZENworks.
2. Clique em **Abrir** após a instalação. Uma descrição resumida do Agente do ZENworks é exibida. O usuário clica em **Continuar**.
3. Clique em **Ativar este administrador do dispositivo** para habilitar o gerenciamento de dispositivo usando o aplicativo.
4. Efetue login no aplicativo especificando o seguinte:

   Nome de Usuário, Senha, Domínio, URL do Servidor: Especifique o nome de usuário, a senha e o domínio de registro (se **Permitir Registro Simples** estiver desabilitado para o usuário) juntamente com o URL do Servidor ZENworks MDM. O usuário pode obter essas informações na carta de convite.
5. Especifique a propriedade do dispositivo (corporativa ou pessoal) se você configurou a política de Registro Móvel para permitir que o usuário especifique a propriedade. Toque em **OK**.
6. Siga os prompts exibidos nas telas restantes, e o dispositivo configurará automaticamente um perfil de trabalho e será registrado no ZENworks. A tela inicial do Aplicativo do Agente do ZENworks é exibida com o dispositivo registrado e ativo.
7. Veja as informações do dispositivo no ZCC. Clique em **Dispositivos** > **Dispositivos Móveis** (ou navegue até a pasta, conforme configurado na Política de Registro Móvel) do painel de navegação esquerdo no ZCC. Clique no dispositivo apropriado e veja os detalhes na página **Resumo**. O modo de registro é exibido como **Aplicativo Android** e o **Modo de Perfil de Trabalho** também está habilitado.

Depois que o dispositivo for registrado, um ícone de Selo anexado ao ícone do Aplicativo do Agente do ZENworks e outros aplicativos do sistema ajudarão a diferenciar os aplicativos de trabalho dos pessoais.

Registro de perfil de trabalho para usuários existentes

Para os usuários que já efetuaram o registro no ZENworks usando o modo básico de registro (apenas Aplicativo Android) e agora desejam ser registrados no modo de perfil de trabalho, atribua a Política de Registro de Perfil do Android a eles.

Após atribuir a Política de Registro Móvel, os usuários receberão uma notificação em seus dispositivos para configurar um perfil de trabalho ao abrir o aplicativo do Agente do ZENworks.

O usuário clica em **Configurar** e segue os prompts para configurar o perfil de trabalho. O dispositivo configurará automaticamente o perfil de trabalho.

Registrando um dispositivo Android no modo de dispositivo gerenciado pela empresa

O modo de dispositivo gerenciado pela empresa permite que os administradores gerenciem todo o dispositivo, restringindo-o apenas ao uso corporativo. Esse modo tem como principal objetivo os dispositivos de propriedade da empresa.

Pré-requisitos

Configurações obrigatórias

- Crie uma Assinatura do Android Empresa.
- Crie e atribua uma Política de Registro Móvel.
- Crie e atribua uma Política de Registro de Perfil do Android.
- Verifique se a versão do Android é 5.0 ou mais recente (para o modo de perfil de trabalho) e 6.0 ou mais recente (para o modo de dispositivo gerenciado pela empresa).

Procedimento

1. Siga as telas de configuração inicial, como configuração de idioma e de Wi-Fi.
2. Especifique o identificador AFW (afw#zenworks) na tela de configuração que exibe o campo ID do E-mail.
3. Clique em **Próximo** na página Android Empresa para continuar a instalação do Aplicativo do ZENworks.

   O download do aplicativo do agente do ZENworks será feito automaticamente no dispositivo.
4. Clique em **Instalar** para instalar o aplicativo no dispositivo e siga os prompts para concluir a configuração dele.
5. Siga os prompts exibidos nas telas restantes para configurar um dispositivo gerenciado pela empresa. Agora, o dispositivo está configurado, mas ainda precisa ser registrado como dispositivo gerenciado pela empresa.
6. Efetue login no aplicativo com os seguintes detalhes:

   Nome de Usuário, Senha, Domínio, URL do Servidor: Especifique o nome de usuário, a senha e o domínio de registro (se **Permitir Registro Simples** estiver desabilitado para o usuário) juntamente com o URL do Servidor ZENworks MDM.

   O dispositivo gerenciado pela empresa é automaticamente configurado no dispositivo.

Veja as informações do dispositivo no ZCC. Clique em **Dispositivos** > **Dispositivos Móveis** (ou navegue até a pasta, conforme configurado na Política de Registro Móvel) do painel de navegação esquerdo no ZCC. Clique no dispositivo apropriado e veja os detalhes na página **Resumo**. O modo de registro é exibido como **Aplicativo Android** e o **Modo de Dispositivo Gerenciado pela Empresa** também está habilitado.

Registrando um dispositivo apenas ActiveSync

Pré-requisitos

Antes de registrar um dispositivo móvel como totalmente gerenciado ou apenas e-mail, você precisa garantir que os seguintes pré-requisitos sejam atendidos:

- O ZENworks suporta dispositivos com ActiveSync 12.1 e versões mais recentes.
- Uma origem de usuário foi configurada e habilitada para o registro do dispositivo móvel.
- Uma política de registro foi criada e atribuída ao usuário.
- Uma função MDM foi atribuída a um Servidor Principal.
- Notificações por servidor push para um dispositivo Android.
- Para habilitar o ZENworks a sincronizar e-mails para contas do Exchange ActiveSync, um servidor ActiveSync deve ser configurado. Além disso, crie e atribua uma Política de E-mail Móvel com o Servidor ZENworks configurado como proxy para o Servidor ActiveSync.

Procedimento

Este cenário mostra como registrar um dispositivo como Apenas E-mail na Zona de Gerenciamento do ZENworks. Este cenário detalha o procedimento para registrar um dispositivo iOS como Apenas E-mail.

1. Insira *endereço_servidor_ZENworks*/zenworks-eup, em que *endereço_Servidor_ZENworks* é o nome DNS ou o endereço IP do Servidor ZENworks MDM em um browser no dispositivo.

   É exibida a tela de login para o Portal do Usuário do ZENworks.

