Referência de Gerenciamento Remoto

Novell®

ZENworks® 10 Configuration Management SP3

10.3

30 de março de 2010

www.novell.com

Informações Legais

A Novell, Inc., não faz nenhuma representação ou garantia com relação ao conteúdo ou uso desta documentação e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novel, Inc., se reserva o direito de revisar esta publicação e fazer mudanças no conteúdo, a qualquer momento, sem obrigação de notificar nenhum pessoa ou entidade sobre essas revisões ou mudanças.

A Novell, Inc., não faz nenhuma representação ou garantia com relação a nenhum software e especificamente se isenta de qualquer garantia expressa ou implícita de comercialização ou adequação a um propósito específico. Além disso, a Novell, Inc., se reserva o direito de fazer mudanças em qualquer ou todas as partes do software da Novell, a qualquer momento, sem nenhuma obrigação de notificar nenhuma pessoa ou entidade sobre essas mudanças.

Qualquer produto ou informação técnica fornecida sob este Contrato pode estar sujeita aos controles de exportação dos Estados Unidos e leis de comércio de outros países. Você concorda em atender a todos os regulamentos de controle de exportação e obter qualquer licença ou classificação necessária para exportar, reexportar ou importar produtos. Você concorda em não exportar ou reexportar para entidades nas listas de exclusão de exportação dos Estados Unidos atuais ou para países terroristas ou com embargo conforme especificado nas leis de exportação dos Estados Unidos. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. Veja a página da Web Novell International Trade Services (http://www.novell.com/info/exports/) para obter mais informações sobre exportação do software da Novell. A Novell não assume nenhuma responsabilidade por sua falha em obter quaisquer aprovações de exportação necessárias.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
E.U.A.
www.novell.com

Documentação Online: para acessar a documentação online mais recente deste e de outros produtos da Novell, consulte a página de Documentação da Novell na Web (http://www.novell.com/documentation).

Marcas Registradas da Novell

Para ver marcas registradas da Novell, consulte a lista de Marcas registradas e Marcas de Serviço da Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de Terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Índice

Sobre este guia

Esta *Referência de Gerenciamento Remoto do ZENworks 10 Configuration Management* contém informações sobre o Gerenciamento Remoto. As informações deste guia estão organizadas da seguinte maneira:

Público

Este guia destina-se aos administradores do Novell® ZENworks®.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no produto. Use o recurso Comentários do Usuário, localizado na parte inferior das páginas de documentação online, ou acesse o site de feedback de documentação da Novell (http://www.novell.com/documentation/feedback.html) para enviar seus comentários.

Documentação adicional

O ZENworks Configuration Management é suportado por documentação adicional (nos formatos PDF e HTML), que pode ser utilizada para que você conheça e implemente o produto. Para obter a documentação adicional, consulte a documentação do ZENworks 10 Configuration Management SP3 (http://www.novell.com/documentation/zcm10/).

Convenções da documentação

Na documentação da Novell, o símbolo de maior que (>) é usado para separar as ações de uma etapa e os itens de um caminho de referência cruzada.

Um símbolo de marca registrada (®, ™, etc.) indica uma marca registrada da Novell. Um asterisco (*) indica uma marca registrada de terceiros.

Quando for possível digitar um determinado nome de caminho com uma barra invertida em algumas plataformas ou com uma barra normal em outras, o nome do caminho será apresentado com uma barra invertida. Os usuários de plataformas que requerem barras normais, por exemplo, Linux*, devem usar essas barras conforme o necessário no software.

Visão geral

1

O Novell® ZENworks® Configuration Management permite gerenciar dispositivos remotamente a partir do console de gerenciamento. O Gerenciamento Remoto permite:

- Controlar remotamente o dispositivo gerenciado
- Executar arquivos executáveis remotamente no dispositivo gerenciado
- Transferir arquivos entre o console de gerenciamento e o dispositivo gerenciado
- Diagnosticar problemas no dispositivo gerenciado
- Ativar remotamente um dispositivo gerenciado desativado

Revise as seguintes seções:

1.1 Terminologia do Gerenciamento Remoto

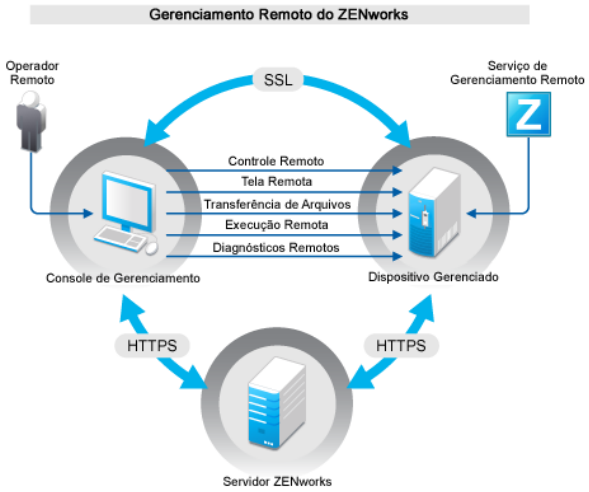
Termos	Descrição
Dispositivo gerenciado	Dispositivo que você deseja gerenciar remotamente. Para gerenciar um dispositivo remotamente, verifique se o componente de Gerenciamento Remoto está instalado no computador e se o serviço de Gerenciamento Remoto está sendo executado no dispositivo.
Servidor de gerenciamento	Um dispositivo em que o servidor ZENworks Configuration Management está instalado.
Console de Gerenciamento	A interface usada para gerenciar e administrar os dispositivos. Para realizar as operações remotas, você deve instalar o viewer de Gerenciamento Remoto no console.
Administrador	Uma pessoa que pode definir políticas e configurações de Gerenciamento Remoto e conceder os direitos correspondentes a operadores remotos.
Serviço de gerenciamento remoto	Um componente do dispositivo gerenciado que permite aos operadores remotos executar operações remotas no dispositivo.
Visualizador de Gerenciamento Remoto	Um aplicativo de console de gerenciamento que permite a um operador remoto executar operações remotas no dispositivo gerenciado. Permite que o operador remoto veja a área de trabalho do dispositivo gerenciado, transfira arquivos e execute aplicativos no dispositivo gerenciado.

Termos	Descrição
Escuta do Gerenciamento Remoto	Um aplicativo de console de gerenciamento que permite que um operador remoto aceite solicitações de assistência remota de usuários de dispositivos gerenciados.
Proxy de Gerenciamento Remoto	Um servidor proxy que encaminha solicitações de operação de Gerenciamento Remoto do Viewer de Gerenciamento Remoto para um dispositivo gerenciado. O proxy é útil quando o viewer não pode acessar diretamente um dispositivo gerenciado que esteja em uma rede privada ou protegida por um firewall ou roteador que utilize NAT (Network Address Translation - Conversão de Endereço de Rede). Como pré-requisito, o proxy deve ser instalado em um dispositivo gerenciado Windows ou um dispositivo Linux (servidor Principal, dispositivo Satélite).

1.2 Compreendendo as operações de gerenciamento remoto

O Gerenciamento Remoto fornece o controle de um dispositivo aos administradores sem a necessidade de uma visita no local. O Gerenciamento Remoto pode poupar tempo e dinheiro para você e para sua empresa. Por exemplo, você ou o suporte técnico de sua empresa pode analisar e corrigir remotamente os problemas do dispositivo gerenciado, sem ir até a estação de trabalho do usuário, o que reduz o tempo de resolução de problemas e aumenta a produtividade.

Figura 1-1 *Operações de gerenciamento remoto*



As seções a seguir ajudam a entender as várias operações de Gerenciamento Remoto:

- Seção 1.2.1, “Controle remoto” na página 13
- Seção 1.2.2, “Tela remota” na página 14
- Seção 1.2.3, “Execução remota” na página 14
- Seção 1.2.4, “Diagnóstico remoto” na página 14
- Seção 1.2.5, “Transferência de arquivos” na página 14
- Seção 1.2.6, “Ativação remota” na página 15

1.2.1 Controle remoto

O Controle Remoto permite que você controle o dispositivo gerenciado remotamente pelo console de gerenciamento, para fornecer assistência ao usuário e ajudar a solucionar problemas do dispositivo.

O Controle Remoto estabelece uma conexão entre o console de gerenciamento e o dispositivo gerenciado. Com conexões de controle remoto, você pode executar todas as operações executadas por um usuário no dispositivo. Para obter mais informações, consulte a Seção 3.1, “Gerenciando uma sessão de controle remoto” na página 53.

1.2.2 Tela remota

A Tela Remota permite que você se conecte remotamente 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 realiza determinadas tarefas em um dispositivo gerenciado para garantir que ele o faça corretamente. Para obter mais informações, consulte a Seção 3.2, “Gerenciando uma sessão de tela remota” na página 57.

1.2.3 Execução remota

A Execução Remota permite executar qualquer arquivo executável com privilégios de sistema no dispositivo gerenciado a partir do console de gerenciamento. Para executar um aplicativo remotamente, especifique o nome do executável na janela Execução Remota. Por exemplo, você pode executar o comando `regedit` para abrir o Editor de Registro no dispositivo gerenciado. Para obter mais informações, consulte a Seção 3.3, “Gerenciando uma sessão de execução remota” na página 58.

1.2.4 Diagnóstico remoto

O Diagnóstico Remoto permite diagnosticar e analisar remotamente os problemas no dispositivo gerenciado. Isto aumenta a produtividade do usuário, por manter as áreas de trabalho em operação. Para obter mais informações, consulte a Seção 3.4, “Gerenciando uma sessão de diagnóstico remoto” na página 58.

O Diagnóstico fornece informações reais que você pode usar para diagnosticar e corrigir os problemas no dispositivo gerenciado. Estes são os aplicativos de diagnóstico padrão no dispositivo gerenciado:

- Informações do Sistema
- Gerenciamento do Computador
- Serviços
- Editor de Registro

1.2.5 Transferência de arquivos

A Transferência de Arquivos executa várias operações de arquivo no console de gerenciamento e no dispositivo gerenciado, como:

- Copiar arquivos entre o console de gerenciamento e o dispositivo gerenciado.

- Renomear arquivos ou pastas
- Apagar arquivos ou pastas
- Criar pastas
- Ver as propriedades de arquivos e pastas
- Abrir arquivos com os aplicativos associados no console de gerenciamento

Para obter mais informações, consulte a Seção 3.5, “Gerenciando uma sessão de transferência de arquivos” na página 60.

Importante: O programa Transferência de Arquivos permite acessar as unidades de rede no dispositivo gerenciado.

1.2.6 Ativação remota

A Ativação Remota permite inicializar remotamente um nó único ou um grupo de nós desativados em sua rede, desde que Wake-on-LAN esteja habilitado na placa de rede do nó. Para obter mais informações, consulte a Seção 3.7, “Ativando um dispositivo remoto” na página 63.

1.3 Compreendendo os recursos de gerenciamento remoto

As seções a seguir ajudam a compreender os vários recursos de Gerenciamento Remoto:

1.3.1 Sinal visível

Permite apresentar uma indicação visível na área de trabalho do dispositivo gerenciado para informar o usuário de que o dispositivo está sendo gerenciado remotamente. O sinal visível exibe a identificação do operador remoto e os detalhes da sessão, como o tipo e o horário de início da sessão remota. O usuário pode encerrar uma sessão remota específica ou fechar a caixa de diálogo de sinal para encerrar todas as sessões remotas.

1.3.2 Detecção de intrusão

O recurso Detecção de Intrusão diminui de maneira significativa o risco de que o dispositivo gerenciado seja invadido. Se o operador remoto falhar ao executar login no dispositivo gerenciado dentro do número especificado de tentativas (o padrão é 5), o serviço de Gerenciamento Remoto será bloqueado e não aceitará nenhuma solicitação de sessão remota até que seja desbloqueado.

1.3.3 Criptografia de sessão

As sessões remotas são asseguradas pelo Secured Socket Layer (protocolo TLSv1).

1.3.4 Sinal sonoro

Quando uma sessão remota está ativa no dispositivo gerenciado, você pode gerar um sinal sonoro em intervalos regulares no dispositivo gerenciado, conforme configurado na política de Gerenciamento Remoto.

1.3.5 Bloqueio de teclado e mouse

Permite bloquear os controles de teclado e mouse do dispositivo gerenciado durante uma sessão remota, de modo que o usuário do dispositivo remoto não possa interromper a sessão.

Observação: Nos dispositivos gerenciados do Windows Vista, os bloqueios de mouse e teclado não funcionam caso o tema Aero esteja habilitado.

1.3.6 Tela em branco

Permite que você limpe a tela do dispositivo gerenciado durante uma sessão remota para impedir que o usuário veja as ações executadas pelo operador remoto durante a sessão. Os controles de teclado e mouse do dispositivo gerenciado também são bloqueados.

Observação: Se a tela de um dispositivo gerenciado do Tablet PC for apagada durante uma sessão remota, o desempenho da sessão será reduzido.

1.3.7 Abend

Permite bloquear o dispositivo gerenciado ou efetuar logout do usuário nesse dispositivo se uma sessão remota for desconectada abruptamente.

1.3.8 Anulando a proteção de tela

Permite anular qualquer proteção de tela protegida por senha no dispositivo gerenciado durante uma sessão remota.

Observação: Esse recurso não está disponível nos dispositivos gerenciados Windows Vista*, Windows Server 2008 e Windows 7.

1.3.9 Encerramento automático de sessão

Encerrará automaticamente uma sessão remota se ela estiver inativa por um período especificado.

1.3.10 Conexão iniciada por agente

Permite que o usuário no dispositivo gerenciado solicite a ajuda de um operador remoto. É possível pré-configurar a lista de operadores remotos para que fiquem disponíveis ao usuário. Para obter mais informações, consulte a Seção 2.8.2, “Iniciando uma sessão pelo dispositivo gerenciado” na página 44.

Observação: Atualmente, este recurso é suportado apenas no Windows.

1.3.11 Colaboração de sessão

Permite que um grupo de operadores remotos colabore para executar em conjunto uma sessão remota. O operador remoto master pode convidar outros operadores remotos para a sessão, delegar os direitos de controle remoto a outro operador remoto para a solução de um problema, retomar o controle do operador remoto e encerrar uma sessão remota. Para obter mais informações, consulte a Seção 3.1.2, “Colaboração de sessão” na página 55.

1.3.12 Auditoria de gerenciamento remoto

Permite gerar registros de auditoria para todas as sessões remotas executadas no dispositivo gerenciado. O registro de auditoria é mantido no dispositivo gerenciado e pode ser visto pelo usuário.

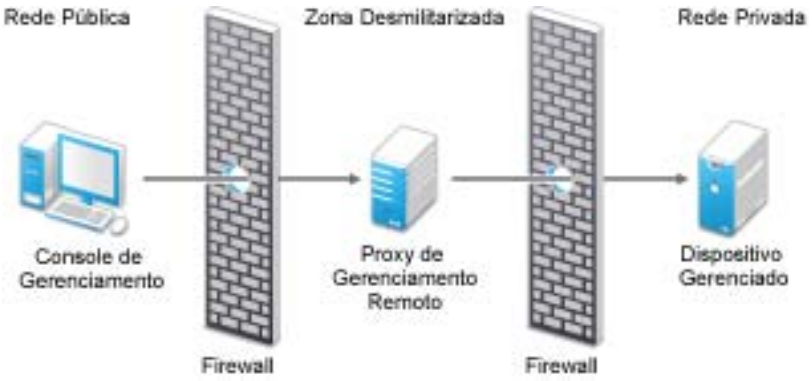
1.4 Entendendo o proxy de gerenciamento remoto

Não é possível executar nenhuma operação de gerenciamento remoto em um dispositivo gerenciado que esteja em uma rede privada ou protegida por um firewall ou roteador que utilize NAT. Isso ocorre porque o firewall do NAT oculta o endereço IP do dispositivo da rede externa e, portanto, bloqueia qualquer solicitação de conexão feita ao dispositivo. Para gerenciar remotamente esse dispositivo, é necessário rotear a operação remota por meio de um Proxy de Gerenciamento Remoto.

Para obter mais informações sobre roteamento de operação remota por meio de proxy ao iniciar uma sessão remota no Console de Gerenciamento, consulte Rotear por Proxy em “Iniciando a sessão de Gerenciamento Remoto no contexto do dispositivo” na página 37.

Para obter mais informações sobre roteamento de operação remota por meio de proxy ao iniciar uma sessão remota do contexto de dispositivo, consulte Rotear por Proxy em “Iniciando uma sessão de Gerenciamento Remoto a partir do contexto do usuário” na página 39.

Figura 1-2 *Proxy de Gerenciamento Remoto*



Você deve instalar o proxy em um dispositivo colocado em uma DMZ (zona desmilitarizada). O dispositivo no qual você instalará o proxy deve estar acessível na rede pública que tem o console de gerenciamento e deve ser capaz de acessar dispositivos que estejam em uma rede privada. Para obter informações sobre como instalar o proxy de gerenciamento remoto, consulte a Seção 2.10, “Instalando um proxy de gerenciamento remoto” na página 49.

Por padrão, o proxy de gerenciamento remoto escuta, na porta 5750, as solicitações de gerenciamento remoto recebidas do Viewer de Gerenciamento Remoto e encaminha as solicitações ao dispositivo.

Configurando o gerenciamento remoto

2

As seções a seguir fornecem informações sobre a implantação do componente de Gerenciamento Remoto do Novell® ZENworks® 10 Configuration Management em um ambiente de produção:

2.1 Definindo configurações de gerenciamento remoto

As configurações do Gerenciamento Remoto são regras que determinam o comportamento ou a execução do serviço de Gerenciamento Remoto no dispositivo gerenciado. São definidas configurações de portas, configurações de sessões e configurações de desempenho durante a sessão remota. Essas configurações podem ser aplicadas nos níveis de zona, pasta e dispositivo.

As seções a seguir fornecem informações sobre a configuração do Gerenciamento Remoto nos diferentes níveis:

2.1.1 Configurando o gerenciamento remoto no nível de zona

Por padrão, as configurações do Gerenciamento Remoto feitas no nível de zona se aplicam a todos os dispositivos gerenciados.

1. No ZENworks Control Center, clique em *Configuração*.
2. No painel Configurações da Zona de Gerenciamento, clique em *Gerenciamento de Dispositivo* e em *Gerenciamento Remoto*.
3. Selecione *Executar Serviço de Gerenciamento Remoto na Porta* e especifique a porta na qual deseja habilitar a execução do serviço de Gerenciamento Remoto.

Por padrão, o serviço de Gerenciamento Remoto escuta na porta número 5950.

4 Selecione as opções de Configurações de Sessão:

Campo	Detalhes
Pesquisar o Nome do Visualizador de DNS no Início da Sessão Remota	Permite que o serviço de Gerenciamento Remoto consulte o nome DNS do console de gerenciamento no início da sessão remota. O nome é gravado nos registros de auditoria e exibido como uma parte das informações da sessão durante as sessões remotas. Se esta opção não for selecionada ou o serviço de Gerenciamento Remoto não puder encontrar o nome do console, ele será exibido como *desconhecido*. Se a pesquisa reversa de DNS não estiver habilitada na sua rede, é recomendável desabilitar essa configuração para que não haja um atraso significativo no início da sessão remota.
Permitir Sessão Remota quando não houver usuários conectados ao dispositivo gerenciado	Permite que um operador remoto gerencie um dispositivo remotamente quando a política permitir a operação remota, mas nenhum usuário tiver efetuado login no dispositivo. Essa opção é selecionada por padrão.

5 Selecione entre as seguintes opções para aprimorar o desempenho durante a sessão remota:

Campo	Detalhes
Suprimir papel de parede	Elimina o papel de parede no dispositivo gerenciado durante uma sessão remota. Isso impede que os dados de bitmap do papel de parede sejam enviados repetidamente ao console de Gerenciamento Remoto, o que melhora o desempenho da sessão remota.
Habilitar driver de otimização	Habilita o driver de otimização que é instalado por padrão em cada dispositivo gerenciado. Se você selecionar essa opção, somente a parte da tela mudada no dispositivo gerenciado será capturada e atualizada no console de Gerenciamento Remoto durante a sessão remota, melhorando, assim, o desempenho dessa sessão.

6 (Opcional) Configure um proxy de gerenciamento remoto para realizar operações remotas no dispositivo gerenciado.

Se o dispositivo gerenciado estiver em uma rede privada ou protegido por um firewall ou roteador que use NAT, a operação de gerenciamento remoto do dispositivo poderá ser roteada por meio de um proxy de gerenciamento remoto. Instale o proxy separadamente. Para obter informações sobre como instalar o proxy de gerenciamento remoto, consulte a Seção 2.10, “Instalando um proxy de gerenciamento remoto” na página 49.

Tarefa	Detalhes
Adicionar um proxy de gerenciamento remoto	1. Clique em *Adicionar* para exibir a caixa de diálogo Adicionar Configurações de Proxy. 2. Preencha os campos a seguir: **Proxy:** especifique o endereço IP ou o nome DNS do proxy de gerenciamento remoto. **Faixa de Endereço IP:** especifique os endereços IP dos dispositivos que deseja gerenciar remotamente por meio do proxy de gerenciamento remoto. Você pode especificar a faixa de endereços IP de uma das seguintes maneiras: ◆ Especifique a faixa de endereços IP que usam a notação CIDR (Classless Inter-Domain Routing - Roteamento Interdomínio sem Uso de Classes). Com o CIDR, a porção decimal pontuada do endereço IP é interpretada como um número binário de 32 bits que foi dividido em quatro bytes de 8 bits. O número após a barra (/n) é o tamanho do prefixo, que é o número de bits iniciais compartilhados, contando a partir do lado esquerdo do endereço. O número /n pode variar de 0 a 32, com 8, 16, 24 e 32 sendo os números normalmente mais usados. Exemplos: 123.45.678.12/16: especifica todos os endereços IP iniciados por 123.45. 123.45.678.12/24: especifica todos os endereços IP iniciados por 123.45.678. ◆ Especifique a faixa de endereços IP no formato **Endereço IP do remetente** - **Endereço IP do destinatário**. Por exemplo: 123.45.678.12 - 123.45.678.15: especifica todos os endereços IP da faixa de 123.45.678.12 a 123.45.678.15.
Apagar um proxy de gerenciamento remoto	1. Selecione o proxy que deseja apagar. 2. Clique em Excluir e depois em *OK*.

7 (Opcional) Configure um aplicativo a ser iniciado no dispositivo durante a sessão de Diagnóstico Remoto adicionando-o à lista de *Aplicativos de Diagnóstico*. Por padrão, a lista contém os seguintes aplicativos:

- Informações do Sistema
- Gerenciamento do Computador
- Serviços
- Editor de Registro

A tabela a seguir lista as tarefas que podem ser realizadas para personalizar a lista de *Aplicativos de Diagnóstico*:

Tarefa	Detalhes
Adicionar um aplicativo	1. Clique em *Adicionar.* 2. Especifique o nome e o caminho do aplicativo no dispositivo gerenciado. 3. Clique em *OK.*
Apagar um aplicativo	1. Selecione o aplicativo a ser apagado. 2. Clique em Apagar e, em seguida, clique em *OK*.
Reverter aos aplicativos padrão	1. Clique em *Reverter* e, em seguida, clique em *OK.*

8 Clique em *Aplicar* e, em seguida, clique em *OK*.

Essas mudanças entrarão em vigor no dispositivo quando ele for atualizado.

2.1.2 Configurando o gerenciamento remoto no nível de pasta

Por padrão, as configurações do Gerenciamento Remoto feitas no nível de zona se aplicam a todos os dispositivos gerenciados. Porém, é possível modificar essas configurações para os dispositivos dentro de uma pasta.

1 No ZENworks Control Center, clique em *Dispositivos*.

2 Clique na pasta (detalhes) para a qual deseja definir as configurações de Gerenciamento Remoto.

3 Clique em *Configurações* e, em seguida, clique em *Gerenciamento de Dispositivo* > *Gerenciamento Remoto*.

4 Clique em *Anular*.

5 Edite as configurações de Gerenciamento Remoto conforme o necessário.

6 Para aplicar as alterações, clique em *Aplicar.*

ou

Para reverter para as configurações do sistema feitas no nível de zona, clique em *Reverter*.

7 Clique em *OK*.

Essas mudanças entrarão em vigor no dispositivo quando ele for atualizado.

2.1.3 Configurando o gerenciamento remoto no nível de dispositivo

Por padrão, as configurações do Gerenciamento Remoto feitas no nível de zona se aplicam a todos os dispositivos gerenciados. Porém, é possível modificar essas configurações para o dispositivo gerenciado:

1 No ZENworks Control Center, clique em *Dispositivos*.

2 Clique em *Servidores* ou *Estações de Trabalho* para exibir a lista de dispositivos gerenciados.

3 Clique no dispositivo para o qual você deseja definir as configurações de Gerenciamento Remoto.

4 Clique em *Configurações* e, em seguida, clique em *Gerenciamento de Dispositivo* > *Gerenciamento Remoto*.

5 Clique em *Anular*.

6 Edite as configurações de Gerenciamento Remoto conforme o necessário.

7 Para aplicar as alterações, clique em *Aplicar*.

ou

Para reverter as configurações de sistema definidas antes no dispositivo, clique em *Reverter*.

Se as configurações de Gerenciamento Remoto no dispositivo foram definidas no nível da pasta, elas serão revertidas para as configurações do nível da pasta definidas; caso contrário, serão revertidas para as configurações do nível da zona padrão.

8 Clique em *OK*.

Essas mudanças entrarão em vigor no dispositivo quando ele for atualizado.

2.2 Habilitando a escuta do gerenciamento remoto

Para habilitar a Escuta do Gerenciamento Remoto e escutar as conexões de um dispositivo gerenciado:

1 No ZENworks Control Center, clique em *Dispositivos*.

2 Em *Tarefas do Dispositivo*, no painel esquerdo, clique em *Escuta do Gerenciamento Remoto*.

3 Na caixa de diálogo Escuta do Gerenciamento Remoto, especifique a porta em que as conexões remotas serão escutadas. Por padrão, o número de porta é 5550.

4 Clique em *OK*.

O ícone da Escuta do Gerenciamento Remoto do ZENworks será exibido na área de notificação.

2.3 Criando a política de gerenciamento remoto

A política de Gerenciamento Remoto permite configurar o comportamento ou a execução de uma sessão de Gerenciamento Remoto no dispositivo gerenciado. A política inclui configurações das operações de Gerenciamento Remoto como Controle Remoto, Tela Remota, Execução Remota, Diagnósticos Remotos e Transferência de Arquivos, além de permitir o controle de configurações para segurança.

Por padrão, uma política segura de Gerenciamento Remoto é criada no dispositivo gerenciado quando o ZENworks Adaptive Agent é implantado com o componente de Gerenciamento Remoto no dispositivo. Você pode usar a política padrão para gerenciar um dispositivo remotamente. Para anular a política padrão, você pode explicitamente criar uma política de Gerenciamento Remoto para o dispositivo.

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

2 Na lista *Políticas*, clique em *Novo* e, em seguida, em *Política* para exibir a página Selecionar Tipo de Política.

3 Selecione *Política de Gerenciamento Remoto*, clique em *Avançar* para exibir a página Definir Detalhes e preencha os campos:

Nome da Política: forneça um nome exclusivo para a política. O nome da política deve ser diferente do nome de qualquer outro item (grupo, pasta etc.) residente na mesma pasta.

Pasta: digite o nome ou vá para a pasta do ZENWorks Control Center na qual deseja que a política resida. O padrão é `/políticas`, mas é possível criar pastas adicionais para organizar as políticas.

Descrição: forneça uma breve descrição do conteúdo da política. Essa descrição aparece na página de resumo da política no ZENworks Control Center.

4 Clique em *Avançar* para exibir a página Configurações Gerais de Gerenciamento Remoto. Para aceitar as configurações padrão, passe para a etapa seguinte ou use as informações especificadas na tabela a seguir para mudar as configurações padrão.

Campo	Detalhes
Permitir que o Usuário Solicite uma Sessão Remota	Permite que o usuário do dispositivo gerenciado solicite a um operador remoto que execute uma sessão remota. O operador remoto deve verificar se a Escuta do Gerenciamento Remoto está em execução.
Encerrar a Sessão Remota Quando a Permissão for Necessária para um Novo Login de Usuário no Dispositivo Gerenciado	Encerra uma sessão remota ininterrupta quando é necessária uma permissão de um novo usuário que tenha efetuado login em um dispositivo gerenciado remotamente.
Exibir Informações de Auditoria da Sessão Remota para o Usuário no Dispositivo Gerenciado	Permite que o usuário do dispositivo gerenciado veja as informações de auditoria das sessões remotas através do ícone do ZENworks.
Exibir as Propriedades de Gerenciamento Remoto no Ícone do ZENworks	Permite que o usuário do dispositivo gerenciado veja as propriedades associadas à política de Gerenciamento Remoto no ícone do ZENworks.
Editar	Para editar a mensagem exibida para o usuário no dispositivo gerenciado antes de iniciar uma sessão remota: 1. Clique em *Editar* para exibir a caixa de diálogo Editar Mensagem. 2. Edite a mensagem. 3. Clique em *OK*.
Restaurar Padrão	Para restaurar a mensagem padrão: 1. Clique em *Restaurar Padrão* para reverter para a mensagem padrão.
Adicionar uma Escuta Remota	Para adicionar uma Escuta Remota: 1. Clique em *Adicionar*. 2. Na caixa de diálogo Adicionar Escuta Remota, especifique o nome DNS ou o endereço IP do console de gerenciamento e o número da porta em que a Escuta do Gerenciamento Remoto escutará as solicitações de sessão remota. 3. Clique em *OK*.

Campo	Detalhes
Apagar uma Escuta Remota	Para apagar uma Escuta Remota: 1. Selecione a Escuta Remota que deseja apagar. 2. Clique em *Apagar*.

5 Clique em *Avançar* para exibir a página Configurações de Controle Remoto. Para aceitar as configurações padrão, passe para a etapa seguinte ou use as informações especificadas na tabela a seguir para mudar as configurações padrão.

Campo	Detalhes
Permitir que o Dispositivo Gerenciado Seja Controlado Remotamente	Permite sessões de Controle Remoto no dispositivo gerenciado. A seleção desta opção habilita as opções subseqüentes na página. Ao anular a seleção da opção, você desabilita a operação de Controle Remoto no dispositivo.
Solicitar Permissão ao Usuário no Dispositivo Gerenciado Antes de Iniciar o Controle Remoto	Permite solicitar permissão do usuário do dispositivo gerenciado antes de iniciar uma sessão de Controle Remoto.
Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado Durante o Controle Remoto	Exibe um sinal visível no canto superior direito da área de trabalho do dispositivo gerenciado durante a sessão de Controle Remoto. O sinal visível permite que o usuário no dispositivo gerenciado saiba que uma sessão de Controle Remoto está em andamento.
Enviar Sinal Sonoro ao Usuário no Dispositivo Gerenciado a Cada [ ] Segundos Durante o Controle Remoto	Gera um sinal sonoro no dispositivo gerenciado durante uma sessão de Controle Remoto. Esse sinal é gerado periodicamente após o número especificado de segundos.
Permitir que a Tela do Dispositivo Gerenciado Fique em Branco Durante o Controle Remoto	Permite que a tela do dispositivo gerenciado fique em branco durante uma sessão de Controle Remoto. Se essa opção for selecionada, o teclado e os controles do mouse também serão bloqueados no dispositivo gerenciado.
Permitir que o Mouse e o Teclado do Dispositivo Gerenciado Sejam Bloqueados Durante o Controle Remoto	Permite bloquear o teclado e o mouse do dispositivo gerenciado durante uma sessão de Controle Remoto.
Permitir que a Proteção de Tela Seja Desbloqueada Automaticamente Durante o Controle Remoto	Habilita o desbloqueio da proteção de tela protegida por senha do Viewer do Controle Remoto antes do início de uma sessão de Controle Remoto no dispositivo gerenciado.
Encerrar a Sessão de Controle Remoto Automaticamente Após Inatividade de [ ] Minutos	Encerra uma sessão de Controle Remoto no dispositivo gerenciado quando ela fica inativa pelo período especificado.

6 Clique em *Avançar* para exibir a página Configurações de Tela Remota. Para aceitar as configurações padrão, passe para a etapa seguinte ou use as informações especificadas na tabela a seguir para mudar as configurações padrão.

Campo	Detalhes
Permitir que o Dispositivo Gerenciado Seja Visto Remotamente	Permite sessões de Tela Remota no dispositivo gerenciado. A seleção desta opção habilita as opções subseqüentes na página. Ao anular a seleção da opção, você desabilita a operação de Tela Remota no dispositivo.
Solicitar Permissão ao Usuário no Dispositivo Gerenciado Antes de Iniciar a Tela Remota	Permite solicitar permissão do usuário no dispositivo gerenciado antes de iniciar uma sessão de Tela Remota.
Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado Durante a Tela Remota	Exibe um sinal visível no canto superior direito da área de trabalho do dispositivo gerenciado durante a sessão de Tela Remota. O sinal visível permite ao usuário do dispositivo gerenciado saber que uma sessão de Tela Remota está em andamento.
Enviar Sinal Sonoro ao Usuário no Dispositivo Gerenciado a Cada [ ] Segundos Durante a Tela Remota	Gera um sinal sonoro no dispositivo gerenciado durante a sessão de Tela Remota. Esse sinal é gerado periodicamente após o número especificado de segundos.

7 Clique em *Avançar* para exibir a página Configurações de Diagnóstico Remoto. Para aceitar as configurações padrão, passe para a etapa seguinte ou use as informações especificadas na tabela a seguir para mudar as configurações padrão.

Campo	Detalhes
Permitir que o Dispositivo Gerenciado Seja Diagnosticado Remotamente	Permite sessões de Diagnóstico Remoto no dispositivo gerenciado. A seleção desta opção habilita as opções subseqüentes na página. Ao anular a seleção da opção, você desabilita a operação de Diagnóstico Remoto no dispositivo.
Solicitar Permissão ao Usuário no Dispositivo Gerenciado Antes de Iniciar o Diagnóstico Remoto	Assegura que o operador remoto solicite permissão do usuário no dispositivo gerenciado antes de iniciar uma sessão de Diagnóstico Remoto.
Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado Durante o Diagnóstico Remoto	Exibe um sinal visível no canto superior direito da área de trabalho do dispositivo gerenciado durante a sessão de Diagnóstico Remoto. O sinal visível permite ao usuário do dispositivo gerenciado saber que uma sessão de Diagnóstico Remoto está em andamento.
Enviar Sinal Sonoro ao Usuário no Dispositivo Gerenciado a Cada [ ] Segundos Durante o Diagnóstico Remoto	Gera um sinal sonoro no dispositivo gerenciado durante a sessão de Diagnóstico Remoto. Esse sinal é gerado periodicamente após o número especificado de segundos.
Permitir que a Tela do Dispositivo Gerenciado Fique em Branco Durante o Diagnóstico Remoto	Permite que a tela do dispositivo gerenciado fique em branco durante uma sessão de Diagnóstico Remoto. O mouse e o teclado do dispositivo gerenciado ficam sempre bloqueados durante uma sessão de Diagnóstico Remoto. A seleção dessa opção também desabilita o sinal visível no dispositivo gerenciado.

Campo	Detalhes
Exibir mensagem de aviso antes da reinicialização durante [ ] segundos	Exibe uma mensagem de aviso no dispositivo gerenciado no início da sessão de Diagnóstico Remoto, lembrando o usuário de gravar todos os aplicativos existentes. Essa mensagem de aviso é exibida pelo período especificado para evitar que o usuário perca qualquer dado não gravado, já que o operador remoto poderá iniciar uma reinicialização do sistema durante a sessão de Diagnóstico Remoto.
Terminar Automaticamente a Sessão de Diagnóstico Remoto Após a Inatividade de [ ] Minutos	Encerra a sessão de Diagnóstico Remoto quando ela fica inativa pelo período especificado.

8 Clique em *Avançar* para exibir a página Configurações de Execução Remota. Para aceitar as configurações padrão, passe para a etapa seguinte ou use as informações especificadas na tabela a seguir para mudar as configurações padrão.

Campo	Detalhes
Permitir que programas sejam executados remotamente no dispositivo gerenciado	Permite que programas sejam executados remotamente no dispositivo gerenciado. A seleção desta opção habilita as opções subseqüentes na página. Ao anular a seleção da opção, você desabilita a operação de Execução Remota no dispositivo.
Solicitar Permissão ao Usuário no Dispositivo Gerenciado Antes da Execução Remota	Assegura que o operador remoto solicite permissão do usuário no dispositivo gerenciado antes de iniciar uma sessão de Execução Remota.
Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado Durante a Execução Remota	Exibe um sinal visível no canto superior direito da área de trabalho do dispositivo gerenciado durante a sessão de Execução Remota. O sinal visível permite que o usuário no dispositivo gerenciado saiba que uma sessão de Execução Remota está em andamento.
Terminar Automaticamente a Sessão de Diagnóstico Remoto Após a Inatividade de [ ] Minutos	Encerra a sessão de Execução Remota quando ela fica inativa pelo período especificado.

9 Clique em *Avançar* para exibir a página Configurações de Transferência de Arquivos. Para aceitar as configurações padrão, passe para a próxima etapa ou use as informações especificadas na tabela a seguir para mudar as configurações de segurança padrão.

Campo	Detalhes
Permitir Transferência de Arquivos no Dispositivo Gerenciado	Habilita a transferência de arquivos entre o console de gerenciamento e o dispositivo gerenciado. A seleção desta opção habilita as opções subseqüentes na página. Ao anular a seleção da opção, você desabilita a operação de Transferência de Arquivos no dispositivo.
Solicitar Permissão ao Usuário do Dispositivo Gerenciado Antes de Iniciar a Transferência de Arquivos	Assegura que o operador remoto solicite permissão do usuário do dispositivo gerenciado antes de iniciar uma sessão de Transferência de Arquivos.

Campo	Detalhes
Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado Durante a Transferência de Arquivos	Exibe um sinal visível no canto superior direito da área de trabalho do dispositivo gerenciado durante a sessão de Transferência de Arquivos. O sinal visível permite que o usuário no dispositivo gerenciado saiba que uma sessão de Transferência de Arquivos está em andamento.
Permitir que o Download de Arquivos Seja Feito no Dispositivo Gerenciado	Permite que um operador remoto abra arquivos no dispositivo gerenciado e os transfira para o console de gerenciamento. Se essa opção não for selecionada, o Operador Remoto poderá somente transferir arquivos do console de gerenciamento para o dispositivo remoto.
Diretório Raiz da Transferência de Arquivos	Especifique o diretório do dispositivo gerenciado a ser visto pelo Operador Remoto durante uma sessão de Transferência de Arquivos. O operador remoto só pode transferir arquivos de e para esse diretório e seus subdiretórios. O diretório padrão é Meu Computador, ou seja, o operador remoto pode ver e transferir arquivos do todo o sistema de arquivos do dispositivo remoto.

10 Clique em *Avançar* para exibir a página Configurações de Segurança. Para aceitar as configurações padrão, passe para a próxima etapa ou use as informações especificadas na tabela a seguir para mudar as configurações de segurança padrão.

Autenticação de senha

Campo	Detalhes
Habilitar Autenticação Baseada em Senha	Permite que o operador remoto use uma senha para a autenticação no dispositivo gerenciado. Selecione essa opção para definir as configurações de tipo de senha.
Tamanho Mínimo da Senha	Permite especificar o tamanho mínimo da senha. Por padrão, são usados 6 caracteres.
Senha da Sessão	Selecione essa opção para solicitar que o usuário no dispositivo gerenciado defina uma senha antes do início de uma nova sessão remota. Essa opção é recomendada porque a senha não é armazenada no dispositivo gerenciado e é válida somente na sessão atual.
Senha Persistente	Selecione esta opção para definir as senhas do ZENworks e do VNC. É recomendável definir a Senha do ZENworks por ela ser mais segura do que a Senha do VNC. Essa senha pode ser definida pelo administrador através da política de Gerenciamento Remoto ou pelo usuário do dispositivo remoto através do ícone do ZENworks. A seleção dessa opção habilita as opções subseqüentes. Para que o usuário possa definir a senha pelo ícone do ZENworks, selecione a opção *Permitir que o usuário substitua as senhas padrão no dispositivo gerenciado*.