2. Digite o nome de usuário e a senha no Portal do Usuário do ZENworks. Se a opção **Permitir Registro Simples** for selecionada para a origem de usuário à qual o usuário pertence, o domínio de registro não precisará ser especificado ou, se preferir, especifique o domínio de registro
3. Toque em **Registrar** no canto superior direito para exibir as opções de registro para o dispositivo.
4. Toque em **Apenas E-mail** para exibir a tela **Registrar como apenas E-mail**. Use as informações exibidas para criar uma conta de e-mail para o usuário.

   Depois que o usuário configurar a conta de e-mail, ele receberá um e-mail informando que o processo de registro precisa ser concluído. É possível editar o conteúdo desse e-mail no ZCC navegando até **Configuração** > **Configurações da Zona de Gerenciamento** > **Evento e Colaboração** > **Notificações por E-mail**. Clique no e-mail relevante e edite o conteúdo.

5. Clique no link para o Portal do Usuário Final do ZENworks incluído no e-mail ou visite esse portal, conforme descrito na Etapa 1.

   No Portal do Usuário do ZENworks, o dispositivo é exibido na lista Meus dispositivos. Neste ponto, o dispositivo foi adicionado à Zona de Gerenciamento do ZENworks, mas o registro está pendente.

6. Toque em **Concluir Registro**.

   Se você configurou a política de Registro Móvel para permitir que o usuário especifique a propriedade do dispositivo (empresa ou pessoal), essas informações são solicitadas. No dispositivo, forneça as informações de registro necessárias e toque em **OK**.

A lista Meus Dispositivos é atualizada para mostrar que o dispositivo está registrado e ativo.

7 Verifique se o dispositivo está recebendo e-mails enviando um e-mail de outra conta para o usuário.

Depois que o dispositivo é registrado na Zona de Gerenciamento do ZENworks, o modo de registro do dispositivo é exibido como **ActiveSync** na página Informações do Dispositivo no ZCC. Para exibir as informações do dispositivo, no painel de navegação esquerdo do ZCC, clique em **Dispositivos** > **Dispositivos Móveis** (ou navegue até a pasta, conforme configurado na Política de Registro Móvel) e selecione o dispositivo apropriado.

10 Gerenciamento de Segurança de Endpoint

O ZENworks Endpoint Security Management simplifica a segurança de endpoint oferecendo um gerenciamento centralizado de políticas de segurança em seus dispositivos gerenciados. É possível controlar o acesso de um dispositivo a dispositivos de armazenamento removível, redes wireless e aplicativos. Além disso, é possível proteger os dados por criptografia e a comunicação de rede por imposição de firewall (portas, protocolos e listas de controle de acesso). Você também pode mudar a segurança de um dispositivo de endpoint com base em seu local.

As seções a seguir explicam como usar o Gerenciamento de Segurança de Endpoint para proteger seus dispositivos no escritório, em casa ou em um terminal público no aeroporto:

Ativando o Gerenciamento de Segurança de Endpoint

Caso não tenha ativado o Gerenciamento de Segurança de Endpoint durante a instalação da Zona de Gerenciamento, concedendo uma chave de licença ou ativando a avaliação, execute as seguintes etapas:

1. No ZENworks Control Center, clique em **Configuração**.
2. No painel Licenças, clique em **ZENworks 2020 Endpoint Security Management**.
3. Selecione **Avaliar/Ativar o produto** e preencha os seguintes campos:

   Avaliação de Uso: Selecione essa opção para habilitar um período de avaliação de 60 dias. Após esse período, você deve inserir a chave de licença para continuar usando o produto.

   Chave de Licença do Produto: Especifique a chave de licença que você adquiriu para o Gerenciamento de Segurança de Endpoint. Para adquirir a licença do produto, acesse o site do produto ZENworks Endpoint Security Management (http://www.novell.com/products/zenworks/endpointsecuritymanagement).
4. Clique em **OK**.

Habilitando o Agente de Segurança de Endpoint

O Agente do ZENworks é responsável pelo registro do dispositivo, pela distribuição do conteúdo e pelas atualizações de software de um dispositivo.

Além do Agente do ZENworks, o Agente de Segurança de Endpoint é instalado nos dispositivos quando o ZENworks Endpoint Security Management é ativado (licença completa ou avaliação). O Agente de Segurança de Endpoint é responsável por assegurar o uso obrigatório das configurações de política de segurança no dispositivo.

Convém verificar se o Agente de Segurança de Endpoint está habilitado. Para obter instruções, consulte “Configurando recursos do Agente do ZENworks” na página 39.

Criando locais

Os requisitos de segurança de um dispositivo podem variar de local para local. Por exemplo, você pode ter restrições de firewall pessoais para um dispositivo localizado no terminal de um aeroporto diferentes das restrições de um dispositivo localizado no escritório protegido pelo firewall da sua empresa.

Para assegurar que os requisitos de segurança de um dispositivo sejam apropriados ao seu local, o Gerenciamento de Segurança de Endpoint suporta ambas políticas globais e baseadas em local. Uma política global é aplicada independentemente do local do dispositivo. Uma política baseada em local é aplicada apenas quando o local atual do dispositivo atende aos critérios de um local associado à política. Por exemplo, se você criar uma política baseada em local para o seu escritório corporativo e atribuí-la a um laptop, ela só será aplicada quando o local do laptop for o escritório corporativo.

Para usar as políticas baseadas em local, defina primeiro os locais adequados à sua organização. O local é um tipo de lugar para o qual você tem requisitos de segurança específicos. Por exemplo, você pode ter requisitos de segurança diferentes para quando um dispositivo é usado no escritório, em casa ou no aeroporto.

Os locais são definidos por ambientes de rede. Suponha que você tenha um escritório em Nova York e um em Tóquio. Os dois escritórios têm os mesmos requisitos de segurança. Portanto, você cria um local Escritório e o associa a dois ambientes de rede: Rede do Escritório de Nova York e Rede do Escritório de Tóquio. Cada um desses ambientes é definido explicitamente definido por um conjunto de serviços de gateway, servidor DNS e ponto de acesso wireless. Sempre que o Agente de Segurança de Endpoint determinar a correspondência de seu ambiente de rede atual com a Rede do Escritório de Nova York ou a Rede do Escritório de Tóquio, ele definirá seu local como Escritório e aplicará as políticas de segurança associadas ao local Escritório.