Campo	Detalhes
Senha do ZENworks	Para limpar a senha do ZENworks: 1. Clique em *Limpar Senha*. 2. Clique em *Aplicar* e, em seguida, clique em *OK*. Para definir a senha do ZENworks: 1. Clique em *Definir Senha*. 2. Digite a senha. O comprimento máximo da senha do é de 255 caracteres. 3. Clique em *Aplicar* e, em seguida, clique em *OK*.
Senha do VNC	Para limpar a senha do VNC: 1. Clique em *Limpar Senha*. 2. Clique em *Aplicar* e, em seguida, clique em *OK*. Para definir a senha do VNC: 1. Clique em *Definir Senha*. 2. Digite a senha. O comprimento máximo da senha do é de 8 caracteres. 3. Clique em *Aplicar* e, em seguida, clique em *OK*.

Detecção de Intrusão

Campo	Detalhes
Habilitar Detecção de Intrusos	Selecione essa opção para permitir a detecção de tentativas inválidas ou não autorizadas para iniciar uma sessão remota no dispositivo gerenciado. A seleção dessa opção habilita as opções subseqüentes na seção Detecção de Intrusão.
Suspender a Aceitação de Conexões Após [ ] Tentativas Sucessivas Inválidas	Especifica o número máximo de tentativas inválidas sucessivas que um Operador Remoto pode fazer antes que o serviço de Gerenciamento Remoto no dispositivo gerenciado seja bloqueado. Por padrão, são permitidas cinco tentativas.
Iniciar Automaticamente a Aceitação de Conexões Após [ ] Minutos	Especifica o tempo, em minutos, após o qual o Agente de Gerenciamento Remoto aceitará automaticamente uma conexão com o dispositivo gerenciado. Para desbloquear manualmente o serviço de Gerenciamento Remoto, clique duas vezes no ícone do ZENworks Adaptive Agent, clique em *Configurações de Segurança*, em seguida, em *Habilitar a aceitação de conexões se bloqueadas devido à detecção de intrusão*. O padrão é 10 minutos.

Segurança da Sessão

Campo	Detalhes
Habilitar Criptografia da Sessão	Habilita criptografia da sessão usando criptografia SSL (protocolo TLSvl) A seleção dessa opção habilita as opções subseqüentes na sessão Segurança da Sessão.

Campo	Detalhes
Permitir Conexão Quando o Console de Gerenciamento Remoto Não Tiver Certificado SSL	Quando uma sessão remota é iniciada no ZENworks Control Center, um certificado é gerado automaticamente para um operador remoto. Esse certificado é usado durante a autenticação. Selecione essa opção para permitir conexões de um console de Gerenciamento Remoto iniciado fora do ZENworks Control Center que talvez não tenha um certificado SSL.
Permitir até [ ] níveis na cadeia de certificado do Viewer	Os esquemas de autenticação com base em direitos e senhas da Novell são reproduzidos sobre uma canal criptografado SSL. O estabelecimento desse canal requer que o viewer apresente um certificado. Esse certificado pode ser assinado por uma autoridade de certificação raiz ou intermediária, criando uma cadeia de certificados. Essa propriedade define o número máximo de níveis permitidos na cadeia de certificados do viewer. Quando a autoridade de certificação interna do ZENworks é aplicada (instalada, por padrão), uma cadeia de certificados do viewer de dois níveis é automaticamente criada enquanto uma sessão remota do ZENworks Control Center é iniciada.

Abend

Campo	Detalhes
Bloquear Dispositivo	Bloqueia o dispositivo gerenciado quando a sessão remota é encerrada de forma anormal.
Logoff de Usuário	Efetua logoff do usuário no dispositivo gerenciado quando a sessão remota é encerrada de forma anormal.

11 Clique em *Avançar* para exibir a página Resumo.

12 Clique em *Concluir* para criar a política agora ou selecione *Definir Propriedades Adicionais* para especificar informações adicionais, como designação, uso obrigatório e status da política e de qual grupo a política será membro.

2.4 Configurando os direitos do operador remoto

Você pode atribuir direitos para um Operador Remoto executar sessões remotas no dispositivo gerenciado. O Operador Remoto pode ter direitos específicos de dispositivo, assim como direitos específicos de usuário.

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

2 No painel Administradores, clique no nome do administrador para quem deseja designar os direitos Gerenciamento Remoto.

3 No painel Direitos Designados, clique em *Adicionar*e, em seguida, clique em *Direito Gerenciamento Remoto* para exibir a caixa de diálogo Direito Gerenciamento Remoto.

4 Selecione o dispositivo ou o usuário para designar os direitos.

A tabela a seguir contém informações sobre os direitos Gerenciamento Remoto:

Direito Gerenciamento Remoto	Detalhes
Controle Remoto	Designe os direitos ao operador remoto para controlar remotamente os dispositivos
Tela Remota	Designe os direitos ao operador remoto para visualizar remotamente os dispositivos
Diagnóstico Remoto	Designe os direitos ao operador remoto para diagnosticar remotamente os dispositivos.
Execução Remota	Designe os direitos ao operador remoto para executar aplicativos remotamente nos dispositivos.
Transferir Arquivos	Atribui ao operador remoto direitos de transferir arquivos para ou de dispositivos.
Desbloquear o Serviço de Gerenciamento Remoto	Atribui ao operador remoto direitos de desbloquear o serviço de Gerenciamento Remoto que foi bloqueado por uma detecção de intrusão.

Observação: Os direitos Gerenciamento Remoto são aplicáveis apenas à autenticação baseada em direitos. Contudo, mediante a permissão da política de Gerenciamento Remoto, o operador remoto pode executar a operação de Gerenciamento Remoto usando a autenticação baseada em senha.

5 Clique em *OK*.

2.5 Configurando a senha de gerenciamento remoto

As seções a seguir fornecem informações sobre a configuração da senha de Gerenciamento Remoto para o serviço de Gerenciamento Remoto no dispositivo gerenciado:

- Seção 2.5.1, “Configurando a senha de gerenciamento remoto usando o ZENworks Control Center” na página 31
- Seção 2.5.2, “Configurando a senha de gerenciamento remoto usando o ZENworks Adaptive Agent” na página 32
- Seção 2.5.3, “Limpando a senha de gerenciamento remoto usando o ZENworks Control Center” na página 33
- Seção 2.5.4, “Limpando a senha de gerenciamento remoto usando o ZENworks Adaptive Agent” na página 33

2.5.1 Configurando a senha de gerenciamento remoto usando o ZENworks Control Center

O Administrador pode definir uma senha de Gerenciamento Remoto na página Configurações de Segurança durante ou após a criação de uma política de Gerenciamento Remoto.

Se você deseja definir a senha durante a criação da política de Gerenciamento Remoto, consulte a Seção 2.3, "Criando a política de gerenciamento remoto" na página 23.

Para editar a definição de senha na política de Gerenciamento Remoto:

1. No ZENworks Control Center, clique em *Políticas*.
2. Clique na política de Gerenciamento Remoto e, em seguida, na guia *Configurações*.
3. No painel Configurações de Segurança, selecione a senha e substitua-a pela nova.
4. Clique em *Aplicar*.
5. Incremente a versão desta política na página Resumo ou nas Tarefas Comuns para atualizar as mudanças de senha no dispositivo gerenciado.

Para definir a senha após a criação da política de Gerenciamento Remoto:

1. No ZENworks Control Center, clique em *Políticas*.
2. Clique na política de Gerenciamento Remoto e, em seguida, na guia *Configurações*.
3. No painel Configurações de Segurança, selecione *Habilitar Autenticação Baseada em Senha* e selecione *Persistente*.
4. Clique em *Definir Senha* e especifique a senha. Se você já tiver definido a senha durante a criação da política de Gerenciamento Remoto, poderá editá-la. Para editar a senha, selecione-a e substitua-a pela nova.
5. Clique em *Aplicar*
6. Incremente a versão desta política na página Resumo ou nas Tarefas Comuns para atualizar as mudanças de senha no dispositivo gerenciado.

2.5.2 Configurando a senha de gerenciamento remoto usando o ZENworks Adaptive Agent

O usuário no dispositivo gerenciado pode definir uma senha para o serviço de Gerenciamento Remoto se a opção *Permitir que o usuário substitua as senhas padrão no dispositivo gerenciado* estiver habilitada na política de Gerenciamento Remoto efetiva no dispositivo gerenciado. Essa senha tem precedência sobre a senha definida na política de Gerenciamento Remoto.

Para definir uma senha no dispositivo gerenciado:

1. Clique duas vezes no ícone *ZENworks Adaptive Agent* para exibir a janela do ZENworks Adaptive Agent.
2. No painel esquerdo, navegue para *Gerenciamento Remoto* e, em seguida, clique em *Segurança*.
3. No painel direito, clique em *Definir Senha* para definir as seguintes senhas:
   - **Senha do ZENworks (recomendada):** usada na autenticação do ZENworks. Ela pode ter até 255 caracteres.
   - **Senha VNC:** usada na autenticação do VNC para interoperabilidade com viewers de VNC de fonte aberta. Ela pode ter até 8 caracteres.
4. Clique em *OK*.

2.5.3 Limpando a senha de gerenciamento remoto usando o ZENworks Control Center

Para limpar a senha de Gerenciamento Remoto definida usando a política:

1. No ZENworks Control Center, clique em *Políticas*.
2. Clique na política de Gerenciamento Remoto e, em seguida, na guia *Configurações*.
3. No painel Configurações de Segurança, selecione *Limpar Senha* e clique em *Aplicar*.
4. Incremente a versão dessa política na página de Resumo ou em Tarefas Comuns para atualizar as mudanças na política no dispositivo gerenciado.

Para limpar a senha de Gerenciamento Remoto definida pelo usuário do dispositivo gerenciado:

1. No ZENworks Control Center, clique em *Políticas*.
2. Clique na política de Gerenciamento Remoto e, em seguida, na guia *Configurações*.
3. No painel Configurações de Segurança, anule a seleção da opção *Permitir que o Usuário Substitua as Senhas Padrão no Dispositivo Gerenciado* e clique em *Aplicar*.
4. Incremente a versão dessa política na página de Resumo ou em Tarefas Comuns para atualizar as mudanças na política no dispositivo gerenciado.

2.5.4 Limpando a senha de gerenciamento remoto usando o ZENworks Adaptive Agent

O usuário do dispositivo gerenciado pode redefinir a senha do Gerenciamento Remoto definida anteriormente.

1. Clique duas vezes no ícone *ZENworks Adaptive Agent* para exibir a janela do ZENworks Adaptive Agent.
2. No painel esquerdo, navegue para *Gerenciamento Remoto* e, em seguida, clique em *Segurança*.
3. No painel direito, clique em *Limpar Senha* para limpar as senhas.
4. Clique em *OK*.

A senha configurada na política será efetiva, pois nenhuma senha foi definida pelo usuário.

2.6 Instalando o viewer de gerenciamento remoto

O Viewer de Gerenciamento Remoto é um aplicativo do console de gerenciamento que permite ao operador remoto realizar operações remotas no dispositivo gerenciado. Permite que o operador remoto veja a área de trabalho do dispositivo gerenciado, transfira arquivos e execute aplicativos no dispositivo gerenciado.

Para instalar o Viewer de Gerenciamento Remoto, clique no link *Instalar Viewer de Gerenciamento Remoto* que é exibida no ZENworks Control Center quando você está realizando uma operação de gerenciamento remoto no dispositivo gerenciado. Esse link será exibido apenas se você estiver realizando uma operação de gerenciamento remoto no dispositivo pela primeira vez e se o viewer ainda não estiver instalado no dispositivo.

Se já houver uma versão anterior do Viewer de Gerenciamento Remoto instalada no dispositivo, o link *Atualizar Viewer de Gerenciamento Remoto* será exibido. Clique nesse link para fazer upgrade da versão do viewer instalado no dispositivo.

Observação: A instalação do Viewer de Gerenciamento Remoto em um SUSE® Linux Enterprise Server 11 (SLES 11) ou SUSE Linux Enterprise Desktop 11 (SLED 11) requer o pacote dependente glitz. Você deve instalar o pacote glitz apropriado pelo site do openSUSE® na Web (http://software.opensuse.org/112/en).

No Windows:

1. No ZENworks Control Center, clique em *Configuração*.
2. No painel de navegação esquerdo, clique em *Fazer Download das Ferramentas do ZENworks*.
3. No painel de navegação esquerdo da página de Download do ZENworks, clique em *Ferramentas Administrativas*.
4. Clique em `novell-zenworks-rm-viewer-<versão>.msi`.
5. (Condicional) Se você tiver iniciado o ZENworks Control Center usando o Internet Explorer*, siga um destes procedimentos:
   - Clique em *Executar* para instalar o viewer.
   - Clique em *Salvar* para gravar o arquivo em um local temporário. Clique duas vezes no arquivo para instalar o viewer.
6. (Condicional) Se você tiver iniciado o ZENworks Control Center usando o Firefox, clique em *Gravar Arquivo* para gravar o arquivo em uma localização temporária e clique duas vezes no arquivo para instalar o viewer.

No Linux:

1. No ZENworks Control Center, clique em *Configuração*.
2. No painel de navegação esquerdo, clique em *Fazer Download das Ferramentas do ZENworks*.
3. No painel de navegação esquerdo da página de Download do ZENworks, clique em *Ferramentas Administrativas*.
4. Clique em `novell-zenworks-rm-viewer-<versão>.noarch.rpm`.
5. Decida se quer instalar o viewer imediatamente ou gravar o arquivo RPM do viewer para instalá-lo mais tarde.
   - Para instalar o viewer imediatamente, clique em *Abrir com* para abrir o Viewer de Gerenciamento Remoto com o zen-installer, especifique a senha de root e depois clique em *OK*.
   - Para gravar o arquivo RPM do viewer no diretório de download padrão, para que seja possível instalá-lo depois, clique em *Gravar em Disco*. Para instalar o RPM, siga um destes procedimentos:
     - Clique no arquivo RPM do viewer, especifique a senha de root e clique em *OK*.
     - Execute o seguinte comando como superusuário ou usuário root:

       ```
       rpm -ivh novell-zenworks-rm-viewer-<versão>.noarch.rpm
       ```

2.7 Fazendo upgrade do viewer de gerenciamento remoto

Se você estiver realizando uma operação de gerenciamento remoto em um dispositivo gerenciado Windows no qual já exista uma versão anterior do Viewer de Gerenciamento Remoto, o link *Atualizar Viewer de Gerenciamento Remoto* será exibido no ZENworks Control Center. Clique nesse link para fazer upgrade da versão do viewer instalado no dispositivo.

Para fazer upgrade do viewer de Gerenciamento Remoto em um dispositivo Linux a partir do Novell ZENworks 10 Configuration Management SP2 (10.2) para o Novell ZENworks 10 Configuration Management SP3 (10.3) ou posterior, execute o comando a seguir como superusuário ou usuário root:

```
rpm -Uvh --nopostun novell-zenworks-rm-viewer-<version>.noarch.rpm
```

Se desejar, desinstale a versão antiga `novell-zenworks-rm-viewer-10.x.x.rpm` e instale a nova. Para obter mais informações sobre a instalação do viewer, consulte a Seção 2.6, “Instalando o viewer de gerenciamento remoto” na página 33.

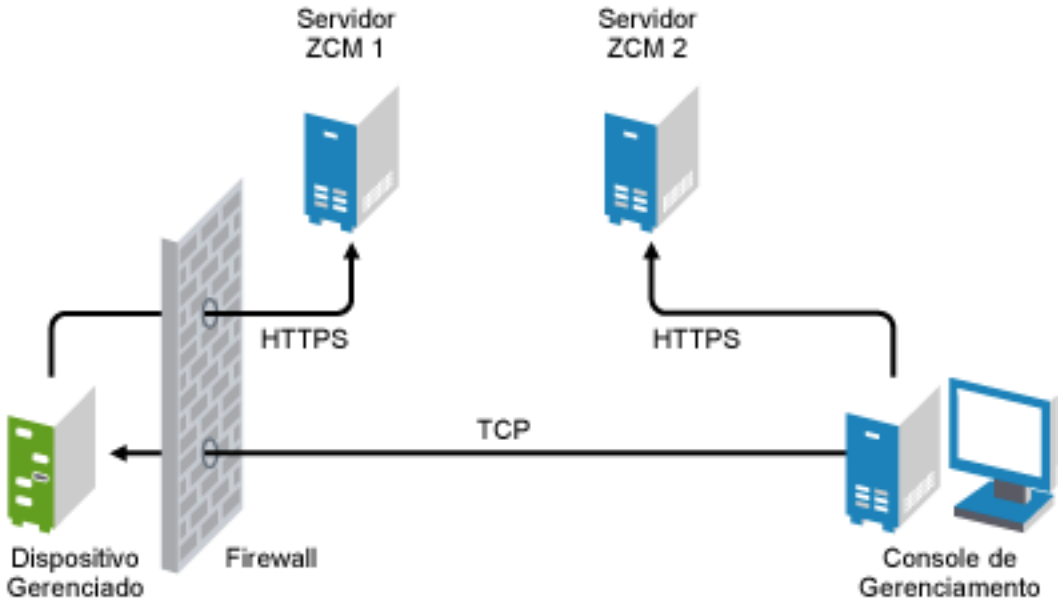
2.8 Iniciando as operações de gerenciamento remoto

A operação remota pode ser iniciada das seguintes maneiras:

2.8.1 Iniciando uma sessão pelo console de gerenciamento

Neste cenário, a sessão remota é iniciada pelo administrador no console de gerenciamento. O console de gerenciamento geralmente é colocado em uma rede corporativa e o dispositivo gerenciado pode estar dentro ou fora dessa rede. A ilustração a seguir mostra uma sessão remota iniciada no dispositivo gerenciado a partir do console de gerenciamento.

Figura 2-1 *Sessão iniciada no console*



O Agente de Gerenciamento Remoto se inicia automaticamente quando o dispositivo gerenciado é inicializado. Uma política de Gerenciamento Remoto é criada no dispositivo gerenciado quando o dispositivo é implantado. Você pode gerenciar remotamente o dispositivo usando esta política padrão somente no modo de autenticação baseada em direitos. Se você criar uma nova política de Gerenciamento Remoto, ela anulará a política padrão.

Se a configuração da Zona de Gerenciamento do ZENworks estiver distribuída por duas ou mais redes privadas habilitadas para NAT que estejam interconectadas por uma rede pública, implante o DNS_ALG nos gateways dessas redes privadas. O DNS_ALG garante que as consultas de pesquisa DNS iniciadas pelos componentes do ZENworks retornem o nome de host correto mapeado para o endereço privado e permite a comunicação entre o console de gerenciamento e os dispositivos gerenciados. Para obter mais informações sobre o DNS_ALG, consulte o RFC - 2694 do DNS ALG (http://www.ietf.org/rfc/rfc2694).

Se você deseja gerenciar remotamente um dispositivo usando seu nome DNS, verifique se o serviço DNS Dinâmico foi implantado na rede.

O operador remoto pode iniciar uma sessão de uma das seguintes formas:

- “Iniciando uma operação de Gerenciamento Remoto no ZENworks Control Center” na página 37
- “Iniciando uma operação de Gerenciamento Remoto no modo independente” na página 43
- “Iniciando uma operação de Gerenciamento Remoto usando as opções de linha de comando” na página 43

Iniciando uma operação de Gerenciamento Remoto no ZENworks Control Center

Você pode iniciar as várias operações de Gerenciamento Remoto do contexto de dispositivo ou do contexto de usuário:

- “Iniciando a sessão de Gerenciamento Remoto no contexto do dispositivo” na página 37
- “Iniciando uma sessão de Gerenciamento Remoto a partir do contexto do usuário” na página 40

Iniciando a sessão de Gerenciamento Remoto no contexto do dispositivo

Para iniciar uma sessão de Gerenciamento Remoto em um dispositivo

1. No ZENworks Control Center, clique na guia *Dispositivos*.
2. Clique em *Servidores* ou *Estações de Trabalho* e selecione o dispositivo que deseja gerenciar remotamente. Clique em *Ação* e, em seguida, selecione a operação de Gerenciamento Remoto que deseja realizar.

   ou

   Em *Tarefas do Dispositivo* no painel esquerdo, selecione a operação de Gerenciamento Remoto que deseja realizar.

   As operações de gerenciamento remoto disponíveis são:

   - **Controle Remoto:** exibe a caixa de diálogo Gerenciamento Remoto, que possibilita a realização de uma operação do Controle Remoto, Tela Remota ou Execução Remota no dispositivo gerenciado.
   - **Diagnóstico Remoto:** exibe a caixa de diálogo Diagnóstico Remoto, que possibilita a realização de uma operação de Diagnóstico Remoto no dispositivo gerenciado.
   - **Transferir Arquivos:** exibe a caixa de diálogo Transferência de Arquivos, que possibilita a realização de uma operação de transferência de arquivos no dispositivo gerenciado.
3. Preencha as opções na caixa de diálogo exibida. A tabela a seguir contém informações sobre as várias opções disponíveis:

Campo	Detalhes
Dispositivo	Especifique o nome de host ou o endereço IP do dispositivo que você deseja gerenciar remotamente.
Operação	Selecione o tipo da operação remota que você deseja realizar no dispositivo gerenciado. Essa opção está disponível apenas na caixa de diálogo Gerenciamento Remoto.
Aplicativo	Selecione o aplicativo a ser iniciado no dispositivo para diagnosticar remotamente. Essa opção está disponível apenas na caixa de diálogo Diagnóstico Remoto.
Autenticação	Selecione o modo que você deseja usar para se autenticar no dispositivo gerenciado. Os modos de autenticação são: ◆ Autenticação baseada em direitos ◆ Autenticação baseada em senha
Porta	Especifique o número da porta em que o 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. Este modo é selecionado por padrão para a operação de Controle Remoto. Se você iniciar a sessão de Controle Remoto no dispositivo gerenciado primeiro, obterá os privilégios de um operador remoto master, entre os quais: ◆ Convidar outros operadores remotos para ingressar na sessão remota. ◆ Delegar direitos Controle Remoto a um operador remoto. ◆ Obter novamente o controle do operador remoto. ◆ Encerrar uma sessão remota. As sessões consecutivas iniciadas nas sessões de Tela Remota. **Observação:** O modo de colaboração ainda não é suportado no Linux. ◆ **Compartilhada:** permite que mais de um operador remoto controle simultaneamente o dispositivo gerenciado. ◆ **Exclusivo:** permite que haja uma sessão remota exclusiva no dispositivo gerenciado. Nenhuma outra sessão remota poderá ser iniciada no dispositivo remoto após uma sessão ter sido iniciada no modo exclusivo. Este modo é selecionado por padrão para a operação de Tela Remota. Essa opção está disponível apenas na caixa de diálogo Gerenciamento Remoto.
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 para operações de Controle Remoto, Tela Remota e Diagnóstico Remoto. Esta opção atualmente é suportada apenas pelo Windows.

Campo	Detalhes
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 para operações de Controle Remoto, Tela Remota e Diagnóstico Remoto.
Habilitar Registro	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 ZCC (ZENworks Control Center) através do Internet Explorer, e no diretório de instalação do mozilla, se você iniciar o ZCC através do Mozilla* FireFox*.
Rotear por Proxy	Habilita o roteamento da operação de gerenciamento remoto do dispositivo gerenciado por meio de um proxy de gerenciamento remoto. Se o dispositivo gerenciado estiver em uma rede privada ou protegido por um firewall ou roteador que use NAT, a operação de gerenciamento remoto do dispositivo poderá ser roteada por meio de um proxy de gerenciamento remoto. Esta opção atualmente é suportada apenas pelo Windows. Preencha os campos a seguir: **Proxy:** especifique o nome DNS ou o endereço IP do proxy de gerenciamento remoto. Por padrão, o proxy definido no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um proxy diferente. **Porta do Proxy:** especifique o número da porta em que o proxy de gerenciamento remoto está escutando. Por padrão, a porta é 5750. **Observação:** A Auditoria do Gerenciamento Remoto exibe o Endereço IP do dispositivo executando o proxy de gerenciamento remoto, e não o endereço IP do console de gerenciamento.
Use o Seguinte Par de Chave para Identificação	Se uma autoridade de certificação (CA) interna foi 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, PEM e PFX. Se o formato PFX for usado, tanto a chave quanto o certificado deverão estar disponíveis no mesmo arquivo. Forneça este arquivo como entrada para a chave e o certificado. **Habilitar Caminho de Cache:** habilita o armazenamento em cache dos caminhos da chave primária e do certificado no console de gerenciamento. Essa opção é suportada apenas pelo Windows.

4 Clique em *OK* para iniciar a operação remota selecionada.

Iniciando uma sessão de Gerenciamento Remoto a partir do contexto do usuário

Se quiser oferecer assistência a um usuário realizando uma sessão remota no dispositivo gerenciado onde ele se conectou:

1. No ZENworks Control Center, clique na guia *Usuários*.
2. Clique na *Origem de Usuário*.
3. Selecione o usuário para gerenciar remotamente o dispositivo onde ele está conectado.
4. Clique em *Ação* e, em seguida, selecione a operação de Gerenciamento Remoto que deseja realizar.

   As operações disponíveis são:

   - **Controle Remoto:** exibe a caixa de diálogo Gerenciamento Remoto, que possibilita a realização de uma operação do Controle Remoto, Tela Remota ou Execução Remota no dispositivo gerenciado.
   - **Diagnóstico Remoto:** exibe a caixa de diálogo Diagnóstico Remoto, que possibilita a realização de uma operação de Diagnóstico Remoto no dispositivo gerenciado.
   - **Transferir Arquivos:** exibe a caixa de diálogo Transferência de Arquivos, que possibilita a realização de uma operação de transferência de arquivos no dispositivo gerenciado.
5. Preencha as opções na caixa de diálogo exibida. A tabela a seguir contém informações sobre as várias opções disponíveis:

Campo	Detalhes
Dispositivo	Especifique o nome de host ou o endereço IP do dispositivo que você deseja gerenciar remotamente.
Operação	Selecione o tipo da operação remota que você deseja realizar no dispositivo gerenciado. Essa opção está disponível apenas na caixa de diálogo Gerenciamento Remoto.
Aplicativo	Selecione o aplicativo a ser iniciado no dispositivo para diagnosticar remotamente. Essa opção está disponível apenas na caixa de diálogo Diagnóstico Remoto.
Autenticação	Selecione o modo que você deseja usar para se autenticar no dispositivo gerenciado. Os modos de autenticação são: ◆ Autenticação baseada em direitos ◆ Autenticação baseada em senha
Porta	Especifique o número da porta em que o 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. Este modo é selecionado por padrão para a operação de Controle Remoto. Se você iniciar a sessão de Controle Remoto no dispositivo gerenciado primeiro, obterá os privilégios de um operador remoto master, entre os quais: ◆ Convidar outros operadores remotos para ingressar na sessão remota. ◆ Delegar direitos Controle Remoto a um operador remoto. ◆ Obter novamente o controle do operador remoto. ◆ Encerrar uma sessão remota. As sessões consecutivas iniciadas nas sessões de Tela Remota. **Observação:** O modo de colaboração ainda não é suportado no Linux. ◆ **Compartilhada:** permite que mais de um operador remoto controle simultaneamente o dispositivo gerenciado. ◆ **Exclusivo:** permite que haja uma sessão remota exclusiva no dispositivo gerenciado. Nenhuma outra sessão remota poderá ser iniciada no dispositivo remoto após uma sessão ter sido iniciada no modo exclusivo. Este modo é selecionado por padrão para a operação de Tela Remota. Essa opção está disponível apenas na caixa de diálogo Gerenciamento Remoto.
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 para operações de Controle Remoto, Tela Remota e Diagnóstico Remoto. Esta opção atualmente é suportada apenas pelo Windows.

Campo	Detalhes
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 para operações de Controle Remoto, Tela Remota e Diagnóstico Remoto.
Habilitar Registro	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 ZCC (ZENworks Control Center) através do Internet Explorer, e no diretório de instalação do mozilla, se você iniciar o ZCC através do Mozilla* FireFox*.
Rotear por Proxy	Habilita o roteamento da operação de gerenciamento remoto do dispositivo gerenciado por meio de um proxy de gerenciamento remoto. Se o dispositivo gerenciado estiver em uma rede privada ou protegido por um firewall ou roteador que use NAT, a operação de gerenciamento remoto do dispositivo poderá ser roteada por meio de um proxy de gerenciamento remoto. Esta opção atualmente é suportada apenas pelo Windows. Preencha os campos a seguir: **Proxy:** especifique o nome DNS ou o endereço IP do proxy de gerenciamento remoto. Por padrão, o proxy definido no painel Configurações de Proxy para executar a operação remota no dispositivo é preenchido nesse campo. Você pode especificar um proxy diferente. **Porta do Proxy:** especifique o número da porta em que o proxy de gerenciamento remoto está escutando. Por padrão, a porta é 5750. **Observação:** A Auditoria do Gerenciamento Remoto exibe o Endereço IP do dispositivo executando o proxy de gerenciamento remoto, e não o endereço IP do console de gerenciamento.
Use o Seguinte Par de Chave para Identificação	Se uma autoridade de certificação (CA) interna foi 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, PEM e PFX. Se o formato PFX for usado, tanto a chave quanto o certificado deverão estar disponíveis no mesmo arquivo. Forneça este arquivo como entrada para a chave e o certificado. **Habilitar Caminho de Cache:** habilita o armazenamento em cache dos caminhos da chave primária e do certificado no console de gerenciamento. Essa opção é suportada apenas pelo Windows.

6 Clique em *OK* para iniciar a operação remota selecionada.

Iniciando uma operação de Gerenciamento Remoto no modo independente

Antes de iniciar a operação de gerenciamento remoto no modo independente, instale o viewer de Gerenciamento Remoto. Para obter mais informações sobre como instalar o viewer, consulte a Seção 2.6, “Instalando o viewer de gerenciamento remoto” na página 33.

Para iniciar a operação de Gerenciamento Remoto no modo independente:

1. Clique duas vezes no arquivo `nzrViewer.exe` para iniciar o Cliente de Gerenciamento Remoto do ZENworks.
2. Na janela Conexão de Gerenciamento Remoto do ZENworks exibida, especifique o nome DNS ou o endereço IP do dispositivo gerenciado e o número da porta no formato *Endereço IP~~Porta*. Por exemplo, 10.0.0.0~~1000.
3. Especifique o nome DNS ou o endereço IP do proxy de gerenciamento remoto e o número da porta em um dos formatos a seguir:
   - *Endereço IP~~Porta*. Por exemplo, 10.0.0.0~~5750.
   - *Endereço IP~Porta*. Por exemplo, 10.0.0.0~50.
4. Clique em *Conectar*.

   Se a autenticação for bem-sucedida, a sessão remota será iniciada. Por padrão, uma sessão de Controle Remoto é iniciada.

Iniciando uma operação de Gerenciamento Remoto usando as opções de linha de comando

Antes de iniciar a operação de Gerenciamento Remoto por linha de comando, instale o viewer de Gerenciamento Remoto. Para obter mais informações sobre como instalar o viewer, consulte a Seção 2.6, “Instalando o viewer de gerenciamento remoto” na página 33.

Para iniciar a operação de Gerenciamento Remoto usando as opções de linha de comando:

1. No prompt de comando, mude para o diretório em que o viewer está instalado. Por padrão, o viewer é instalado no diretório `<Pasta_de_Dados_do_Aplicativo_de_Usuário>\Novell\ZENworks\Remote Management\bin`.
2. Execute o seguinte comando:

   `nzrViewer [/opções<parâmetros, se houver>][endereço IP do dispositivo gerenciado] [~~porta]`

   A porta padrão do dispositivo gerenciado é 5950.

   Para obter informações sobre as opções de linha de comando disponíveis, consulte a Seção 2.9.1, “Opções de linha de comando para iniciar uma operação remota” na página 46.
3. Clique em *Conectar*.

   Se a autenticação for bem-sucedida, a sessão remota será iniciada. Se você não especificou o tipo de operação remota na linha de comando, uma sessão de Controle Remoto será iniciada por padrão.

No entanto, iniciar a operação de Gerenciamento Remoto usando as opções de linha de comando implica as seguintes limitações:

- Se não quiser especificar as opções de linha de comando `key`, `cert` e `CAcert` no comando `nzrViewer` para autenticação SSL, verifique se a opção *Permitir conexão quando o Console de Gerenciamento Remoto não tiver certificado SSL* nas configurações de segurança da política de Gerenciamento Remoto está habilitada. Entretanto, essa ação não é recomendada, pois a segurança do dispositivo fica reduzida.
- Se o dispositivo gerenciado fizer parte da Zona de Gerenciamento, verifique se o certificado apresentado pelo viewer é válido, está assinado e encadeado à CA; caso contrário, haverá falha na autenticação.

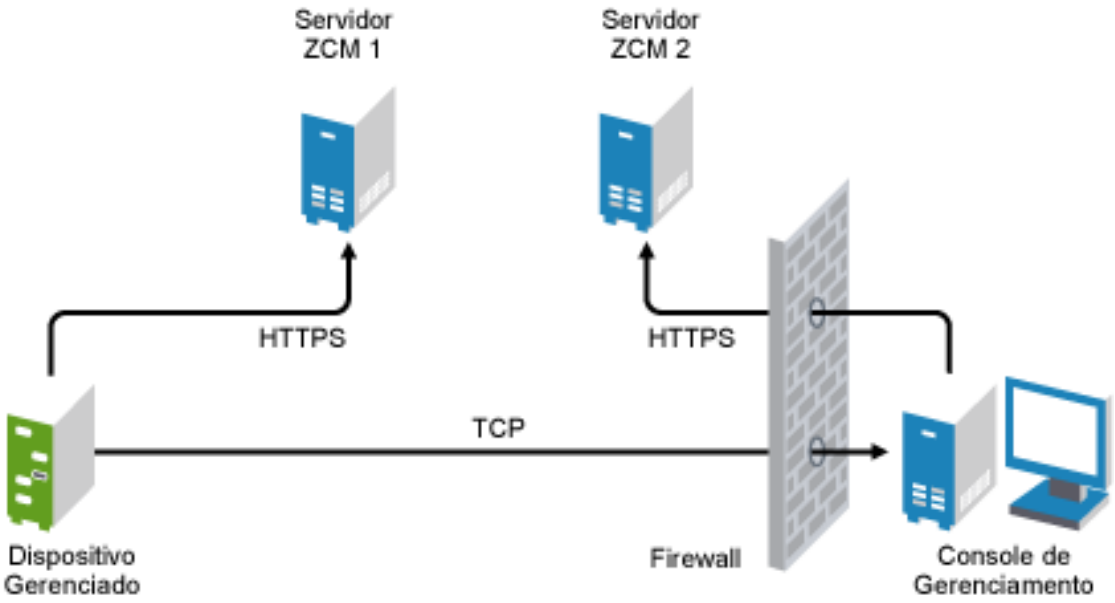
Observação: Quando você inicia uma sessão remota a partir do ZENworks Control Center (ZCC), o certificado é automaticamente gerado pelo ZCC e encaminhado ao viewer para que ele inicie a sessão. A validade do certificado é de apenas quatro dias.

- O dispositivo gerenciado usa o certificado fornecido pelo viewer para identificar o operador remoto. Se o viewer não fornecer um certificado, o usuário não será identificado e será registrado como *desconhecido* na mensagem de permissão, no sinal visível e nos registros de auditoria.

2.8.2 Iniciando uma sessão pelo dispositivo gerenciado

Neste cenário, a sessão remota é iniciada pelo usuário no dispositivo gerenciado. Isso será útil caso o console de gerenciamento não consiga se conectar com o dispositivo gerenciado. A ilustração a seguir mostra uma sessão remota iniciada pelo usuário no dispositivo gerenciado.

Figura 2-2 *Sessão iniciada pelo agente*



O usuário no dispositivo remoto pode solicitar a um operador remoto que execute uma sessão remota no dispositivo se:

- O operador remoto tiver iniciado a escuta do Gerenciamento Remoto para solicitações de sessão remota do usuário.
- A opção *Permitir que o usuário solicite uma sessão remota* estiver habilitada na política de Gerenciamento Remoto.
- A porta em que o Gerenciamento Remoto faz a escuta de conexões remotas precisar estar aberta no firewall do console de gerenciamento. A porta padrão é 5550.

Para solicitar uma sessão:

1. Clique duas vezes no ícone do ZENworks, na área de notificação.
2. No painel esquerdo, navegue até *Gerenciamento Remoto* e clique em *Geral*.
3. Clique em *Solicitar Sessão de Gerenciamento Remoto* para exibir a caixa de diálogo Solicitar Sessão.

   A capacidade de solicitação de uma sessão de Gerenciamento Remoto é controlada pelo administrador, o que significa que a opção pode estar desabilitada, especialmente se sua empresa ou seu departamento não tiver uma equipe de suporte técnico dedicada para atuar como operadores remotos de plantão. Se a opção *Solicitar Sessão de Gerenciamento Remoto* não for exibida como texto vinculado, a opção estará desabilitada.
4. Na lista *Escutando Operadores Remotos*, selecione o operador remoto com o qual deseja abrir a sessão remota.

   ou

   Se o operador remoto não estiver listado, digite suas informações de conexão nos campos *Solicitar Conexão*.
5. No campo *Operação*, selecione o tipo de operação (Controle Remoto, Tela Remota, Diagnósticos Remotos, Transferência de Arquivos ou Execução Remota) que deseja abrir.

   Para obter informações sobre cada operação, consulte a Seção 1.2, “Compreendendo as operações de gerenciamento remoto” na página 12.
6. Clique em *Solicitar* para iniciar a sessão.

Se quiser permitir conexões feitas de uma rede pública para uma rede privada, distribua o DNS_ALG (DNS Application Level Gateway). Para obter mais informações sobre o DNS_ALG, consulte o RFC 2694 (http://www.ietf.org/rfc/rfc2694).

2.9 Opções para iniciar uma operação de gerenciamento remoto

Ao iniciar uma operação de gerenciamento remoto por linha de comando, você pode especificar as opções para controlar o comportamento da sessão remota. Por exemplo, especifique a opção `remotecontrol` para iniciar uma operação de Controle Remoto no dispositivo, e a opção `notoolbar` para ocultar a barra de ferramentas da janela de exibição.

O Gerenciamento Remoto usa determinadas opções internamente quando você inicia uma operação de gerenciamento remoto no dispositivo. Por exemplo, a opção `zenrights` especifica o esquema de autenticação como Autenticação de Direitos do ZENworks. Você não deve especificar essas opções

internas quando usar a linha de comando para iniciar uma operação de gerenciamento remoto no dispositivo. Para obter mais informações sobre as opções usadas internamente, consulte a Seção 2.9.2, “Opções internas para iniciar uma operação remota” na página 49.

Consulte as seções a seguir para obter mais informações sobre as opções de gerenciamento remoto:

2.9.1 Opções de linha de comando para iniciar uma operação remota

Use as seguintes opções de linha de comando para controlar uma operação remota:

Tabela 2-1 *Opções de linha de comando para iniciar uma operação remota*

Opção de linha de comando	Parâmetro	Descrição
listen	*port*	Permite a escuta de solicitações de sessão remota na porta especificada. Por padrão, a porta é 5550.
restricted		Oculta a barra de ferramentas e o menu do sistema.
viewonly		Inicia uma operação de Tela Remota no dispositivo gerenciado.
remotecontrol		Inicia uma operação de Controle Remoto no dispositivo gerenciado.
ftponly		Inicia uma operação de Transferência de Arquivo no dispositivo gerenciado.
remoteexecute		Inicia uma operação de Execução Remota no dispositivo gerenciado.
diagnostics	*nome_aplicativo*	Inicia uma operação de Diagnóstico Remoto no dispositivo gerenciado. Se o parâmetro nome_do_aplicativo for especificado, o aplicativo será iniciado no dispositivo gerenciado.
filecompressionlevel	*nível*	Fornece um meio de otimizar o processo de compactação de arquivos para aumentar a velocidade ou melhorar a compactação durante uma operação de transferência de arquivos. O nível de compactação pode variar de 0 a 9: ◆ 0 indica nenhuma compactação ◆ 1 indica melhor velocidade ◆ 9 indica melhor compactação Se o nível de compactação não for especificado, será usado o nível padrão 6, que é otimizado tanto para velocidade como para compactação.
noencrypt		Inicia a sessão remota em um modo não criptografado.
fullscreen		Inicia uma operação remota no modo de tela cheia no dispositivo gerenciado.