Para obter informações detalhadas sobre como criar locais, consulte a “Criando locais” na página 35.

Criar uma diretiva de segurança

Há 12 políticas de segurança diferentes:

As configurações de segurança de um dispositivo são controladas pelas políticas de segurança aplicadas pelo Agente de Segurança de Endpoint. Há 8 políticas de segurança que controlam uma faixa de recursos relacionados à segurança. É possível usar todas ou algumas das políticas, dependendo das necessidades da sua empresa.

Política	Finalidade
Controle de aplicações	Bloqueia a execução de aplicativos ou nega o acesso dos aplicativos à Internet. Especifique os aplicativos bloqueados ou com acesso à Internet negado.
Hardware de comunicação	Desabilita o seguinte hardware de comunicação: 1394-Firewire, IrDA-Infrared, Bluetooth, serial/paralelo, discagem, com fio e wireless. Cada hardware de comunicação é configurado individualmente, isto é, você pode desabilitar alguns tipos de hardware (por exemplo, Bluetooth e discagem) e deixar outros habilitados
Criptografia de Dados	Habilita a criptografia de dados de arquivos em dispositivos de armazenamento removível.
Firewall	Controla a conectividade de rede desabilitando portas, protocolos e endereços de rede (IP e MAC).
Criptografia de Dados da Microsoft	Gerencia a criptografia de unidades de dados removíveis e pastas de discos fixos usando o Microsoft BitLocker e o Microsoft Encrypting File System (EFS), respectivamente.
Criação de Scripts	Executa um script (JScript ou VBScript) no dispositivo. É possível especificar os acionadores que executam o script. Os acionadores podem ser baseados nas ações, nas alterações de local ou nos intervalos de tempo do Agente de Segurança de Endpoint.
Controle de Dispositivo de Armazenamento	Controla o acesso a unidades de CD/DVD, de disquete e de armazenamento removível. Cada tipo de dispositivo de armazenamento é configurado individualmente, isto é, você pode desabilitar alguns e habilitar outros.
Conectividade USB	Controla o acesso aos dispositivos USB, como dispositivos de armazenamento removível, impressoras, dispositivos de entrada (teclados, mouse etc). É possível especificar dispositivos individuais ou grupos de dispositivos. Por exemplo, você pode desabilitar o acesso a determinada impressora e habilitar o acesso a todos os dispositivos USB Sandisk.
Imposição de VPN	Impõe uma conexão VPN com base no local do dispositivo. Por exemplo, se o local do dispositivo for desconhecido, você poderá impor uma conexão VPN pela qual todo o tráfego da Internet será roteado.
Wi-Fi	Desabilita adaptadores wireless, bloqueia conexões wireless, controla conexões a pontos de acesso wireless etc.

Além das políticas de segurança acima, as seguintes políticas de segurança ajudam na proteção e configuração do Agente de Segurança de Endpoint. Devido à natureza dessas duas políticas, é recomendável criá-las a atribuí-las primeiro.

Política	Finalidade
Configurações de segurança	Protege o Agente de Segurança de Endpoint contra adulteração e desinstalação. Para obter informações sobre a configuração de Segurança do Agente do ZENworks, consulte a "Configurando a segurança do Agente do ZENworks" na página 41.
Atribuição de Local	Apresenta uma lista dos locais permitidos para um dispositivo ou usuário. O Agente de Segurança de Endpoint avalia para saber se seu ambiente de rede corresponde a algum dos locais permitidos. Em caso positivo, esse local torna-se o local de segurança e o agente aplica as políticas de segurança associadas ao local. Se nenhum local da lista corresponder, as políticas de segurança associadas ao local Desconhecido serão aplicadas. Se você pretende usar as políticas baseadas em local, verifique se uma política de Atribuição de Local está atribuída a cada dispositivo ou usuário. Se um dispositivo, ou o usuário do dispositivo, não tiver uma política de Atribuição de Local atribuída, o Agente de Segurança de Endpoint não poderá aplicar nenhuma política baseada em local ao dispositivo.

Para criar uma política de segurança:

1. No ZENworks Control Center, clique em **Políticas** para exibir a página Políticas.
2. No painel Políticas, clique em **Nova** > **Política** para iniciar o Assistente de Criação de Nova Política.
3. Na página Selecionar Plataforma, selecione **Windows** e clique em **Próximo**.
4. Na página Selecionar Categoria de política, selecione **Políticas de Segurança de Endpoint do Windows**, depois clique em **Próximo**.
5. Na página Selecionar Tipo de política, selecione o tipo de política que deseja criar e clique em **Próximo**.

   Se você criou locais e pretende usar as políticas baseadas em local, precisará criar no mínimo uma política de Atribuição de Local a atribuí-la a dispositivos ou usuários dos dispositivos. Do contrário, nenhum dos locais criados estará disponível aos dispositivos; portanto, nenhuma política baseada em local poderá ser aplicada.
6. Na página Definir Detalhes, digite o nome da política e selecione a pasta na qual deseja colocá-la.

   O nome deve ser exclusivo dentre todas as outras políticas localizadas na pasta selecionada.
7. (Condicional) Se a página Configurar Herança e Atribuições de Local aparecer, defina as seguintes configurações e depois clique em **Avançar**.
   - **Herança:** Deixe a configuração **Herdar da hierarquia de políticas** selecionada para habilitar esta política para herdar as configurações de políticas do mesmo tipo que são atribuídas a um nível mais alto da hierarquia de políticas. Por exemplo, se você atribuir esta política a

um dispositivo e outra política (do mesmo tipo) à pasta do dispositivo, essa opção habilitada permitirá que esta política herde as configurações da política atribuída à pasta do dispositivo. Anule a seleção da configuração **Herdar da hierarquia de políticas** se não quiser permitir que esta política herde as configurações de política.

- **Atribuições de Local:** As políticas podem ser globais ou baseadas em local. Uma política global é aplicada independentemente do local. Uma política baseada em local é aplicada apenas quando o dispositivo detecta que está dentro dos locais atribuídos à política.