Opção de linha de comando	Parâmetro	Descrição
notoolbar		Oculta a barra de ferramentas da janela de exibição.
exclusive		Inicia a sessão remota em um modo exclusivo.
8bit		Especifica a profundidade de cores a ser usada para renderizar os dados da sessão.
shared		Habilita uma conexão compartilhada, permitindo que você compartilhe a área de trabalho com outros clientes que já estão fazendo uso dela. Por padrão, essa opção é Verdadeira.
collaborate		Inicia a sessão remota em um modo colaborativo. Essa opção ainda não é suportado no Linux.
noshared		Habilita uma conexão não compartilhada, que desconecta outros clientes conectados ou recusa sua conexão, dependendo da configuração do servidor.
swapmouse		Inverte os botões do mouse.
nocursor		Exibe apenas o ponteiro do mouse do dispositivo gerenciado. O ponteiro do mouse local não aparece.
dotcursor		Exibe o ponteiro do mouse local como um ponto. Por padrão, essa opção é Verdadeira.
smalldotcursor		Exibe o ponteiro do mouse local como um ponto pequeno.
normalcursor		Exibe o ponteiro do mouse local na forma padrão.
belldeiconify		Permite a transmissão de um caractere de campainha, causando um sinal sonoro no viewer. Esta opção também faz com que um vncviewer minimizado seja maximizado quando o caractere de campainha é recebido.
emulate3		Usuários com mouse de dois botões podem emular um botão do meio pressionando os dois ao mesmo tempo. Por padrão, essa opção é Verdadeira.
noemulate3		Não emula um mouse de três botões.
nojpeg		Desabilita a compactação de JPEG. Não é recomendado, pois pode reduzir a eficiência do codificador. Esta opção pode ser usada se for absolutamente necessário obter uma qualidade de imagem perfeita.
nocursorshape		Desabilita as atualizações de forma do cursor para tratar os movimentos do cursor remoto. Usar as atualizações de forma do cursor diminui os atrasos ao movimentar o cursor remoto e pode melhorar o uso da largura de banda de forma substancial.
noremotecursor		Não mostra o cursor remoto.
fitwindow		Oculta a barra de rolagem da janela de visualização.
scale	*porcentagem*	Amplia a janela de visualização para a porcentagem de expansão especificada.
emulate3timeout	*ms*	Especifica o tempo de espera para emular um mouse de três botões.

Opção de linha de comando	Parâmetro	Descrição
disableclipboard		Desabilita a cópia de dados para a área de transferência.
delay		Renderiza a área de exibição e aguarda o tempo especificado antes de recuperar a próxima atualização.
loglevel	*n*	Especifica os níveis de registro de informações.
console		Registra informações em uma janela do console.
logfile	*nome_do_arquivo*	Nome do arquivo de registro em que as informações devem ser registradas.
config	*nome_do_arquivo*	Nome do arquivo de configuração a ser usado para carregar configurações predefinidas.
key	*nome_do_arquivo*	Nome do arquivo em que a chave privada é armazenada. Essa chave é usada para estabelecer uma comunicação SSL com o dispositivo gerenciado. **Importante:** A chave e as opções de certificação devem ser usadas juntas. Se você usar essas opções junto com o comando `nzrViewer`, por motivos de segurança, deverá desabilitar a opção *Permitir conexão quando o Console de Gerenciamento Remoto não tiver certificado SSL* nas configurações de segurança da política de Gerenciamento Remoto.
cert	*nome_do_arquivo*	Nome do arquivo em que o certificado correspondente à chave privada é armazenado. **Importante:** A chave e as opções de certificação devem ser usadas juntas. Se você usar essas opções junto com o comando `nzrViewer` , por razões de segurança deverá desabilitar a opção *Permitir conexão quando o Console de Gerenciamento Remoto não tiver certificado SSL* nas configurações de segurança da política de Gerenciamento Remoto.
CAcert	*nome_do_arquivo*	Nome do arquivo em que o certificado raiz é armazenado. Esse certificado é usado para verificar o certificado do dispositivo gerenciado quando se estabelece uma comunicação SSL.
encoding	*nome_da_codificação*	Especifica a codificação desejada a ser usada na sessão. Os diferentes tipos de codificação são: Raw, CopyRect, RRE, CoRRE, Hextile, Zlib e Tight.
compresslevel	*n*	Especifica o nível de compactação a ser usado nos dados da sessão remota, de 0 a 9. O nível 1 usa o mínimo de tempo da CPU e obtém taxas de compactação baixas. O nível 9 oferece melhor compactação, mas é lento em termos de consumo de tempo da CPU no servidor. Use níveis altos em conexões de rede muito lentas e níveis baixos ao trabalhar em LANs de alta velocidade. Não recomendamos o uso da compactação de nível 0.

Opção de linha de comando	Parâmetro	Descrição
quality	*n*	Especifica o nível de qualidade de JPEG de 0 a 9. O nível 0 denota uma qualidade de imagem baixa, mas com taxas de compactação bem altas. O nível 9 oferece excelente qualidade de imagem a taxas de compactação mais baixas.
zenpasswd		Especifica que o esquema de autenticação a ser usado é a Autenticação de Senha do ZENworks.
locale		Especifica o idioma em que os recursos serão exibidos. Por padrão, é usado o inglês. Os valores para esta opção são: inglês, francês, alemão, espanhol, português, japonês, italiano, chinês (simplificado) e chinês (tradicional).
proxy	servidor_proxy	Especifica o nome DNS ou o endereço IP do proxy de gerenciamento remoto e o número da porta em um dos formatos a seguir: ◆ *Endereço IP~~Porta*. Por exemplo, 10.0.0.0~~5750. ◆ *Endereço IP~Porta*. Por exemplo, 10.0.0.0~50. A porta padrão do proxy é 5750.

2.9.2 Opções internas para iniciar uma operação remota

A tabela a seguir lista as opções que o Gerenciamento Remoto usa internamente. Essas opções não devem ser usadas quando você inicia uma operação de gerenciamento remoto por linha de comando.

Tabela 2-2 *Opções internas para iniciar uma operação remota*

Opção	Descrição
zenrights	Especifica a Autenticação de Direitos do ZENworks como o esquema de autenticação.
pipe	Especifica as informações de autenticação.

2.10 Instalando um proxy de gerenciamento remoto

Se o dispositivo gerenciado estiver em uma rede privada ou protegido por um firewall ou roteador que use NAT, a operação de gerenciamento remoto do dispositivo poderá ser roteada por meio de um proxy de gerenciamento remoto. É possível instalar o proxy em um dispositivo gerenciado Windows ou um dispositivo Linux (Servidor Principal ou Servidor Satélite). Por padrão, o proxy de gerenciamento remoto escuta na porta 5750.

Para obter mais informações sobre Proxy de Gerenciamento Remoto, consulte a Seção 1.4, “Entendendo o proxy de gerenciamento remoto” na página 16.

Para obter informações sobre os requisitos do sistema aos quais o dispositivo gerenciado Windows ou o dispositivo Linux deve atender para habilitar a instalação do proxy no dispositivo, consulte “Requisitos do sistema” no *Guia de Instalação do ZENworks 10 Configuration Management*.

Para instalar o proxy, execute as seguintes etapas:

No Windows:

1. No dispositivo, abra um browser da Web e vá para a página de download do ZENworks:

   https://*servidor*/zenworks-setup

   onde *servidor* é o nome DNS ou o endereço IP de um Servidor ZENworks.
2. No painel de navegação esquerdo, clique em *Ferramentas Administrativas*.
3. Clique em `novell-zenworks-rm-repeater-<versão>.msi` e grave o arquivo em um local temporário.

   versão é a versão do produto ZENworks.
4. Instale o aplicativo proxy executando o seguinte comando:

   ```
   msiexec /i novell-zenworks-rm-repeater-<versão>.msi
   TARGETDIR="ZENworks_Installation_directory”.
   ```

No Linux:

1. No dispositivo, abra um browser da Web e vá para a página de download do ZENworks:

   https://*servidor*/zenworks-setup

   onde *servidor* é o nome DNS ou o endereço IP de um Servidor ZENworks.
2. No painel de navegação esquerdo, clique em *Ferramentas Administrativas*.
3. Clique em `novell-zenworks-rm-repeater-<versão>.noarch.rpm`.
4. Decida se deseja instalar o proxy imediatamente ou gravar o arquivo RPM do proxy para instalá-lo mais tarde.
   - Para instalar o proxy imediatamente, clique em *Open With* (Abrir com) para abrir o Proxy de Gerenciamento Remoto com zen-installer, especifique a senha de root e clique em *OK*.
   - Para gravar o arquivo RPM do proxy no diretório de download padrão, para que seja possível instalá-lo mais tarde, clique em *Save to Disk* (Gravar no Disco). Para instalar o RPM, siga um destes procedimentos:
     - Clique no arquivo RPM do proxy, especifique a senha de root e clique em *OK*.
     - Execute o seguinte comando como superusuário ou usuário root:

       ```
       rpm -ivh novell-zenworks-rm-repeater-<versão>.noarch.rpm
       ```

O Proxy de Gerenciamento Remoto foi projetado para ser executado automaticamente na instalação. Você pode optar por personalizar seu comportamento modificando as configurações padrão no dispositivo. Para obter mais informações sobre as configurações de Proxy de Gerenciamento Remoto, consulte a Seção 2.11, “Configurando um proxy de gerenciamento remoto” na página 51.

2.11 Configurando um proxy de gerenciamento remoto

Quando você instala um Proxy de Gerenciamento Remoto no dispositivo, algumas configurações são definidas no dispositivo, por padrão. É possível editar as configurações.

- Seção 2.11.1, “Configurações de proxy de gerenciamento remoto no dispositivo Windows” na página 51
- Seção 2.11.2, “Configurações de proxy de gerenciamento remoto em um servidor principal ou servidor satélite Linux” na página 51

2.11.1 Configurações de proxy de gerenciamento remoto no dispositivo Windows

No dispositivo Windows, as configurações de Registro do proxy de Gerenciamento Remoto estão disponíveis em `HKLM\SOFTWARE\Novell\ZCM\Remote Management\Proxy`.

ClientPort: especifica o número da porta que o proxy usa para escutar as solicitações de sessão remota do Viewer de Gerenciamento Remoto. O valor padrão é 5750.

SessionEncryption: especifica se o fluxo inicial de dados entre o proxy e o Viewer de Gerenciamento Remoto será criptografado. O valor padrão é Verdadeiro. A configuração não é aplicável depois que o proxy estabelece uma conexão com o dispositivo gerenciado. A criptografia da sessão é controlada pela política de Gerenciamento Remoto e pelas preferências do operador remoto. Convém deixar essa configuração como Verdadeiro, pois se deixá-la como Falso permitirá que processos externos não autenticados diferentes do Viewer de Gerenciamento Remoto estabeleçam conexões com os dispositivos dentro da rede privada.

SSLClientAuthentication: especifica se o proxy deverá aceitar as solicitações de conexão de um viewer sem certificado válido. Os valores possíveis são Verdadeiro e Falso. O valor padrão é Verdadeiro.

2.11.2 Configurações de proxy de gerenciamento remoto em um servidor principal ou servidor satélite Linux

Em um Servidor Principal ou Servidor Satélite Linux, as configurações para o proxy de Gerenciamento Remoto estão disponíveis no arquivo `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`. Algumas das configurações são:

viewerport: especifica o número da porta que o proxy de Gerenciamento Remoto usa para escutar as solicitações de sessão remota do Viewer de Gerenciamento Remoto. O valor padrão é 5750.

runasuser: especifica o usuário que o proxy deverá representar. O Proxy de Gerenciamento Remoto exige apenas privilégios de usuário para realizar as operações remotas. O valor padrão é zenworks. No entanto, é possível especificar um usuário diferente.

strictimpersonation: especifica se a sessão remota deve continuar como `root` quando o usuário especificado como runasuser não existir. Os valores possíveis são verdadeiro ou falso. O valor padrão é falso, indicando que a sessão remota continua como `root` quando o usuário especificado como runasuser não existir.

sslauth: especifica se a autenticação SSL fica habilitada ou desabilitada. Os valores possíveis são 0 ou 1. O valor padrão é 1, indicando que a autenticação SSL fica habilitada.

Aviso: Não é recomendável desabilitar a autenticação SSL porque permite que processos externos acessem os dispositivos da rede sem nenhuma autenticação.

---

verifyViewerCert: especifica se os certificados do Viewer de Gerenciamento Remoto precisam ser verificados. Essa configuração aplica-se apenas quando a autenticação SSL está habilitada. Os valores possíveis são 0 ou 1. O valor padrão é 1, indicando que os certificados do Viewer de Gerenciamento Remoto devem ser verificados. Quando uma sessão é iniciada de um viewer independente, o operador remoto pode não ter os certificados necessários encadeados à Autoridade de Certificação root. Se esse for o caso, ocorrerá falha no proxy para conectar-se ao servidor.

loggingenabled: especifica se as mensagens deverão ser registradas no dispositivo. Os valores possíveis são verdadeiro ou falso. O valor padrão é verdadeiro.

Para obter informações sobre outras configurações de Registro, consulte o arquivo `/etc/opt/novell/zenworks/repeater/nzrepeater.ini`.

Gerenciando sessões remotas 3

As seções a seguir fornecem informações para ajudá-lo a gerenciar com eficiência as sessões remotas do Novell® ZENworks® 10 Configuration Management:

3.1 Gerenciando uma sessão de controle remoto

O Gerenciamento Remoto permite controlar remotamente um dispositivo gerenciado. Com as conexões de controle remoto, o operador remoto pode ir além de visualizar o dispositivo gerenciado para controlá-lo, o que ajuda na assistência ao usuário e na resolução de problemas do dispositivo gerenciado. Para obter informações sobre a inicialização de uma sessão de Controle Remoto, consulte Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.

3.1.1 Usando as opções da barra de ferramentas no viewer de gerenciamento remoto

A tabela a seguir descreve as várias opções da barra de ferramentas disponíveis no viewer de Gerenciamento Remoto durante uma sessão de Controle Remoto. Também lista as teclas de atalho se elas estiverem disponíveis

Tabela 3-1 *Opções da barra de ferramentas no viewer de Gerenciamento Remoto*

Opção	Tecla de atalho	Funcionalidade
Opções de Conexão 	Ctrl+Alt+Shift+P	Possibilita a configuração de vários parâmetros de sessão, como formato e decodificação, para melhorar o desempenho da sessão, registro, local e manuseio de cursor remoto.
Informações sobre Conexões 	Ctrl+Alt+Shift+I	Fornece informações como nome do host, porta, resolução de tela e versão de protocolo do dispositivo gerenciado.
Tela Cheia 	Ctrl+Alt+Shift+F	Permite alternar entre o modo de tela cheia e o modo normal.

Opção	Tecla de atalho	Funcionalidade
Solicitar Atualização de Tela 	Ctrl+Alt+Shift+H	Atualiza a tela de visualização.
Enviar Ctrl-Alt-Del 		Envia as seqüências de teclas Ctrl+Alt+Del para o dispositivo gerenciado. O recurso de simular a funcionalidade Ctrl+Alt+Del no dispositivo Windows 7 está desabilitado.
Enviar Ctrl-Esc 		Chama o menu Iniciar no dispositivo gerenciado.
Pressionar/Liberar Envio de Tecla Alt 		Clicar nessa opção e pressionar a tecla ALT do teclado envia o toque Alt para o dispositivo gerenciado.
Tela em Branco/ Cheia 	Ctrl+Alt+Shift+B	Deixa em branco ou exibe a tela no dispositivo gerenciado. Quando a tela do dispositivo é deixada em branco, as operações realizadas pelo operador remoto no dispositivo não ficam visíveis para o usuário no dispositivo. Os controles de teclado e mouse no dispositivo gerenciado também são bloqueados. Essa opção fica habilitada somente quando a opção *Permitir que a tela do dispositivo gerenciado fique em branco* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado.
Bloquear/ Desbloquear Teclado-Mouse 	Ctrl+Alt+Shift+L	Bloqueia e desbloqueia os controles do teclado e do mouse para o dispositivo gerenciado. Quando os controles do mouse e do teclado são bloqueados, o usuário no dispositivo gerenciado não pode usá-los. Essa opção fica habilitada somente quando a opção *Permitir que o mouse e o teclado do dispositivo gerenciado sejam bloqueados durante o Controle Remoto* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado.
Transferir Arquivos 	Ctrl+Alt+Shift+T	Inicia uma sessão para transferir arquivos de e para o dispositivo gerenciado. Essa opção fica habilitada somente quando a opção *Permitir transferência de arquivos no dispositivo gerenciado* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado. Para obter mais informações sobre transferência de arquivos, consulte Seção 3.5, “Gerenciando uma sessão de transferência de arquivos” na página 60.

Opção	Tecla de atalho	Funcionalidade
Colaboração 		Inicia uma Sessão de Colaboração do Gerenciamento Remoto do ZENworks no dispositivo gerenciado, o que permite convidar vários operadores remotos para se juntar à sessão de gerenciamento remoto. Você também pode delegar os direitos de Controle Remoto a outro operador remoto para ajudá-lo a resolver um problema. Esta opção atualmente é suportada apenas pelo Windows. Para obter mais informações sobre colaboração de sessão, consulte a Seção 3.1.2, “Colaboração de sessão” na página 55.
Execução Remota 	Ctrl+Alt+Shift+U	Inicia a sessão Execução Remota no dispositivo gerenciado, possibilitando que você inicie remotamente qualquer executável no dispositivo gerenciado. Essa opção fica habilitada somente quando a opção *Permitir que programas sejam executados remotamente no dispositivo gerenciado* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado.
Anular Proteção de Tela 	Ctrl+Alt+Shift+O	Anula qualquer proteção de tela protegida por senha no dispositivo gerenciado durante a sessão remota. Essa opção fica habilitada somente quando a opção *Permitir que a proteção de tela seja desbloqueada automaticamente durante o controle remoto* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado.
Desconectar 	Alt+F4	Fecha a sessão remota.

3.1.2 Colaboração de sessão

O recurso Colaboração de Sessão permite convidar vários operadores remotos para entrarem na sessão de Gerenciamento Remoto se eles tiverem iniciado a escuta do Gerenciamento Remoto para solicitações de sessão remota. Também é possível delegar os direitos de Controle Remoto a um operador remoto para ajudá-lo a resolver um problema e depois obter novamente o controle do operador remoto. Esta opção atualmente é suportada apenas pelo Windows.

Se você iniciar a sessão Controle Remoto no dispositivo gerenciado primeiro, obterá todos os privilégios de um operador remoto master. Você pode usar a Colaboração de Sessão para:

- Convidar vários operadores remotos a se juntarem à sessão Controle Remoto.
- Delegar os direitos Controle Remoto a um operador remoto para que ele ajude você a solucionar um problema e, depois, retomar o controle.
- Terminar uma sessão remota.

Iniciar a Colaboração de Sessão:

1. Inicie a sessão de Controle Remoto no dispositivo gerenciado no modo de colaboração.

   Para obter informações sobre como iniciar uma sessão de Controle Remoto, consulte a Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.

2. Na barra de ferramentas do Gerenciamento Remoto, clique em  para exibir a janela Colaboração de Sessão.

A janela Colaboração de Sessão lista os operadores remotos na política de Gerenciamento Remoto efetiva no dispositivo. Cada operador remoto é listado como uma entrada separada precedida por um círculo colorido:

- Um círculo cinza indica que o Operador Remoto não entrou na sessão.
- Um círculo vermelho indica que o Operador Remoto entrou na sessão e está no modo Tela Remota.
- Um círculo verde indica que o operador remoto entrou na sessão e recebeu direitos Controle Remoto na sessão.

Para obter mais informações sobre a Adição de Operadores Remotos, consulte a “Seção 2.3, “Criando a política de gerenciamento remoto” na página 23”.

A tabela a seguir lista as ações que você, como um operador remoto master, pode realizar durante a colaboração de sessão:

Tabela 3-2 *Opções da janela Colaboração de Sessão*

Tarefa	Etapas	Detalhes adicionais
Convidar um operador remoto para se juntar à uma sessão remota	1. Selecione um operador remoto listado na janela de colaboração de sessão. 2. Clique em *Convidar*.	Se o operador remoto aceitar a solicitação e entrar na sessão, o círculo cinza do operador remoto mudará para vermelho. Por padrão, a nova sessão começa no modo Tela Remota.
Delegar direitos Controle Remoto ao operador remoto	1. Selecione o operador remoto ao qual você deseja delegar os direitos de Controle Remoto. 2. Clique em *Delegar*.	O operador remoto selecionado está agora no Modo Controle remoto e o círculo vermelho do operador remoto muda para verde. O operador remoto master alterna automaticamente para o modo Tela Remota
Recuperar os direitos Controle Remoto do operador remoto	1. Clique em *Retomar Controle*.	O operador remoto alterna para o modo Tela Remota e o círculo verde do operador remoto muda para vermelho. O operador remoto master alterna automaticamente para o modo Controle Remoto.

Tarefa	Etapas	Detalhes adicionais
Encerrar a sessão remota	1. Selecione o operador remoto a ser encerrado a partir da Sessão Remota. 2. Clique em *Encerrar.*	Se o operador remoto selecionado estiver no modo Controle Remoto, você retomará os direitos Controle Remoto. A sessão do operador remoto será encerrada e a cor do círculo do operador remoto mudará para cinza.
Convidar um operador remoto externo	1. Clique em *Convidar Externo* para convidar os operadores remotos não listados na janela Colaboração de Sessão para se reunirem na sessão remota. 2. Especifique o nome DNS ou endereço IP do dispositivo do operador remoto e o número da porta. Por exemplo: 10.0.0.0~~1000. 3. Clique em *Convidar.*	

Se o operador remoto master desconectar a sessão remota, todos os operadores remotos serão encerrados da sessão.

3.2 Gerenciando uma sessão de tela remota

A tela remota permite que você se conecte remotamente a um dispositivo gerenciado para que possa ver a área de trabalho do dispositivo gerenciado. Para obter informações sobre a inicialização de uma sessão Controle Remoto, consulte a Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.

A tabela a seguir descreve as várias opções da barra de ferramentas disponíveis no viewer de Gerenciamento Remoto durante uma sessão Controle Remoto.

Tabela 3-3 *Opções da barra de ferramentas no viewer de Gerenciamento Remoto*

Opção	Tecla de atalho	Funcionalidade
Opções de Conexão 	Ctrl+Alt+Shift+P	Possibilita a configuração de vários parâmetros de sessão, como formato e decodificação, para melhorar o desempenho da sessão, registro, local e manuseio de cursor remoto.
Informações sobre Conexões 	Ctrl+Alt+Shift+I	Fornece informações como nome do host, porta, resolução de tela e versão de protocolo do dispositivo gerenciado.

Opção	Tecla de atalho	Funcionalidade
Tela Cheia 	Ctrl+Alt+Shift+F	Permite alternar entre o modo de tela cheia e o modo normal.
Solicitar Atualização de Tela 	Ctrl+Alt+Shift+H	Atualiza a tela de visualização.
Desconectar 	Alt+F4	Fecha a sessão remota.

3.3 Gerenciando uma sessão de execução remota

A Execução Remota permite que você execute remotamente executáveis com privilégios de sistema no dispositivo gerenciado. Para executar um aplicativo em um dispositivo gerenciado, inicie a sessão Execução Remota.

1. Inicie a sessão Execução Remota.

   Para obter informações sobre a inicialização de uma sessão Execução Remota, consulte a Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.
2. Especifique o nome executável.

   Se o aplicativo não estiver no caminho de sistema do dispositivo gerenciado, especifique seu caminho completo. Se você não especificar a extensão do arquivo que deseja executar no dispositivo gerenciado, a Execução Remota anexará a extensão `.exe`.
3. Clique em *Executar*.

A execução remota do aplicativo especificado pode falhar se o aplicativo não estiver disponível no dispositivo gerenciado no caminho definido.

Aviso: Por padrão, o módulo de Gerenciamento Remoto é executado como um serviço, com privilégios de sistema no dispositivo gerenciado. Portanto, todos os aplicativos iniciados durante a sessão de Execução Remota também executarão privilégios de sistema. Por motivos de segurança, é recomendável fechar o aplicativo após sua utilização.

3.4 Gerenciando uma sessão de diagnóstico remoto

O Gerenciamento Remoto permite diagnosticar e analisar remotamente os problemas no 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.

Quando você inicia a sessão de Diagnóstico Remoto no dispositivo gerenciado, pode acessar somente os aplicativos de diagnóstico definidos para o dispositivo nas configurações de Gerenciamento Remoto para diagnosticar e corrigir problemas no dispositivo. Durante a sessão, os aplicativos de diagnósticos são exibidos como ícones em uma barra de ferramentas. Por padrão, os seguintes aplicativos de diagnóstico são definidos nas Configurações de Gerenciamento Remoto:

Tabela 3-4 *Opções da barra de ferramentas no viewer de Gerenciamento Remoto*

Opção	Tecla de atalho	Funcionalidade
Opções de Conexão 	Ctrl+Alt+Shift+P	Possibilita a configuração de vários parâmetros de sessão, como formato e decodificação, para melhorar o desempenho da sessão, registro, local e manuseio de cursor remoto.
Informações sobre Conexões 	Ctrl+Alt+Shift+I	Fornece informações como nome do host, porta, resolução de tela e versão de protocolo do dispositivo gerenciado.
Tela Cheia 	Ctrl+Alt+Shift+F	Permite alternar entre o modo de tela cheia e o modo normal.
Solicitar Atualização de Tela 	Ctrl+Alt+Shift+H	Atualiza a tela de visualização.
Transferir Arquivos 	Ctrl+Alt+Shift+T	Inicia uma sessão para transferir arquivos de e para o dispositivo gerenciado. Essa opção fica habilitada somente quando a opção *Permitir transferência de arquivos no dispositivo gerenciado* é habilitada na política efetiva de Gerenciamento Remoto no dispositivo gerenciado. Para obter mais informações sobre transferência de arquivos, consulte a Seção 3.5, “Gerenciando uma sessão de transferência de arquivos” na página 60.
Desconectar 	Alt+F4	Fecha a sessão remota.

Tabela 3-5 *Aplicativos de Diagnóstico Remoto*

Ícone	Aplicativo
	*Informações sobre o sistema*

Ícone	Aplicativo
	*Gerenciamento do computador*
	*Serviços*
	*Editor de Registros*

Você pode configurar os aplicativos a serem iniciados no dispositivo gerenciado durante a sessão Diagnóstico Remoto. Para obter mais informações sobre a configuração de aplicativos de diagnóstico, consulte a Seção 2.1, “Definindo configurações de gerenciamento remoto” na página 19.

3.5 Gerenciando uma sessão de transferência de arquivos

O Gerenciamento Remoto permite transferir arquivos entre o console de gerenciamento e o dispositivo gerenciado. Para obter informações sobre a inicialização de uma sessão de Transferência de Arquivos, consulte a Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.

Na janela Transferência de Arquivos, o painel Computador Local exibe todos os arquivos e pastas no console de gerenciamento, e o painel Computador Remoto exibe todos os arquivos e pastas no diretório especificado na opção *Diretório Raiz da Transferência de Arquivos* na política de Gerenciamento Remoto. Se a opção *Diretório Raiz da Transferência de Arquivos* não for especificada na política ou se o dispositivo gerenciado não tiver nenhuma política associada a ele, você poderá realizar as operações de Transferência de Arquivos no sistema de arquivo completo do dispositivo remoto.

A tabela a seguir explica os controles e opções de Transferência de Arquivos disponíveis para trabalhar com arquivos na janela Transferência de Arquivos. a opção de menu *Ações* ainda não é suportada no Linux. Contudo, você pode executar a operação clicando no ícone adequado na barra de ferramentas.

Tabela 3-6 *Opções da janela Transferência de Arquivos*

Tarefas	Teclas de Atalho	Etapas	Detalhes adicionais
Criar nova pasta local	Alt+L	1. Clique em *Ações* > *Nova Pasta Local*. ou Clique em no painel Computador Local. 2. Siga os prompts na tela.	
Criar nova pasta remota	Alt+W	1. Clique em *Ações* > *Nova Pasta Remota*. ou Clique em no painel Computador Remoto. 2. Siga os prompts na tela.	
Abrir um arquivo		1. Clique duas vezes no arquivo para abri-lo no seu aplicativo associado.	
Renomear arquivos ou pastas	Alt+N	1. Selecione o arquivo ou a pasta a ser renomeada. 2. Clique em *Ações* > *Renomear.* ou Clique em . 3. Siga os prompts na tela.	
Apagar arquivos ou pastas	Alt+D	1. Selecione os arquivos ou as pastas a serem apagadas. 2. Clique em *Ações* > *Apagar.* ou Clique em . 3. Siga os prompts na tela.	Você pode usar as teclas Shift ou Ctrl para selecionar vários arquivos.

Tarefas	Teclas de Atalho	Etapas	Detalhes adicionais
Atualizar a pasta local	Alt+E	1. Clique em *Ações* > *Atualizar a Pasta Local*. ou Clique em no painel Computador Local.	
Atualizar a pasta remota	Alt+M	1. Clique em *Ações* > *Atualizar a Pasta Remota*. ou Clique em no painel Computador Remoto.	
Classificar arquivos locais		1. Clique em *Ações* > *Classificação Local*. 2. Selecione o tipo de classificação. Você pode classificar os arquivos por nome, tamanho ou data.	Você também pode classificar os arquivos clicando nos respectivos cabeçalhos de coluna.
Classificar arquivos remotos		1. Clique em *Ações* > *Classificação Remota*. 2. Selecione o tipo de classificação. Você pode classificar os arquivos por nome, tamanho ou data	Você também pode classificar os arquivos clicando nos respectivos cabeçalhos de coluna.
Carregar arquivos/pastas		1. Selecione os arquivos a serem carregados para o computador remoto. 2. Selecione a pasta de destino no painel do computador remoto. 3. Clique em *Ações* > *Upload.* ou Clique em ➡	A opção *Ação* > *Upload* está disponível apenas quando o foco está no computador local. Você pode usar a tecla Shift ou Ctrl para selecionar vários arquivos.

Tarefas	Teclas de Atalho	Etapas	Detalhes adicionais
Fazer download de arquivos/pastas	Alt+O	1. Selecione os arquivos para download para o computador local. 2. Selecione a pasta de destino no painel do computador local. 3. Clique em *Ações* > *Carregar.* ou Clique em ⬅	A opção *Ação* > *Download está* disponível apenas quando o foco estiver no computador remoto. Você pode usar a tecla Shift ou Ctrl para selecionar vários arquivos.
Cancelar Transferência de Arquivo	Alt+C	1. Clique em *Ações* > *Cancelar Transferência de Arquivo*.	Também é possível cancelar a operação de transferência de arquivo clicando no botão cancelar.
Exibir as propriedades do arquivo	Alt+P	1. Selecione os arquivos. 2. Clique em *Ações* > *Propriedades.* ou Clique em	Você pode usar a tecla Shift ou Ctrl para selecionar vários arquivos. Exibe o tamanho cumulativo dos arquivos e das pastas selecionadas.
Mover para a pasta pai		1. Clique em .. para mover para a pasta pai.	

3.6 Gerenciando uma sessão de proxy de gerenciamento remoto

O Proxy de Gerenciamento Remoto permite executar uma operação de Gerenciamento Remoto em um dispositivo gerenciado que esteja em uma rede privada ou protegido por um firewall ou roteador que utilize NAT.

Para obter mais informações sobre um Proxy de Gerenciamento Remoto, consulte a Seção 1.4, “Entendendo o proxy de gerenciamento remoto” na página 16.

Para obter mais informações sobre como instalar um Proxy de Gerenciamento Remoto, consulte a Seção 2.10, “Instalando um proxy de gerenciamento remoto” na página 49.

Para obter mais informações sobre como configurar um Proxy de Gerenciamento Remoto, consulte a Seção 2.11, “Configurando um proxy de gerenciamento remoto” na página 51.

3.7 Ativando um dispositivo remoto

A Ativação Remota permite ativar remotamente um nó único ou um grupo de nós desativados em sua rede, se a placa de rede no nó estiver habilitada para Wake-on-LAN.

A ativação de um dispositivo com várias NICs (Network Interface Cards - Placas de Interface de Rede) somente será bem-sucedida se uma ou mais NICs estiverem configuradas para uma sub-rede contendo o dispositivo que está transmitindo o pacote Wake-on-LAN.

3.7.1 Pré-requisitos

Antes que os dispositivos gerenciados sejam ativados, os seguintes requisitos devem ser satisfeitos:

- Verifique se a placa de rede no dispositivo gerenciado suporta Wake-on-LAN. Além disso, verifique se você habilitou a opção Wake-on-LAN na configuração do BIOS do dispositivo gerenciado.
- Verifique se o dispositivo gerenciado está registrado na Zona de Gerenciamento do ZENworks.
- Verifique se o nó remoto está em um estado virtual desativado. No estado soft-power off, a CPU é desligada e uma quantidade mínima de energia é utilizada por sua placa de interface de rede. Ao contrário do estado hard-off (desligamento mecânico, consumo zero), no estado soft-off a alimentação de energia elétrica continua quando a máquina é desligada.

3.7.2 Ativando remotamente os dispositivos gerenciados

Para executar uma Ativação Remota:

1. No ZENworks Control Center, clique em *Dispositivos*.
2. Clique em *Servidores* ou *Estações de Trabalho* para exibir a lista de dispositivos gerenciados.
3. Selecione o dispositivo a ser ativado.
4. Clique em *Tarefas Rápidas* > *Ativar* para exibir a caixa de diálogo Ativar.
5. Selecione uma das seguintes opções para especificar os servidores que enviarão uma solicitação de acionamento para os dispositivos gerenciados:
   - **Detectar o servidor automaticamente:** o ZENworks detecta automaticamente o Servidor Principal mais próximo ao dispositivo gerenciado. Se o servidor e o dispositivo remoto estiverem em sub-redes diferentes, verifique se o roteador que os conecta está configurado para encaminhar broadcasts orientados por sub-rede na porta UDP 1761.
   - **Use os seguintes dispositivos:** clique em *Adicionar* para selecionar um dispositivo proxy que exista na mesma sub-rede do dispositivo que você deseja acionar.

     Se o roteador estiver configurado para encaminhar broadcasts orientados por sub-rede na porta UDP 1761, não haverá a necessidade de um proxy.
6. (Opcional) Selecione uma das seguintes opções para especificar o endereço IP a ser usado no envio de broadcast de acionamento:
   - **Detectar o endereço IP automaticamente:** o ZENworks detecta automaticamente o endereço de broadcast padrão da sub-rede para enviar o broadcast de acionamento ao dispositivo gerenciado.
   - **Usar o seguinte endereço IP:** especifique o endereço IP para enviar o broadcast de acionamento ao dispositivo gerenciado e clique em *Adicionar*.
7. Na opção *Número de Tentativas*, especifique o número de tentativas para ativar o dispositivo. O padrão é 1.

8 Na opção *Intervalo de Tempo Entre as Tentativas*, especifique o tempo entre cada tentativa. O padrão é 2 minutos.

9 Clique em *OK*.

Os valores padrão das opções *Número de Tentativas* e Intervalo de Tempo Entre as Tentativas são configurados no nível de zona. É possível anular esses valores no nível do dispositivo.

3.8 Melhorando o desempenho do gerenciamento remoto

O desempenho do Gerenciamento Remoto em um link lento ou rápido durante uma sessão remota varia conforme o tráfego na rede. Para obter um melhor tempo de resposta, tente uma das seguintes opções:

- Seção 3.8.1, “No console de gerenciamento” na página 65
- Seção 3.8.2, “No dispositivo gerenciado” na página 65

3.8.1 No console de gerenciamento

Na janela Conexão de Gerenciamento Remoto do ZENworks no console, clique em *Opções* e defina os seguintes valores:

- Para maximizar o desempenho do Gerenciamento Remoto em um link lento:
  - Selecione a opção *Usar cores de 8 bits*.
  - Defina o *Nível compactação person.* para o nível 6.
- Selecione a opção *Bloquear Eventos Mov. Mouse*.
- Habilite a opção *Suprimir Papel de Parede* nas Configurações de Gerenciamento Remoto.

3.8.2 No dispositivo gerenciado

- A velocidade da sessão de Gerenciamento Remoto depende da capacidade de processamento do dispositivo gerenciado. É recomendável usar o processador Pentium* III, 700MHz (ou superior) com 256 MB de RAM ou superior.
- Não defina um padrão de papel de parede.

Segurança

4

As seções a seguir fornecem informações sobre segurança que você deve ter em mente ao usar o componente de Gerenciamento Remoto do Novell® ZENworks® 10 Configuration Management:

4.1 Autenticação

O serviço de Gerenciamento Remoto deve ser instalado em um dispositivo para o operador remoto para gerenciar remotamente o dispositivo. O serviço é iniciado automaticamente quando o dispositivo gerenciado é inicializado. Quando um operador remoto inicia uma sessão remota no dispositivo gerenciado, o serviço inicia a sessão remota somente se o operador remoto estiver autorizado a realizar operações remotas no dispositivo gerenciado.

Para evitar o acesso não autorizado ao dispositivo gerenciado, o serviço de Gerenciamento Remoto no dispositivo gerenciado usa os seguintes modos de autenticação:

4.1.1 Autenticação de gerenciamento remoto baseada em direitos

Na autenticação baseada em direitos, os direitos são atribuídos ao operador remoto para iniciar uma sessão remota no dispositivo gerenciado. Por padrão, o administrador do ZENworks e o superadministrador têm direitos para realizar operações remotas em todos os dispositivos gerenciados, independentemente do fato do usuário local ou do usuário do ZENworks estar conectado no dispositivo.

O operador remoto não precisa de direitos exclusivos para realizar uma sessão remota no dispositivo gerenciado se nenhum usuário estiver conectado ao dispositivo gerenciado ou se um usuário tiver se conectado ao dispositivo gerenciado, mas não tiver se conectado ao ZENworks. Porém, o operador remoto precisa de direitos Gerenciamento Remoto exclusivos para realizar a operação remota no dispositivo gerenciado quando um usuário do ZENworks tiver se conectado ao dispositivo. É recomendável que você use a autenticação baseada em direitos porque ela é segura.

O uso da autenticação com base em direitos requer a instalação do ZENworks Adaptive Agent no dispositivo. Não é suficiente instalar apenas o serviço de Gerenciamento Remoto no dispositivo.

Esse modo de autenticação não é suportado quando se inicia a operação de gerenciamento remoto no modo independente ou por linha de comando.

4.1.2 Autenticação de gerenciamento remoto baseada em senha

Na autenticação de Gerenciamento Remoto baseada em senha, o operador remoto é solicitado a digitar uma senha para iniciar a sessão remota no dispositivo gerenciado.

Os dois tipos de esquema de autenticação de senha usados são:

- **Senha do ZENworks:** esse esquema é baseado no protocolo SRP (Secure Remote Password) (versão 6a). O comprimento máximo de uma senha do ZENworks é de 255 caracteres.
- **Senha do VNC:** esse é o esquema de autenticação de senha do VNC tradicional. O comprimento máximo da senha do VNC é de 8 caracteres. Esse esquema de senha é naturalmente fraco e fornecido somente para interoperabilidade com os componentes de código fonte aberto.