  Selecione se a política é global ou baseada em local. Se você selecionar a política baseada em local, clique em **Adicionar**, selecione os locais aos quais deseja atribuir a política e clique em **OK** para adicioná-los à lista.

8 Defina as configurações específicas à política e clique em **Avançar** até chegar à página Resumo.

  Para obter informações sobre as configurações de uma política, clique em **Ajuda** > **Página Atual** no ZENworks Control Center.

9 Na página Resumo, revise as informações para verificar se estão corretas. Se não estiverem corretas, clique no botão **Voltar** para rever a página do assistente apropriada e fazer mudanças. Se estiverem corretas, selecione uma das seguintes opções (se desejado) e clique em **Concluir**.

- **Criar como Área de Segurança:** Selecione essa opção para criar a política como versão de área de segurança. A versão de área de segurança é isolada dos usuários e dispositivos até sua publicação. Por exemplo, é possível atribuí-la a usuários e dispositivos, mas ela é aplicada apenas após sua publicação.
- **Definir Propriedades Adicionais:** Selecione essa opção para exibir as páginas de propriedades da política. Essas páginas permitem modificar as configurações de política e atribuir a política a usuários e dispositivos.

Atribuindo uma política a usuários e dispositivos

Após criar uma política, você precisa aplicá-la aos dispositivos atribuindo a política aos dispositivos ou usuários do dispositivo.

1 No painel Políticas, marque a caixa de seleção ao lado da política que deseja atribuir.

2 Clique em **Ação** > **Designar o ao Dispositivo**.

  ou

  Clique em **Ação** > **Designar ao Usuário.**

3 Siga os prompts para atribuir a política.

  Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

  Ao concluir o assistente, os dispositivos ou usuários atribuídos são adicionados à página Relacionamentos da política. É possível clicar na política para ver as atribuições.

Atribuindo uma política à zona

É possível atribuir políticas de segurança à Zona de Gerenciamento. Ao determinar as políticas efetivas que terão seu uso obrigatório assegurado no dispositivo, as políticas da Zona serão avaliadas após todas as outras políticas atribuídas a usuários e dispositivos. Considere as seguintes situações:

- Nenhuma política de Firewall está atribuída a um dispositivo ou ao usuário do dispositivo (seja diretamente ou por meio de grupo ou pasta). A política de Firewall da Zona torna-se a política efetiva para o dispositivo e seu uso obrigatório é assegurado no dispositivo.
- As políticas de Firewall são atribuídas a um dispositivo e seu respectivo usuário. Ambas as políticas são avaliadas e fundidas para determinar a política de Firewall efetiva que será aplicada ao dispositivo. Após determinada a política efetiva a partir das políticas atribuídas ao usuário e ao dispositivo, a política de Firewall da Zona é usada para fornecer quaisquer valores que 1) estejam indefinidos na política de Firewall efetiva e 2) sejam adicionáveis (como as tabelas multivalor de Regras de Porta/Protocolo).

Você pode definir as políticas de Zona em três níveis. Isso lhe permite atribuir políticas de Zona diferentes a dispositivos diferentes dentro da sua Zona de Gerenciamento.

- **Zona de Gerenciamento:** As políticas atribuídas na Zona de Gerenciamento tornam-se as políticas da Zona de todos os dispositivos, exceto se você especificar políticas diferentes da Zona no nível do dispositivo ou da pasta de dispositivo.
- **Pasta de Dispositivo:** As políticas que você define em uma pasta de dispositivo anulam a Zona de Gerenciamento (e qualquer pasta pai de dispositivo) e tornam-se as políticas de Zona para todos os dispositivos contidos na estrutura de pastas, a menos que sejam especificadas políticas de Zona diferentes para uma subpasta ou para um dispositivo individual.
- **Dispositivo:** As políticas que você define para um dispositivo individual anulam a Zona de Gerenciamento e a pasta de dispositivo, e tornam-se as políticas de Zona para o dispositivo.

As etapas a seguir apresentam instruções para atribuir políticas na Zona de Gerenciamento.

1. No ZENworks Control Center, clique em **Configuração** para exibir a página Configuração.
2. No painel Configurações da Zona de Gerenciamento, clique em **Gerenciamento de Segurança de Endpoint**.
3. Clique em **Configurações de Política de Zona** para exibir a página Configurações de Política de Zona.
4. Clique em **Adicionar**, procure e selecione as políticas que deseja atribuir à zona e clique em **OK** para adicioná-las à lista.
5. Quando terminar de adicionar as políticas, clique em **OK**.

Onde encontrar mais informações

Para obter mais informações sobre o ZENworks Endpoint Security Management, consulte o seguinte:

- *ZENworks Endpoint Security Policies Reference* (Referência de Políticas de Segurança de Endpoint do ZENworks)
- *ZENworks Endpoint Security Agent Reference* (Referência do Agente de Segurança de Endpoint do ZENworks)

- *ZENworks Endpoint Security Utilities Reference* (Referência de Utilitários de Segurança de Endpoint do ZENworks)
- *ZENworks Endpoint Security Scripting Reference* (Referência de Criação de Scripts de Segurança de Endpoint do ZENworks)

11 Criptografia de disco cheio

O ZENworks Full Disk Encryption protege os dados do dispositivo contra acesso não autorizado quando o dispositivo é desligado ou entra no modo de hibernação. Para isso, ele usa uma combinação de criptografia de disco e autenticação pré-inicialização.

A Criptografia de Disco Cheio oferece criptografia baseada em software em discos rígidos padrão, de estado sólido e autocriptografados. Todos os volumes do disco (ou os volumes selecionados do disco) são criptografados, incluindo todos os arquivos temporários, de troca e de sistema operacional nos volumes. É possível acessar os dados somente quando um usuário válido efetua login com êxito, e os dados nunca podem ser acessados inicializando o dispositivo a partir de mídia, como CD/DVD, disquete ou unidade USB. Para o usuário autenticado, o acesso aos dados em disco criptografado é igual ao acesso aos dados em um disco não criptografado.