Se você usa autenticação baseada em senha, é altamente recomendável utilizar o esquema de senha do ZENworks, que é mais seguro que o esquema de senha do VNC.

Os esquemas de senha operam nos seguintes modos:

- **Modo de Sessão:** a senha definida nesse modo é válida somente para a sessão atual. O usuário no dispositivo gerenciado deve definir uma senha no início da sessão remota e comunicá-la ao operador remoto por um meio externo, como o telefone. Quando inicializar uma sessão remota com o dispositivo gerenciado, o operador remoto deverá digitar a senha correta na caixa de diálogo exibida de senha da sessão. Se o operador remoto não digitar a senha correta dentro de dois minutos depois que a caixa de diálogo for exibida, a sessão será fechada por motivos de segurança. Se você usar a autenticação baseada em senha, é recomendável que você use esse modo de autenticação porque a senha é válida somente para a sessão atual e não será gravada no dispositivo gerenciado.
- **Modo persistente:** nesse modo, a senha pode ser definida pelo administrador por meio da política de Gerenciamento Remoto ou pelo usuário do dispositivo gerenciado por meio do ícone do ZENworks, se a opção *Permitir que o usuário substitua as senhas padrão no dispositivo gerenciado* estiver selecionada nas configurações de segurança da política de Gerenciamento Remoto.

  Se a senha for definida pelo usuário do dispositivo gerenciado e na política, a senha definida pelo usuário terá precedência sobre a senha configurada na política.

  O administrador pode evitar que o usuário do dispositivo gerenciado defina a senha e pode até mesmo redefinir a senha definida pelo usuário para assegurar que a senha configurada na política seja sempre obrigatória durante a autenticação. Para obter mais informações sobre a redefinição da senha definida pelo usuário do dispositivo gerenciado, consulte a Seção 2.5.3, “Limpando a senha de gerenciamento remoto usando o ZENworks Control Center” na página 33.

4.2 Força da senha

Use senhas seguras. Lembre-se das seguintes diretrizes:

- **Tamanho:** o tamanho mínimo recomendado é de 6 caracteres. Uma senha segura tem, no mínimo, 8 caracteres; senhas maiores são melhores. O tamanho máximo da senha são 255 caracteres para uma senha do ZENworks e 8 caracteres para uma senha do VNC.
- **Complexidade:** uma senha segura contém uma mistura de letras e números. Ela deve conter letras maiúsculas e minúsculas e pelo menos um caractere numérico. Adicionar números às senhas, especialmente quando eles são adicionados no meio e não somente no começo e no final da senha, pode aumentar a eficiência da senha. Caracteres especiais como &, *, $, e > podem melhorar muito a força da senha. Não use palavras que podem ser reconhecidas, como nomes próprios ou palavras de um dicionário, e não use informações pessoais, como números de telefone, datas de nascimento e aniversário, endereços ou CEPs.

4.3 Portas

Por padrão, o serviço de Gerenciamento Remoto é executado na porta 5950 e a Escuta do Gerenciamento Remoto é executada na porta 5550. O firewall é configurado para permitir qualquer porta usada pelo serviço de Gerenciamento Remoto, mas você deve configurar o firewall para permitir a porta usada pela Escuta do Gerenciamento Remoto.

Por padrão, o proxy de gerenciamento remoto escuta na porta 5750.

4.4 Auditoria

O ZENworks Configuration Management mantém um registro de todas as sessões de assistência remota realizadas no dispositivo gerenciado. Esse registro é mantido no dispositivo gerenciado e pode ser visto pelo usuário e pelo administrador. O administrador pode ver os registros de todas as sessões remotas realizadas no dispositivo. O usuário pode ver os registros de todas as sessões remotas executadas no dispositivo quando ele estava conectado.

Para ver o registro de auditoria:

1. Clique duas vezes no ícone do ZENworks na área de notificação do dispositivo gerenciado.
2. No painel esquerdo, navegue para *Gerenciamento Remoto* e, em seguida, clique em *Segurança*.
3. Clique em *Exibir Informações de Auditoria* para exibir as informações de auditoria das operações remotas realizadas no dispositivo.

Campo	Descrição
Usuário do ZENworks	Nome do usuário do ZENworks conectado ao dispositivo gerenciado no início da sessão remota.
Operador remoto	Nome do operador remoto que executou a operação.
Máquina Console	Nome de host do dispositivo a partir do qual a operação foi executada.

Campo	Descrição
IP do Console	Endereço IP do dispositivo a partir do qual a operação remota foi executada.
	Observação: Se a operação de gerenciamento remoto do dispositivo for roteada por meio de um proxy de Gerenciamento Remoto, o endereço IP do dispositivo executando o proxy será exibido.
Operação	O tipo de operação realizada: Controle Remoto, Execução Remota, Tela Remota, Diagnóstico Remoto, Transferência de Arquivos.
Horário de Início	O horário de início da operação remota.
Horário de Término	O horário de conclusão da operação remota.
Status	O status da operação remota: Sucesso, Executando ou Falha. A causa da falha também é exibida.

4.5 Solicitar permissão do usuário do dispositivo gerenciado

O administrador pode configurar a política de Gerenciamento Remoto para permitir que os operadores remotos solicitem a permissão do usuário do dispositivo gerenciado antes de começar uma operação remota no dispositivo.

Quando o operador remoto inicia a sessão remota no dispositivo gerenciado, o serviço de Gerenciamento Remoto verifica se a opção *Solicitar permissão ao usuário no dispositivo gerenciado* para aquela operação remota está habilitada na política efetiva no dispositivo. Se a opção estiver habilitada e nenhum usuário tiver se conectado ao dispositivo, a sessão remota continuará. Mas se a opção estiver habilitada e um usuário tiver se conectado ao dispositivo gerenciado, uma mensagem configurada na política de Gerenciamento Remoto será exibida ao usuário, solicitando permissão para iniciar a sessão remota no dispositivo. A sessão é iniciada somente se o usuário conceder a permissão.

4.6 Abend

Quando uma sessão remota é repentinamente desconectada, o recurso abend permite que você bloqueie o dispositivo gerenciado ou desconecte o usuário no dispositivo gerenciado, dependendo da definição das configurações de segurança da política de Gerenciamento Remoto. A sessão remota é encerrada de maneira anormal nas seguintes circunstâncias:

- As redes falham e o viewer de Gerenciamento Remoto e o serviço de Gerenciamento Remoto não conseguem se comunicar.
- O viewer de Gerenciamento Remoto é fechado repentinamente através do gerenciador de tarefas.
- A rede é desabilitada no dispositivo gerenciado ou no console de gerenciamento.

Sob algumas circunstâncias, o serviço de Gerenciamento Remoto pode levar até um minuto para determinar o encerramento anormal da sessão.

4.7 Detecção de intrusão

O recurso Detecção de Intrusão diminui significativamente o risco de invasão do dispositivo gerenciado. Se o operador remoto não conseguir se conectar ao dispositivo gerenciado dentro do número de tentativas especificado (o padrão é 5), o serviço de Gerenciamento Remoto será bloqueado e não aceitará nenhuma sessão remota até que seja desbloqueado. O administrador pode desbloquear o serviço de Gerenciamento Remoto manualmente ou automaticamente.

4.7.1 Desbloqueando automaticamente o serviço de gerenciamento remoto

O serviço de Gerenciamento Remoto é automaticamente desbloqueado após o tempo especificado na opção *Começar a aceitar automaticamente as conexões após [] minutos* na política de Gerenciamento Remoto. O tempo padrão é 10 minutos. Você pode mudar o período padrão nas configurações de segurança da política de Gerenciamento Remoto.

4.7.2 Desbloqueando manualmente o serviço de gerenciamento remoto

Você pode desbloquear manualmente o serviço de Gerenciamento Remoto pelo dispositivo gerenciado ou pelo ZENworks Control Center.

Para isso, o operador remoto deve ter direitos de Desbloquear o serviço de Gerenciamento Remoto pelo dispositivo gerenciado.

1. No ZENworks Control Center, clique em *Dispositivos*.
2. Clique em *Servidores* ou *Estações de Trabalho* para exibir a lista de dispositivos gerenciados.
3. Selecione o dispositivo a ser desbloqueado.
4. Clique em *Ação* e, em seguida, clique em *Desbloquear o Gerenciamento Remoto*.
5. Clique em *OK*.

Para desbloquear o serviço de Gerenciamento Remoto do dispositivo gerenciado:

1. Clique duas vezes no ícone do ZENworks na área de notificação do dispositivo gerenciado.
2. No painel esquerdo, navegue para *Gerenciamento Remoto* e, em seguida, clique em *Segurança*.
3. Clique em *Habilitar a Aceitação de Conexões Se Bloqueadas Devido à Detecção de Intrusão.*

4.8 Identificação de operador remoto

Quando um operador remoto inicia uma sessão remota no ZENworks Control Center, é gerado automaticamente um certificado que ajuda o dispositivo gerenciado a identificar o operador remoto. Porém, se o operador remoto iniciar a sessão em um modo independente, o certificado não será gerado e o operador remoto será registrado como *Usuário Desconhecido* nos registros de auditoria, a caixa de diálogo Sinal Visível e Pedir Permissão do Usuário. O serviço de Gerenciamento Remoto recupera a identidade do operador remoto usando o certificado fornecido pelo console de gerenciamento durante o handshake SSL (Secure Socket Layer). O handshake SSL acontece para todos os tipos de autenticação, exceto para a autenticação de senha do VNC.

O serviço de Gerenciamento Remoto no dispositivo exibe os detalhes do operador remoto na caixa de diálogo de sinal visível, se a opção *Enviar Sinal Visível ao Usuário no Dispositivo Gerenciado* estiver habilitada na política efetiva no dispositivo. Além disso, ele inclui as informações do operador remoto nos registros de Auditoria do Gerenciamento Remoto.

4.9 Configuração do browser

Se você usa o Internet Explorer para iniciar o ZENworks Control Center em dispositivos do Windows Vista, desligue o modo protegido nas configurações de segurança do browser (*Ferramentas* > *Opções de Internet* > *Segurança*) e reinicie o browser.

4.10 Segurança da sessão

O ZENworks Configuration Management usa o SSL (Secure Socket Layer) para proteger sessões remotas. Porém, as sessões remotas iniciadas com a autenticação baseada em senha do VNC não são protegidas. O processo de autenticação ocorre em um canal seguro quando se estabelece comunicação SSL, independentemente de a criptografia da sessão estar ou não configurada na política de Gerenciamento Remoto.

Após a conclusão da autenticação, a sessão remota alternará para um modo inseguro se a opção *Habilitar Criptografia de Sessão* estiver desabilitada na política de Gerenciamento Remoto e se a opção *Criptografia da Sessão* for desabilitada pelo operador remoto durante a inicialização de uma sessão remota no dispositivo gerenciado. Entretanto, é recomendável que você prossiga com a sessão em um modo seguro, pois não há impacto significativo sobre o desempenho da sessão.

4.10.1 Handshake SSL

Quando o ZENworks Adaptive Agent é instalado em um dispositivo gerenciado, o serviço de Gerenciamento Remoto gera um certificado auto-assinado válido por 10 anos.

Quando um operador remoto inicia uma sessão remota no dispositivo gerenciado, o viewer do Gerenciador Remoto solicita que operador remoto verifique o certificado do dispositivo gerenciado. O certificado exibe detalhes como nome do dispositivo gerenciado, autoridade emissora certificada, validade do certificado e impressões digitais. Por motivos de segurança, o operador remoto deve verificar as credenciais do dispositivo gerenciado fazendo a correspondência das impressões digitais do certificado com as impressões digitais comunicadas pelo usuário do dispositivo gerenciado através de meios out-of-band. Em seguida, o operador remoto pode executar uma das seguintes ações:

- **Aceitar o certificado permanentemente:** se um usuário que se conectou no console de gerenciamento aceitar o certificado permanentemente, o certificado não será exibido nas sessões remotas subseqüentes iniciadas pelos usuários conectados naquele console.
- **Aceitar o certificado temporariamente:** se um usuário que se conectou no console de gerenciamento aceitar o certificado temporariamente, ele será aceito somente para a sessão atual. O usuário é solicitado a verificar o certificado da próxima vez que uma conexão for iniciada no dispositivo gerenciado.
- **Rejeitar o certificado:** se um usuário que se conectou no console de gerenciamento rejeitar o certificado, a sessão remota será encerrada.

4.10.2 Mais uma geração do certificado

O dispositivo gerenciado gera mais uma vez um novo certificado auto-assinado se:

- O nome do dispositivo gerenciado mudou
- O certificado está pós-datado e não é mais válido
- O certificado venceu
- O certificado está para vencer
- O certificado está ausente

Por padrão, o certificado é gerado novamente uma vez a cada 10 anos.

Guias de solução de problemas

5

As seções a seguir explicam os cenários que podem ser encontrados na utilização do componente de Gerenciamento Remoto do Novell® ZENworks® 10 Configuration Management.

- “Durante a sessão de Controle Remoto, clicar no ícone Ctrl+Alt+Del no viewer de Gerenciamento Remoto poderá exibir a janela Secure Attention Sequence (Seqüência de Atenção Segura) sem nenhum controle” na página 81
- “A área de trabalho de um dispositivo talvez não esteja visível quando o dispositivo for controlado ou visto remotamente” na página 81
- “Impossível transferir arquivos remotamente para pastas restritas no dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2” na página 82
- “Impossível iniciar uma sessão remota no dispositivo SUSE Linux Enterprise Server 11 por meio do Mozilla Firefox” na página 82
- “O link Atualizar Viewer de Gerenciamento Remoto não aparece quando você inicia o ZENworks Control Center pelo Internet Explorer 8” na página 83

Não é possível anular a proteção de tela no dispositivo gerenciado

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Quando uma proteção de tela protegida por senha é ativada no dispositivo gerenciado antes do início de uma sessão Controle Remoto, o serviço de Gerenciamento Remoto tenta anular a proteção de tela para habilitar o operador remoto para ver a área de trabalho do usuário. O operador remoto também pode anular a proteção de tela durante a sessão remota clicando no ícone *Anular Proteção de Tela* na barra de ferramentas do viewer de Gerenciamento Remoto.

Causa possível: Se a proteção de tela é ativada por inatividade da sessão remota.

Ação: Clique no ícone *Anular Proteção de Tela* na barra de ferramentas do viewer de Gerenciamento Remoto. Pode ser necessário clicar no ícone algumas vezes até que ela seja anulada.

Causa possível: Não é suportado anular o recurso de Proteção de Tela em um dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2.

Ação: Nenhuma.

Causa possível: A proteção de tela pode ser interrompida se qualquer movimento do mouse for enviado para o dispositivo gerenciado.

Ação: Selecione a opção *Bloquear eventos mov. mouse* na janela de opções do viewer de Gerenciamento Remoto do ZENworks para evitar que os movimentos do mouse sejam enviados ao dispositivo gerenciado.

Causa possível: O GINA (graphical identification and authentication - identificação e autenticação gráfica) no dispositivo gerenciado é ativado por causa da interrupção da proteção de tela no dispositivo gerenciado.

Ação: Efetue login no dispositivo gerenciado novamente.

Durante a sessão de Gerenciamento Remoto, se você efetuar logout e em seguida login novamente em um computador Windows 2000* Professional, o papel de parede definido no computador talvez não seja restaurado

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Ação: Nenhuma.

Impossível iniciar uma sessão remota no dispositivo gerenciado, que está sendo executado com uma qualidade de cor muito baixa

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Pode não ser possível iniciar as sessões Controle Remoto, Tela Remota ou Diagnóstico Remoto em um dispositivo gerenciado que esteja sendo executado em uma qualidade muito baixa de cor (menos de 8 bits por pixel (bpp)).

Ação: Aumente a qualidade da cor do dispositivo para 16 bpp ou superior usando o procedimento a seguir:

1. Clique o botão direito na área de trabalho.
2. Clique em *Propriedades*.
3. Na janela Propriedades de Exibição, clique em *Configurações*.
4. Selecione a qualidade de cor apropriada e, em seguida, clique em *OK*.

Impossível iniciar o viewer de Gerenciamento Remoto

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: O viewer de Gerenciamento Remoto pode não ser iniciado se o arquivo executável do viewer de Gerenciamento Remoto for apagado ou renomeado.

Ação: Reinstale o viewer de Gerenciamento Remoto fazendo download da última versão do `novell-zenworks-rm-viewer.msi` de `https://`*`EndereçoIP_servidor_ZENworks`*`/zenworks-remote-management`.

O Abend de Sessão pode falhar no dispositivo gerenciado Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Durante uma sessão remota, se o usuário desabilitar a conexão de rede no dispositivo gerenciado Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2, o ZENworks poderá não detectar isso como abend e não bloquear o dispositivo nem desconectar o usuário do dispositivo.

Ação: Nenhuma.

A Escuta do Gerenciamento Remoto não aceita as solicitações de sessão remota do dispositivo gerenciado, se a porta na qual a escuta está vinculada não for aberta no firewall do console de gerenciamento

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Ação: No firewall do console de gerenciamento, abra a porta da escuta.

Mensagens de erro de solução de problemas encontradas durante o uso do componente de Gerenciamento Remoto

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Ação: Para solucionar o problema das mensagens de erro encontradas durante o uso do componente de Gerenciamento Remoto, envie os seguintes arquivos de registro para o Suporte da Novell (http://support.novell.com):

- Arquivos `WinVNCApp.log` e `WinVNC.log` para o dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2
- Arquivo `WinVNC.log` para outros dispositivos gerenciados

Para acessar o arquivo de registro:

1. Abra o Editor de Registro.
2. Vá para `HKLM\Software\Novell\ZCM\Remote Management\Agent`.
3. Crie um DWORD chamado DebugMode e defina o valor para 2.
4. Crie um DWORD chamado DebugLevel e defina o valor hexadecimal para `a` (valor decimal igual a 10).
5. Reinicie o Serviço de Gerenciamento Remoto.

Os arquivos de registro do Gerenciamento Remoto a seguir são criados em *`diretório_instalação_ZENworks`*`\logs`:

- `WinVNC.log`
- `WinVNCApp.log`

Como habilitar o registro de depuração de Gerenciamento Remoto no dispositivo que inicia o ZENworks Control Center

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Ação: Para habilitar os registros, consulte o TID 3418069 no Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Instalar uma nova versão do driver espelhado

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: Quando você instala o ZENworks Adaptive Agent em um dispositivo gerenciado de 64 bits Windows 2003, o driver espelhado não é instalado no dispositivo. A mensagem `Instalar nova versão do driver de espelhamento` é conectada no ZENworks Control Center.

É possível realizar sessões remotas no dispositivo, mas o desempenho diminui.

Ação: Ignore esta mensagem.

Causa possível: Se você controla remotamente um dispositivo que já está conectado usando a Conexão da Área de Trabalho Remota (RDP), a mensagem `Instalar nova versão do driver de espelhamento` será conectada no ZENworks Control Center.

Você pode executar sessões remotas no dispositivo, mas o desempenho diminuirá.

Ação: Ignore esta mensagem.

O dispositivo gerenciado não pôde inicializar o esquema de criptografia da Novell para a sessão. Verifique se o horário UTC do dispositivo gerenciado foi sincronizado com o sistema. Se o problema persistir, entre em contato com os Serviços Técnicos da Novell

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: O dispositivo gerenciado foi atualizado ou registrado, e essas informações podem não estar atualizadas no Registro do dispositivo gerenciado.

Ação: Quando o dispositivo gerenciado é atualizado ou registrado, faça o seguinte:

1. Atualize o nome de domínio do novo certificado da CA no registro com os novos detalhes:

   Chave: HKLM\Software\Novell\ZCM

   Valor: CASubject
2. Importe o certificado da CA da nova zona para o armazenamentodecertificado raiz confiável.
3. Remova o certificado da CA da antiga zona de armazenamentodecertificado raiz confiável.

Causa possível: O dispositivo gerenciado foi movido para uma nova Zona de Gerenciamento.

Ação: Gerencie o dispositivo pela nova Zona de Gerenciamento.

Aplicativos como o Regedit, quando iniciados em dispositivos gerenciados de 64 bits pela Execução Remota, não têm acesso a determinadas chaves de registro

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: Os aplicativos iniciados no dispositivo gerenciado de 64 bits usando a Execução Remota são executados em ambiente WOW (Windows On Windows).

Ação: Inicie os aplicativos usando Diagnóstico Remoto.

A opção de tela em branco poderá não funcionar enquanto um dispositivo Windows for controlado remotamente

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: Drivers legados do Windows não aceitam a opção de energia de tela em branco.

Ação: Você deve instalar o driver gráfico específico do sistema.

Quando uma sessão de gerenciamento remoto é iniciada em um dispositivo gerenciado do Windows 2000 Professional, o dispositivo é reinicializado

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: O driver de vídeo não está instalado no dispositivo.

Ação: Você deve instalar o driver de vídeo específico do sistema.

Várias instâncias do viewer de Gerenciamento Remoto são iniciadas no dispositivo que tem o browser Internet Explorer 7

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Causa possível: Se você iniciar uma operação de Gerenciamento Remoto em um dispositivo que tiver o browser Internet Explorer 7, várias instâncias do viewer serão iniciadas no dispositivo se houver um software acelerador de download, como o FlashGet, instalado no console de gerenciamento.

Ação: Desabilite temporariamente os complementos dos aceleradores de download:

1. Inicie o browser Internet Explorer 7.
2. Clique em *Ferramentas* > *Gerenciar Complementos*.
3. Clique em *Habilitar ou Desabilitar Complementos* e desabilite o complemento do acelerador de download.
4. Inicie a operação de Gerenciamento Remoto.

Ação: Tente usar o browser Firefox para executar a operação.

Impossível usar o ícone Ctrl-Alt-Del durante o controle remoto de um dispositivo Windows Vista, Windows Server 2008 ou Windows Server 2008 R2

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Se você iniciar uma operação de Controle Remoto em um dispositivo Windows Vista, Windows Server 2008 ou Windows Server 2008 R2 que tenha o UAC (User Account Control - Controle de Conta de Usuário) desabilitado, o ícone *Ctrl-Alt-Del* ficará esmaecido.

Ação: Habilite o UAC.

O modo de sessão padrão não está selecionado no snap-in de Gerenciamento Remoto

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Se você usar o Internet Explorer para abrir o ZENworks Control Center e executar uma operação de Gerenciamento Remoto em um dispositivo, o modo de sessão padrão não será selecionado no snap-in de Gerenciamento Remoto. Entretanto, se você não selecionar nenhum modo de sessão, a operação de Controle Remoto será iniciada no modo Colaborar padrão e a operação de Tela Remota será iniciada no modo Exclusivo padrão.

Ação: Selecione o modo de sessão no qual executar a Operação Remota.

O link Instalar Viewer de Gerenciamento Remoto permanece ativo no dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 que tem o browser Internet Explorer 7

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Em um dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 que tem o browser Internet Explorer 7, o *Viewer de Gerenciamento Remoto* poderá não ser instalado se o controle ActiveX* não for ativado.

Ação: Faça o seguinte para ativar o UAC (Controle de Conta de Usuário) no dispositivo do Vista:

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle* > *Contas de Usuário* > *Contas de Usuário* > *Ativar ou Desativar o Controle de Conta de Usuário*.
2. Selecione *Utilizar o UAC (Controle de Conta de Usuário) para ajudar a proteger o computador*.
3. Clique em *OK*.

Ação: Se não quiser ativar o UAC no dispositivo Windows Vista, convém fazer upgrade para o Windows Vista SP1.

A instalação do viewer de Gerenciamento Remoto pode falhar

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: A instalação do viewer de Gerenciamento Remoto pode falhar. Esse erro é inerente à estrutura MSI.

Ação: Execute uma das seguintes etapas:

- Desinstale o viewer de Gerenciamento Remoto usando Adicionar ou Remover Programas e depois o reinstale
- Use o Utilitário de Limpeza do Microsoft Windows Installer para limpar o aplicativo e depois reinstale-o. É possível fazer download desse utilitário do Suporte da Microsoft (http://support.microsoft.com/kb/290301)

O viewer de Gerenciamento Remoto não é iniciado em um dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: No dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2, o viewer de Gerenciamento Remoto não é iniciado, mesmo que o prompt de segurança seja concluído com êxito.

Ação: Adicione o servidor que executa o ZENworks Control Center à lista de sites confiáveis e repita.

Durante a sessão de Controle Remoto, clicar no ícone Ctrl+Alt+Del no viewer de Gerenciamento Remoto poderá exibir a janela Secure Attention Sequence (Seqüência de Atenção Segura) sem nenhum controle

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Ação: Clique no ícone *Ctrl+Alt+Del* no viewer de Gerenciamento Remoto e pressione a tecla Esc para sair da janela Secure Attention Sequence (SAS) (Seqüência de Atenção Segura (SAS)). Em seguida, clique no ícone *Ctrl+Alt+Del* no viewer de Gerenciamento Remoto.

A área de trabalho de um dispositivo talvez não esteja visível quando o dispositivo for controlado ou visto remotamente

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Se um dispositivo no qual uma sessão RDP foi executada for controlado ou visto remotamente, uma tela escura poderá ser exibida em vez da área de trabalho do dispositivo.

Ação: Para ver a área de trabalho do dispositivo:

1. Desbloqueie a área de trabalho manualmente.
2. Reinicie uma sessão RDP na sessão de console do dispositivo, executando o seguinte comando:

```
mstsc /console
```

Impossível transferir arquivos remotamente para pastas restritas no dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Se você iniciar uma operação de Transferência de Arquivos para transferir arquivos remotamente para as pastas restritas em um dispositivo Windows Vista, Windows 7, Windows Server 2008 ou Windows Server 2008 R2 que tenha o UAC (User Account Control - Controle de Conta de Usuário) habilitado, a operação falhará.

Ação: Faça o seguinte para desativar o Controle de Conta de Usuário (UAC) no dispositivo Windows Vista:

1. Clique em *Iniciar* > *Configurações* > *Painel de Controle* > *Contas de Usuário* > *Contas de Usuário* > *Ativar ou Desativar o Controle de Conta de Usuário*.
2. Anule a seleção de *Use User Account Control (UAC) to help protect your computer* (Utilizar o Controle de Conta de Usuário (UAC) para ajudar a proteger o computador).
3. Clique em *OK*.

Ação: Faça o seguinte para desativar o Controle de Conta de Usuário (UAC) no dispositivo Windows 7:

1. Clique em *Iniciar* > *Painel de Controle* > *Contas de Usuário* > > *Alterar Configurações de Controle de Conta de Usuário*.
2. Deslize a barra até o valor mais baixo (em direção a *Never Notify* (Nunca Notificar) com uma descrição que exibe Never notify me (Nunca me notificar).
3. Clique em *OK*.
4. Reinicie o dispositivo.

Impossível iniciar uma sessão remota no dispositivo SUSE Linux Enterprise Server 11 por meio do Mozilla Firefox

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: O plug-in do Gerenciamento Remoto para Firefox é instalado no diretório `/usr/lib/firefox`, que também é o diretório de instalação padrão do Firefox. Se você instalou o Firefox em um diretório diferente no dispositivo SLES 11, ocorrerá falha ao iniciar uma sessão remota pelo Firefox no dispositivo.

Ação: Copie o arquivo `nsZenworksPluginSample.so` do diretório `/usr/lib/firefox/plugins` para o diretório de plug-ins do Firefox.

O link Atualizar Viewer de Gerenciamento Remoto não aparece quando você inicia o ZENworks Control Center pelo Internet Explorer 8

Origem: ZENworks 10 Configuration Management; Gerenciamento Remoto.

Explicação: Se você fizer upgrade para o ZENworks Configuration Management SP3 a partir do ZENworks Configuration Management SP2 e iniciar o ZENworks Control Center pelo Internet Explorer 8, o link *Atualizar Viewer de Gerenciamento Remoto* não aparecerá no ZENworks Control Center.

Ação: Para ver o link *Atualizar Viewer de Gerenciamento Remoto*, realize as seguintes etapas:

1. Inicie o browser Internet Explorer 8.
2. Clique em *Ferramentas* > *Opções da Internet* para exibir a caixa de diálogo Opções da Internet.
3. Clique na guia *Segurança*.
4. Clique na opção *Nível personalizado*.
5. Verifique se as configurações a seguir estão habilitadas:
   - *Executar controles ActiveX e plug-ins*
   - *Inicializar e criar script de controles ActiveX não marcados como seguros para script*
6. Reinicie o browser.

Detalhes criptográficos

A

As seções a seguir contêm os detalhes sobre os vários certificados gerados durante a utilização do componente de Gerenciamento Remoto do Novell® ZENworks® 10 Configuration Management.

A.1 Detalhes de chave par do dispositivo gerenciado

Certificado gerado por: serviço de Gerenciamento Remoto
Certificado gerado usando: OpenSSL v0.9.8e (versão da Novell)
Certificado assinado por: auto-assinado
Certificado assinado usando: OpenSSL v0.9.8e (versão da Novell)
Certificado verificado por: viewer de Gerenciamento Remoto
Certificado verificado usando: OpenSSL v0.9.8e (versão da Novell)
Usado por: serviço de Gerenciamento Remoto
Usado para: estabelecer uma sessão segura com o viewer de Gerenciamento Remoto
Tipo de chave privada: RSA
Força da chave: 1024 bits
Algoritmo de assinatura: RSA-SHA256
Validade: 10 anos

A.2 Detalhes de chave par do operador remoto

Este certificado é válido apenas quando a CA Interna é implantada.

Certificado Gerado por: ZENworks Control Center hospedado pelo Servidor ZENworks
Certificado Gerado Usando: biblioteca Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificado Assinado por: ZENworks Control Center hospedado pelo Servidor ZENworks
Certificado Assinado Usando: Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificado Verificado por: serviço de Gerenciamento Remoto
Certificado Verificado Usando: OpenSSL v0.9.8e (versão da Novell)
Usado por: viewer de Gerenciamento Remoto e serviço de Gerenciamento Remoto
Usado para: estabelecer uma sessão segura e identificar o operador remoto
Tipo de Chave Privada: RSA
Força da Chave: 1024 bits
Algoritmo de Assinatura: RSA-SHA1
Validade: 4 dias

A.3 Detalhes do ticket de gerenciamento remoto

Este certificado é válido apenas para a Autenticação de Direitos.

Ticket Gerado por: ZENworks Control Center hospedado pelo Servidor ZENworks
Ticket Gerado Usando: biblioteca Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificado Assinado por: ZENworks Control Center hospedado pelo Servidor ZENworks
Ticket Assinado Usando: biblioteca Bouncy Castle (`bcprov-jdk15-134.jar`)
Certificado Verificado por: serviço Web de Gerenciamento Remoto (no Servidor ZENworks)
Certificado Verificado Usando: biblioteca Bouncy Castle (`bcprov-jdk15-134.jar`)
Usado por: viewer de Gerenciamento Remoto e serviço Web de Gerenciamento Remoto
Usado para: autenticar o operador remoto e verificar os direitos para executar uma operação
Algoritmo de Assinatura: RSA-SHA1
Validade: 2 minutos

A.4 Detalhes de criptografia da sessão

Sessão estabelecida entre: serviço de Gerenciamento Remoto e viewer de Gerenciamento Remoto
Protocolo de criptografia: SSL (TLSv1)
Código da sessão: AES256-SHA
Modo de autenticação SSL: mútuo/servidor

Melhores práticas

B

As seções a seguir explicam as melhores práticas a serem seguidas ao usar o componente de Gerenciamento Remoto do Novell® ZENworks® 10 Configuration Management.

B.1 Fechando a escuta do gerenciamento remoto

Quando um operador remoto lança a Escuta do Gerenciamento Remoto para escutar as solicitações de sessão remota do usuário do dispositivo gerenciado, o ZENworks emite um ticket para habilitar o operador remoto a autenticar o dispositivo gerenciado. A duração desse ticket é de dois dias.

A Escuta do Gerenciamento Remoto continua a ser executada mesmo depois que o operador remoto se desconecta ou fecha o ZENworks Control Center. Se o ticket ainda for válido, qualquer outro operador remoto poderá usar a escuta para escutar as solicitações de sessão remota dos usuários do dispositivo gerenciado. Para propósitos de segurança, você deve fechar a Escuta do Gerenciamento Remoto antes de se desconectar ou fechar o browser.

Para fechar a Escuta do Gerenciamento Remoto, clique o botão direito do mouse no ícone de *Escuta do Gerenciamento Remoto do ZENworks* na área de notificação e em *Fechar daemon de escuta*.

B.2 Fechando aplicativos iniciados durante a operação de execução remota

Por padrão, o módulo Gerenciamento Remoto funciona como um serviço com privilégios de sistema no dispositivo gerenciado. Assim, todos os aplicativos iniciados durante uma sessão de Execução Remota também são executados com privilégios de sistema. Por segurança, é altamente recomendável que você feche o aplicativo após o uso.

B.3 Identificando o operador remoto no dispositivo gerenciado

Quando um operador remoto inicia uma sessão remota em um dispositivo gerenciado por meio do ZENworks Control Center, um certificado que ajuda o dispositivo gerenciado a identificar o operador remoto será gerado automaticamente pelo ZENworks se uma CA interna for usada. No entanto, se uma CA externa for utilizada, o operador remoto terá que fornecer manualmente o certificado encadeado à CA externa implantada e será certificado para Autenticação de Cliente SSL. Para obter mais informações sobre o uso da CA externa, consulte *Usar o par de chaves a seguir para identificação* na Seção 2.8, “Iniciando as operações de gerenciamento remoto” na página 35.

Se um operador remoto iniciar uma operação remota em um dispositivo gerenciado sem fornecer um certificado, o nome desse operador remoto será registrado como *Usuário Desconhecido* nos registros de auditoria, na caixa de diálogo Sinal Visível e Pedir Permissão ao Usuário. Para assegurar que o operador remoto forneça o certificado, desmarque a opção *Permitir conexão quando o Console de Gerenciamento Remoto não tiver certificado SSL* na política de Gerenciamento Remoto.

B.4 Executando uma sessão de controle remoto em um dispositivo já conectado por meio de uma conexão à área de trabalho remota

Para controlar remotamente um dispositivo já conectado por meio de RDP (Remote Desktop Connection - Conexão à Área de Trabalho Remota), verifique o seguinte:

- A sessão de RDP está em andamento no dispositivo gerenciado
- O dispositivo gerenciado foi bloqueado manualmente após o fim da sessão de RDP do dispositivo.

B.5 Determinando o nome do console de gerenciamento

Se a opção *Pesquisar o nome do visualizador de DNS no início da sessão remota* estiver habilitada na política de Gerenciamento Remoto, o dispositivo gerenciado tentará determinar o nome do console de gerenciamento no início de uma sessão remota. Isso poderá causar um atraso significativo no início da sessão remota se a rede não tiver a pesquisa de DNS reversa habilitada. Para evitar esse atraso, desabilite a opção *Pesquisar o nome do visualizador de DNS no início da sessão remota* na política.

B.6 Usando o tema Aero nos dispositivos Windows Vista, Windows 7, Windows Server 2008 e Windows Server 2008 R2

Para aperfeiçoar o desempenho de uma sessão remota, o Gerenciamento Remoto usa um driver espelhado para detectar as mudanças na tela. Se o driver espelhado não for compatível com o tema da área de trabalho Aero, uma tentativa de carregar esse driver em um dispositivo que tenha esse

tema habilitado fará com que o tema padrão da área de trabalho seja usado no dispositivo. Isso poderá afetar a experiência do usuário, portanto, não é recomendável usar o tema Aero em um dispositivo que você queira gerenciar remotamente.

Se quiser manter o tema Aero durante a sessão remota do dispositivo gerenciado, desabilite o driver espelhado no dispositivo. Para desabilitar o driver espelhado, anule a seleção da configuração *Habilitar driver de otimização* no dispositivo. Para obter mais informações sobre a configuração Habilitar driver de otimização, consulte Configurando o gerenciamento remoto no nível de zona.

Entretanto, habilitar o tema Aero no dispositivo gerenciado pode reduzir o desempenho da sessão remota no dispositivo.

B.7 Habilitando o botão de seqüência de atenção segura (Ctrl+Alt+Del) ao controlar remotamente um dispositivo Windows Vista ou Windows Server 2008

Para habilitar o ícone  (Ctrl+Alt+Del) na barra de ferramentas do viewer de Gerenciamento Remoto ao controlar remotamente um dispositivo Windows Vista ou Windows Server 2008, verifique se o UAC (Controle de Conta de Usuário) está habilitado no dispositivo gerenciado.

B.8 Instalando o serviço de gerenciamento remoto em um dispositivo Windows XP por meio de RDP

Durante a instalação do Serviço de Gerenciamento Remoto em um dispositivo gerenciado, o ZENworks instala automaticamente um driver espelhado denominado DFMirage no dispositivo. Para instalar o serviço de Gerenciamento Remoto em um dispositivo Windows XP por meio de uma sessão de RDP (Conexão à Área de Trabalho Remota), verifique se o patch fornecido no site de Suporte da Microsoft na Web (http://support.microsoft.com/kb/952132) está instalado no dispositivo.

B.9 Desempenho de gerenciamento remoto

O desempenho em um link lento ou rápido durante uma sessão de Gerenciamento Remoto varia conforme o tráfego da rede. Para obter um tempo de resposta melhor, consulte a Seção 3.8, “Melhorando o desempenho do gerenciamento remoto” na página 65.

Atualizações da documentação

C

Esta seção contém informações sobre as mudanças feitas no conteúdo da documentação desta *Referência de Gerenciamento Remoto do ZENworks* para o Novell® ZENworks® 10 Configuration Management SP3. As informações ajudarão o usuário a se manter atualizado em relação à documentação.

A documentação deste produto é fornecida na Web em dois formatos: HTML e PDF. Ambos os formatos estão atualizados com relação às mudanças listadas nesta seção.

Para você saber se uma cópia da documentação em PDF usada é a mais recente, verifique a data de publicação na página do título do documento em PDF.

Foram feitas a seguintes atualizações no documento:

- Seção C.1, “30 de março de 2010: SP3 (10.3)” na página 91

C.1 30 de março de 2010: SP3 (10.3)

Foram feitas atualizações nas seguintes seções:

Local	Mudança
“Proxy de Gerenciamento Remoto” na página 12	A seção foi atualizada.
Seção 1.3, “Compreendendo os recursos de gerenciamento remoto” na página 15	A seção foi atualizada.
Seção 2.5, “Configurando a senha de gerenciamento remoto” na página 31	A seção foi atualizada.
Seção 2.9, “Opções para iniciar uma operação de gerenciamento remoto” na página 45	A seção foi adicionada.
Seção 2.10, “Instalando um proxy de gerenciamento remoto” na página 49	Seção atualizada para adicionar o suporte à instalação do proxy de Gerenciamento Remoto no Linux.
Seção 2.11, “Configurando um proxy de gerenciamento remoto” na página 50	A seção foi adicionada.
Seção 3.7, “Ativando um dispositivo remoto” na página 63	Seção atualizada para adicionar informações sobre como acionar um dispositivo que tem vários NICs.
Seção 3.6, “Gerenciando uma sessão de proxy de gerenciamento remoto” na página 63	A seção foi adicionada.

Local	Mudança
Capítulo 5, “Guias de solução de problemas” na página 75	Os seguintes cenários foram adicionados: ◆ “Impossível iniciar uma sessão remota no dispositivo SUSE Linux Enterprise Server 11 por meio do Mozilla Firefox” na página 82 ◆ “O link Atualizar Viewer de Gerenciamento Remoto não aparece quando você inicia o ZENworks Control Center pelo Internet Explorer 8” na página 83
Capítulo 5, “Guias de solução de problemas” na página 75	O seguinte cenário foi adicionado: Impossível transferir arquivos remotamente para as pastas restritas em um dispositivo Windows Vista ou Windows 7
Seção B.6, “Usando o tema Aero nos dispositivos Windows Vista, Windows 7, Windows Server 2008 e Windows Server 2008 R2” na página 88	A seção foi atualizada.