A Criptografia de Disco Cheio fornece autenticação pré-inicialização opcional para discos rígidos. O componente Autenticação Pré-inicialização do ZENworks (PBA) é instalado como uma pequena partição Linux no disco rígido. O login ocorre pelo ZENworks PBA, que está protegido contra modificação porque utiliza checksums MDT e extração de senha por meio de criptografia forte para as chaves.

O ZENworks PBA suporta single sign-on com o login do Windows, permitindo que os usuários digitem apenas um conjunto de credenciais (usuário/senha ou smart card) para efetuar login tanto no ZENworks PBA quanto no sistema operacional Windows.

Ativando a criptografia de disco cheio

Caso você não tenha ativado a Criptografia de Disco Cheio durante a instalação da Zona de Gerenciamento, inserindo uma chave de licença ou ativando a avaliação, será necessário fazer isso agora.

Para ativar a Criptografia de Disco Cheio:

1. No ZENworks Control Center, clique em **Configuração**.
2. No painel Licenças, clique em **ZENworks 2020 Full Disk Encryption**.
3. Selecione **Avaliar/Ativar o produto** e preencha os seguintes campos:

   Avaliação de Uso: Selecione essa opção para habilitar um período de avaliação de 60 dias. Após esse período, você deve inserir a chave de licença para continuar usando o produto.

Chave de Licença do Produto: Especifique a chave de licença que você adquiriu para o ZENworks Full Disk Encryption. Para adquirir a licença do produto, acesse o site do produto ZENworks Full Disk Encryption (http://www.novell.com/products/zenworks/full-disk-encryption).

4 Clique em **OK**.

Habilitando o agente de criptografia de disco cheio

O Agente do ZENworks é responsável pelo registro do dispositivo, pela distribuição do conteúdo e pelas atualizações de software de um dispositivo.

Além do Agente do ZENworks, o Agente de Criptografia de Disco Cheio é instalado nos dispositivos quando o ZENworks Full Disk Encryption é ativado (licença completa ou avaliação). O Agente de Criptografia de Disco Cheio é responsável pela criptografia e decodificação de discos, de acordo com a política de Criptografia de Disco aplicada ao dispositivo.

Verifique se o Agente de Criptografia de Disco Cheio está habilitado. Para obter instruções, consulte Configurando recursos do Agente do ZENworks.

Importante: O ZENworks Full Disk Encryption não suporta Inicialização Segura do Windows, e esse recurso deve ser desabilitado antes da instalação do Agente de Criptografia de Disco Cheio em dispositivos. Para obter mais informações sobre requisitos do sistema, consulte "System Requirements" (Requisitos do sistema) na *ZENworks Full Disk Encryption Agent Reference* (Referência do Agente do ZENworks Full Disk Encryption).

Criando uma política de criptografia de disco

Tanto a criptografia de discos de um dispositivo quanto o uso da Autenticação Pré-inicialização do ZENworks (opcional) são controlados pela política de Criptografia de Disco.

Para criar uma política de Criptografia de Disco:

1 No ZENworks Control Center, clique em **Políticas** para exibir a página Políticas.

2 No painel Políticas, clique em **Nova** > **Política** para iniciar o Assistente de Criação de Nova Política.

3 Na página Selecionar Plataforma, selecione **Windows** e clique em **Próximo**.

4 Na página Selecionar Categoria de Política, selecione **Políticas de Criptografia de Disco Cheio do Windows**, depois clique em **Avançar**.

5 Na página Selecionar Tipo de Política, selecione **Política de Criptografia de Disco** e clique em **Avançar**.

6 Na página Definir Detalhes, digite o nome da política e selecione a pasta na qual deseja colocá-la.

O nome deve ser exclusivo dentre todas as outras políticas localizadas na pasta selecionada.

7 Defina as configurações específicas à política e clique em **Avançar** até chegar à página Resumo.

Para obter informações sobre as configurações de uma política, clique em **Ajuda** > **Página Atual** no ZENworks Control Center.

8 Na página Resumo, revise as informações para verificar se estão corretas. Se não estiverem corretas, clique no botão **Voltar** para rever a página do assistente apropriada e fazer mudanças. Se estiverem corretas, selecione uma das seguintes opções (se desejado) e clique em **Concluir**.

- **Criar como Área de Segurança:** Selecione essa opção para criar a política como versão de área de segurança. A versão de área de segurança é isolada dos usuários e dispositivos até sua publicação. Por exemplo, é possível atribuí-la a usuários e dispositivos, mas ela é aplicada apenas após sua publicação.
- **Definir Propriedades Adicionais:** Selecione essa opção para exibir as páginas de propriedades da política. Essas páginas permitem modificar as configurações de política e atribuir a política a usuários e dispositivos.

Atribuindo a política aos dispositivos

Após criar a política de Criptografia de Disco, você precisará atribuir dispositivos a ela.

A política de Criptografia de Disco é uma política apenas de dispositivo. E possível atribuí-la a dispositivos e pastas de dispositivos. Impossível atribuí-la a grupos de dispositivos, usuários, grupos de usuários ou pastas de usuários.

Além disso, apenas a política mais próxima ao dispositivo é aplicada. Por exemplo, se políticas diferentes forem atribuídas a um dispositivo e à pasta do dispositivo, a política atribuída diretamente ao dispositivo será aplicada.

Importante: A política de Criptografia de Disco não é suportada em dispositivos Windows que usam UEFI BIOS. Se você atribuir uma política de Criptografia de Disco a um dispositivo Windows UEFI, a política não será aplicada ao dispositivo.

---

1 No painel Políticas, marque a caixa de seleção ao lado da política de Criptografia de Disco que deseja atribuir.

2 Clique em **Ação** > **Designar o ao Dispositivo**.

3 Siga os prompts para atribuir a política.

Clique no botão **Ajuda** em cada página do assistente para obter informações detalhadas sobre a página.

Ao concluir o assistente, os dispositivos atribuídos serão adicionados à página Relacionamentos da política. É possível clicar na política para ver as atribuições.

Entendendo o que acontece após uma política ser atribuída a um dispositivo

Depois que você atribuir uma política ao dispositivo, o workflow de imposição da política e de criptografia de disco poderá variar um pouco se você usar a autenticação pré-inicialização. Veja a seguir os conceitos de criptografia de disco e autenticação pré-inicialização que você precisa entender ao aplicar uma política de Criptografia de Disco a um dispositivo.

Criptografia de disco

O ZENworks Full Disk Encryption oferece criptografia baseada em software em discos rígidos padrão, de estado sólido e autocriptografados.

O Full Disk Encryption oferece criptografia baseada em setor do disco inteiro ou de volumes selecionados (partições). Todos os arquivos no volume são criptografados, incluindo arquivos temporários, de troca ou do sistema operacional. Como todos os arquivos são criptografados, os dados não podem ser acessados quando o computador é inicializado de mídia externa, como CD-ROM, disquete ou unidade USB.

Os discos rígidos compatíveis são qualquer um de 2,5 ou 3,5 polegadas com padrão de interface IDE, SATA ou PATA.

Você pode escolher o algoritmo de criptografia padrão do setor (AES, Blowfish, DES ou DESX) e o comprimento da chave mais adequado às necessidades de suas organizações. Se o firmware do dispositivo estiver configurado para UEFI, o algoritmo AES e o comprimento da chave de 256 serão automaticamente utilizados.

Observação: O módulo de criptografia usado no ZENworks Full Disk Encryption para criptografar discos rígidos padrão *não* é certificado pelo padrão FIPS 140-2. No entanto, o módulo de criptografia implementa padrões consistentes com a certificação FIPS 140-2 Nível 1.

Autenticação pré-inicialização

O ZENworks Full Disk Encryption protege os dados do dispositivo quando o dispositivo é desligado ou está no modo de hibernação. Assim que alguém efetua login com êxito no sistema operacional Windows, os volumes criptografados não são mais protegidos e os dados podem ser acessados livremente. Para proporcionar maior segurança no login, é possível usar a Autenticação Pré-inicialização do ZENworks (PBA).

O ZENworks PBA é um componente baseado no Linux. Quando a política de Criptografia de Disco é aplicada a um dispositivo, é criada uma partição de 500 MB com um kernel do Linux e o ZENworks PBA no disco rígido.

Durante a operação normal, o dispositivo é inicializado na partição Linux e carrega o ZENworks PBA. Assim que o usuário insere as credenciais apropriadas (ID de usuário/senha ou smart card), a PBA é terminada e o sistema operacional Windows é inicializado, dando acesso aos dados criptografados nas unidades do Windows que antes estavam ocultas e inacessíveis.

A partição Linux é reforçada para aumentar a segurança, e o ZENworks PBA é protegido contra modificação por meio do uso de checksums MD5 e utiliza criptografia avançada para chaves de autenticação.

A Autenticação Pré-inicialização do ZENworks é altamente recomendada. Se você não usa o ZENworks PBA, os dados criptografados são protegidos apenas pela autenticação do Windows.

Para obter mais informações sobre a Autenticação Pré-inicialização do ZENworks, consulte a *ZENworks Full Disk Encryption PBA Reference* (Referência de PBA do ZENworks Full Disk Encryption).

Onde encontrar mais informações

Para obter mais informações sobre o ZENworks Full Disk Encryption, consulte:

- *ZENworks Full Disk Encryption Policy Reference* (Referência de Políticas do ZENworks Full Disk Encryption)
- *ZENworks Full Disk Encryption Agent Reference* (Referência do Agente do ZENworks Full Disk Encryption)
- *ZENworks Full Disk Encryption PBA Reference* (Referência de PBA do ZENworks Full Disk Encryption)
- *ZENworks Full Disk Encryption Emergency Recovery Reference* (Referência de Recuperação de Emergência do ZENworks Full Disk Encryption)

12 Gerenciamento de patch

O Patch Management permite aplicar patches de software de forma automática e consistente para minimizar vulnerabilidades e problemas.

O Gerenciamento de Patch mantém-se atualizado com os patches e as correções mais recentes, por meio da comunicação comum de Internet com o Serviço de Inscrição de Patch do ZENworks. Após o período de avaliação inicial de 60 dias, você precisa de uma assinatura paga do Gerenciamento de Patch para continuar o download diário das últimas informações sobre vulnerabilidades e patches.

Quando um novo patch fica disponível pelo serviço de assinatura, um Servidor ZENworks faz download das informações sobre esse patch. Você pode distribuir o patch para dispositivos ou desconsiderá-lo.

Com o Patch Management, após o download dos patches para o servidor ZENworks e a execução de uma exploração de patch, você poderá identificar os dispositivos vulneráveis em sua zona. No entanto, não será possível identificar facilmente a vulnerabilidade resolvida pelo patch. Para identificá-la, você precisa abrir a janela Ver Detalhes do Patch ou saber o Identificador CVE que deve ser usado para executar uma pesquisa. Entretanto, como parte do recurso de Segurança, agora o ZENworks oferece uma nova tela de segurança que simplifica a configuração e o monitoramento de segurança na zona. Você detecta rapidamente a postura de segurança dos seus dispositivos com a tela e a abordagem de correção com base na vulnerabilidade. Você pode identificar os patches de acordo com as informações do CVE e corrigir os dispositivos vulneráveis aplicando a política ou o bundle de correção do patch relevante. Veja a seguir o processo que o ZENworks utiliza para identificar essas vulnerabilidades:

1. O administrador cria e executa uma assinatura do CVE para importar os dados do repositório NVD.
2. O administrador cria e executa uma assinatura de Patch para importar os dados do repositório de Conteúdo do Patch.

   Após a execução das assinaturas do CVE e de Patch, os CVEs e os Patches serão importados para o Servidor ZENworks configurado.
3. O ZENworks mapeia os patches para os CVEs com base no Identificador CVE associado à assinatura de patch.

   Quando uma exploração de patch é executada no dispositivo como parte da atualização, os dispositivos vulneráveis são identificados. Os usuários também podem configurar a programação de exploração de patch ou executar manualmente a tarefa rápida Iniciar Exploração de Patch de acordo com os requisitos.
4. Os patches aplicáveis são implantados nos dispositivos vulneráveis, seja por meio das políticas ou dos bundles de correção.

Depois que todos os patches do CVE são instalados no dispositivo, o dispositivo deixa de ser vulnerável.

As seções a seguir explicam como usar os recursos do CVE e do Patch Management para identificar as vulnerabilidade e os problemas que podem ocorrer com software desatualizado ou sem patch.

Criando e configurando a assinatura do CVE

Para permitir que o ZENworks importe os dados do CVE do National Vulnerability Database (NVD), você precisa primeiro criar e executar a assinatura do CVE.

Criando a assinatura do CVE

Para criar a assinatura do CVE:

1. Efetue login no ZENworks Control Center e clique em **Assinar e Compartilhar**.
2. Na lista Assinaturas, clique em **Novo** > **Assinatura**.
3. Na página Selecionar Tipo de Inscrição, selecione Assinatura do CVE e clique em **Próximo**.
4. Na página Definir Detalhes, especifique os seguintes detalhes:
   - **Nome da assinatura:** Um nome exclusivo para a assinatura.
   - **Pasta:** Digite o nome da pasta ou navegue até a pasta em que esta assinatura será criada. Por padrão, a assinatura será criada na pasta /Inscrições.
   - **Descrição:** Uma breve descrição da assinatura. Essa descrição é exibida na página Resumo da assinatura.
5. Clique em **Próximo**.
6. Na página Selecionar Servidor de Assinatura do CVE, navegue até o Servidor Principal no qual o serviço de Assinaura do CVE será executado. O download dos dados do CVE do repositório NVD será feito nesse servidor.
7. Selecione a frequência com que o download dos dados do CVE deverá ser feito do repositório NVD. Por padrão, o download dos dados do CVE é feito Diariamente às 23:00 horas (11 p.m.).

   A assinatura do CVE deve ser executada antes da assinatura do Patch para que a assinatura do Patch realize o mapeamento entre CVE e Patch. Se a assinatura do CVE for executada após a assinatura do Patch, o mapeamento não será realizado até a próxima assinatura do Patch, que pode ser no dia seguinte.
8. Clique em **Próximo** para exibir a página Resumo.
9. Revise as informações e, se for necessário mudar alguma coisa, use o botão **Voltar**.

10 (Condicional) Marque a caixa de seleção **Definir Propriedades Adicionais** para exibir a página Resumo da assinatura após a conclusão do assistente.

   Você pode usar as várias guias da página Resumo para editar as informações da assinatura.

11 (Condicional) Marque a caixa de seleção **Executar Assinatura Agora** para executar o serviço de assinatura logo após a criação da assinatura. Você também pode executar a assinatura posteriormente navegando até a página **Assinar e Compartilhar** e clicando na assinatura do CVE.

12 Clique em **Concluir** para criar a assinatura.

Configurando a assinatura do CVE

Ao criar a assinatura do CVE, se você não selecionou a opção para iniciar o serviço de assinatura logo após a conclusão da assinatura do CVE, pode iniciar a assinatura e também fazer modificações nela selecionando o objeto Assinatura do CVE.

1 No ZCC, clique em **Assinar e Compartilhar** no painel esquerdo.

2 Na página Inscrições, clique no objeto Assinatura do CVE. Os detalhes da Assinatura do CVE são exibidos:

   O painel Geral exibe as seguintes informações:

   - Nome: Exibe o nome da assinatura.
   - Tipo: Exibe o tipo de assinatura.
   - Criado por: Exibe o nome do usuário que criou a assinatura.
   - GUID: Exibe o GUID (Global Unique Identifier) da assinatura, uma string gerada aleatoriamente que fornece um identificador exclusivo para a assinatura.
   - Descrição: Exibe uma descrição da assinatura, se ela foi fornecida quando a assinatura foi criada. A descrição é exibida apenas no ZENworks Control Center. Clique em Editar para mudar a descrição.
   - Habilitado: Mostra se a assinatura está ou não habilitada.
   - Registros de Inscrição: Exibe mensagens associadas à última execução da assinatura. Clique no link Ver Registro para ver os registros de assinatura.

   O painel Inscrição apresenta um resumo da assinatura do CVE. É possível ver os seguintes detalhes:

   - URL dos Feeds do CVE NVD: O URL do repositório NVD de onde os feeds do CVE são importados. Você pode clicar no link Editar para mudar o URL.

     Importante: NÃO mude o URL, a menos que seja orientado pelo Atendimento ao Cliente (Customer Care) da Micro Focus.

   - Servidor de Assinatura do CVE: O servidor que é sincronizado com o repositório NVD, faz download e armazena os dados do CVE no banco de dados do ZENworks.

- Última Replicação: O dia e horário em que o servidor de Assinatura foi sincronizado com o repositório NVD pela última vez. Você pode selecionar as opções relevantes para:
  - Executar Agora: Sincroniza imediatamente sem esperar a programação. Quando a sincronização é feita pela primeira vez, uma execução completa é realizada para fazer download de todos os dados do CVE. No entanto, se a última execução foi executada há menos de 8 dias, é feito o download apenas das mudanças desde a última execução.
  - Importar Manualmente: Faça download dos dados do repositório NVD no formato de arquivo JSON e, em seguida, faça upload do arquivo zip JSON para o servidor. Não é necessário que você execute esta etapa, a menos que haja algum problema com o serviço de assinatura. Para fazer upload do arquivo manualmente, você precisa navegar para https://nvd.nist.gov/vuln/data-feeds e selecionar o arquivo zip referente ao ano em que deseja fazer download dos dados. Você também pode selecionar o arquivo zip referente ao nome do feed **CVE-Modified** para fazer download somente dos dados do CVE modificados.
- Execução Completa: Se nenhum download de dados do CVE foi feito ou se a última execução foi realizada há mais de 8 dias, use esse recurso para fazer download de todos os dados do repositório NVD.
- Status: Indica o status da última sincronização com o repositório NVD.
- Programar Intervalo: O intervalo de execução da sincronização com o servidor NVD. Você pode executar a sincronização em um horário específico, todos os dias (diariamente) ou em um intervalo por hora.

Ativando o gerenciamento de patch

1. No ZENworks Control Center, clique em **Configuração**.
2. No painel Licenças, clique em **ZENworks 2020 Patch Management**.
3. Selecione **Ativar Produto** e preencha os campos:

   Número de Série de Inscrição do Produto: O número de série que você recebe quando compra a licença de assinatura. Caso não tenha adquirido uma licença de assinatura, digite o código de avaliação. Após o período de 60 dias de avaliação, o Gerenciamento de Patch exige uma licença de assinatura paga para que você continue recebendo patches do serviço de assinatura. Para adquirir uma licença de assinatura, consulte o site do produto ZENworks Patch Management (http://www.novell.com/products/zenworks/patchmanagement).
4. Clique em **Aplicar**.

Habilitando o gerenciamento de patch no Agente do ZENworks

Para que o Agente do ZENworks execute as operações de Gerenciamento de Patch no dispositivo, o recurso Gerenciamento de Patch do agente deve ser habilitado. O recurso Gerenciamento de Patch é habilitado por padrão quando o ZENworks Patch Management é ativado (licença completa ou de avaliação).

Verifique se o recurso Gerenciamento de Patch do agente está habilitado. Para obter instruções, consulte “Configurando recursos do Agente do ZENworks” na página 39.

Iniciando o serviço de assinatura de patch

Antes de iniciar o recebimento dos patches, é preciso iniciar o serviço de assinatura em um dos servidores ZENworks e ajustar a programação diária para baixar os patches.

Quando um novo patch está disponível no serviço de assinatura, um Servidor ZENworks faz seu download automaticamente. A página Patches (na guia **Segurança**) exibe o novo patch juntamente com a descrição e o impacto nos negócios. Você pode distribuir o patch para dispositivos ou desconsiderá-lo.

O Gerenciamento de Patch mantém-se atualizado com os patches e as correções mais recentes, por meio da comunicação comum de Internet com o Serviço de Inscrição de Patch do ZENworks. Após um período inicial de avaliação de 60 dias, o Gerenciamento de Patch requer uma assinatura paga para continuar seu download diário das informações mais recentes de vulnerabilidade e patch.

Se houver vários Servidores ZENworks em sua Zona de Gerenciamento, você poderá selecionar qualquer um deles como o Servidor de Gerenciamento de Patch. O servidor selecionado como Servidor de Gerenciamento de Patch deve ter a melhor conectividade com a Internet, pois fará download de novos patches e atualizações diariamente.

Para iniciar o serviço de assinatura:

1. No ZENworks Control Center, clique na guia **Configuração**.
2. No painel Configurações da Zona de Gerenciamento, clique em **Segurança** e clique em **Informações do Serviço de Assinatura de Patch**.
3. Na lista **Iniciar o Serviço de Inscrição**, selecione o servidor ZENworks em que você deseja executar o serviço de assinatura e depois clique em **Iniciar serviço**.

   Quando for iniciada a execução do serviço de assinatura, o botão **Iniciar Serviço** exibirá **Serviço em Execução**.
4. Na lista **Intervalo de Comunicação de Inscrição (Todos os Dias às)**, selecione o horário em que deseja fazer download dos patches diariamente.
5. Clique em **OK**.

Criando políticas de patch

Antes de você começar a implantar patches nos dispositivos, o Agente do ZENworks deve realizar a tarefa DAU (Discover Applicable Updates - Atualizações Aplicáveis de Descoberta). A tarefa DAU permite que o Agente do ZENworks detecte o status (Com Patch, Sem Patch ou Não Aplicável) de cada patch, dependendo dos dispositivos na rede.

O ciclo de detecção de patch ocorre todos os dias no Servidor ZENworks em que a tarefa DAU está programada para todos os dispositivos (servidores e estações de trabalho). É possível também iniciar uma tarefa DAU em um agente individual. Você pode ver os resultados da exploração de detecção de patch na seção Patches da guia **Segurança** ou da guia **Dispositivos** do Servidor ZENworks. Os resultados estão disponíveis mesmo quando a estação de trabalho está desconectada da rede.

Para implantar patches, crie políticas de patch ou use a Implantação de Correção. As políticas de patch automatizam o processo de implantação de patches e são recomendadas no lugar da Implantação de Correção. Você pode definir regras nas políticas de patch para limitar o armazenamento em cache de patch e a distribuição apenas para os patches necessários aos seus dispositivos.

As etapas a seguir pressupõem que um ou mais patches estejam disponíveis no serviço de assinatura.

1. No ZENworks Control Center, navegue até **Segurança** > **Políticas de Patch**.
2. Clique em **Novo** na página Políticas de Patch.
3. Siga os prompts para criar uma política de patch.

   Clique no botão **Ajuda** em cada página para obter informações detalhadas sobre a página.
4. Clique na política de patch depois que ela for criada e selecione a página **Relacionamentos**.
5. Clique em **Adicionar** no painel Atribuições de Dispositivo e atribua um ou mais dispositivos à política.
6. Clique em **Publicar** para distribuir e executar os patches aplicáveis aos dispositivos de acordo com a configuração da política de patch.

Importante: Inicialmente, recomenda-se aplicar patches a um dispositivo de teste antes de aplicá-los aos dispositivos em toda a zona. Quaisquer dispositivos configurados como "Teste" aplicarão os patches automaticamente aos dispositivos de teste atribuídos por meio da Área de Segurança sem executar a Etapa 6 (publicação da política).

Ao criar a política de patch pela primeira vez, você também pode configurá-la para **Aprovar automaticamente os patches após imposições de teste bem-sucedidas**. A seleção dessa opção na configuração da política a publicará automaticamente em todos os dispositivos atribuídos a ela após 100% de aprovação dos dispositivos de Teste (acabando com a necessidade de publicação (Etapa 6 acima)).

Onde encontrar mais informações

Para obter mais informações sobre como monitorar as vulnerabilidades de software em dispositivos usando os dados do CVE e, em seguida, como responder a essas vulnerabilidades aplicando os patches apropriados, consulte a *ZENworks CVE Reference* (Referência do CVE para ZENworks).

Para obter mais informações sobre como configurar o Gerenciamento de Patch, automatizar a distribuição de patch na zona de gerenciamento usando políticas de patch e usar a Implantação de Correção, consulte a *Referência do ZENworks Patch Management*.