AUTHORIZED DOCUMENTATION

Guia de Instalação

January 5, 2009

Novell®
ZENworks® Endpoint Security Management

3.5

www.novell.com

Informações Legais

A Novell, Inc. não faz representações ou garantias quanto ao conteúdo ou à utilização desta documentação e especificamente se isenta de quaisquer garantias de comerciabilidade expressas ou implícitas ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de revisar esta publicação e fazer mudanças em seu conteúdo, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade sobre essas revisões ou mudanças.

Além disso, a Novell, Inc. não faz representações nem garantias com relação a qualquer software, e se isenta de quaisquer garantias de comerciabilidade expressas ou implícitas ou adequação a qualquer propósito específico. A Novell, Inc. reserva-se o direito de fazer mudanças em qualquer e em todas as partes do software Novell, a qualquer momento, sem a obrigação de notificar qualquer pessoa ou entidade sobre essas mudanças.

Quaisquer informações técnicas ou sobre produtos fornecidas de acordo com este Contrato estão sujeitas aos controles de exportação dos EUA e às leis comerciais de outros países. Você concorda em cumprir todos os regulamentos do controle de exportação e em obter as licenças ou a classificação necessárias para exportar, reexportar ou importar produtos finais. Você concorda em não exportar nem reexportar para entidades que constam nas listas de exclusão de exportação atual dos EUA ou para qualquer país embargado ou terrorista conforme especificado nas leis de exportação dos EUA. Você concorda em não usar produtos para fins proibidos relacionados a armas nucleares, biológicas e químicas ou mísseis. Consulte a página International Trade Services da Novell na Web (http://www.novell.com/info/exports/) para obter mais informações sobre como exportar softwares da Novell. A Novell não se responsabiliza pela falha em obter as aprovações necessárias para exportação.

A Novell, Inc. é titular de direitos de propriedade intelectual relativos à tecnologia incorporada no produto descrito neste documento. Especificamente e sem limitações, esses direitos de propriedade intelectual podem incluir uma ou mais das patentes dos EUA listadas na página de patentes legais da Novell na Web (http://www.novell.com/company/legal/patents/) e uma ou mais patentes adicionais ou aplicativos com patente pendente nos EUA e em outros países.

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

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

Marcas registradas da Novell

Para conhecer as 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

Este *Guia de Instalação do Novell® ZENworks® Endpoint Security Management* fornece instruções de instalação completas para os componentes do ZENworks Endpoint Security Management e ajuda os administradores a colocar esses componentes em execução.

As informações deste guia estão organizadas da seguinte maneira:

Público

Este guia foi escrito para os administradores do ZENworks Endpoint Security Management.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no GroupWise. 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

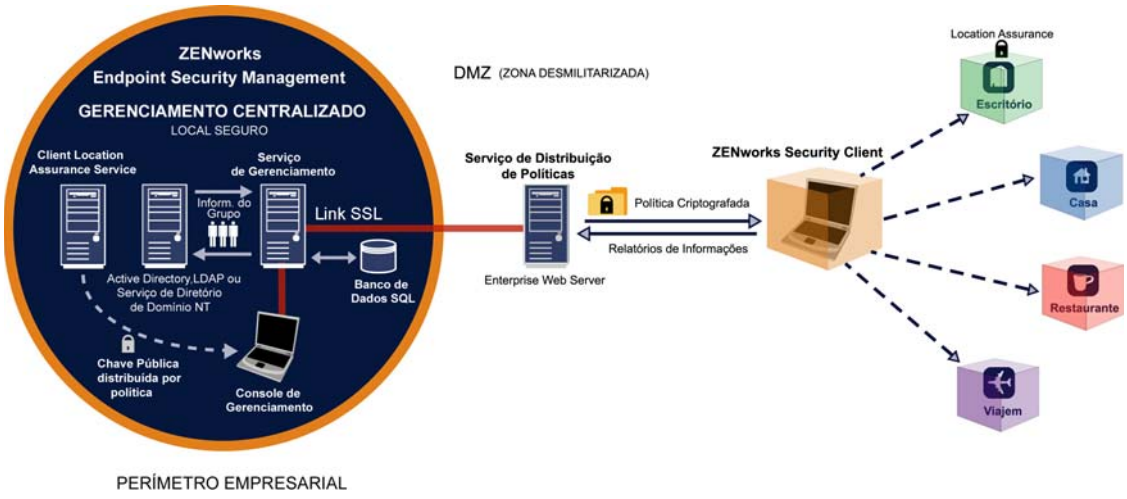
O ZENworks Endpoint Security Management é suportado por documentação adicional (nos formatos PDF e HTML), que pode ser utilizada para que você conheça e implemente o produto. Para obter mais informações, consulte o site de documentação do ZENworks Endpoint Security Management 3.5 na web (http://www.novell.com/documentation/zesm35).

Visão geral sobre o ZENworks Endpoint Security Management

1

O Novell® ZENworks® Endpoint Security Management consiste em cinco componentes funcionais de alto nível: Serviço de Distribuição de Política, Serviço de Gerenciamento, Console de Gerenciamento, Client Location Assurance Service e Endpoint Security Client. A figura a seguir mostra esses componentes na arquitetura:

Figura 1-1 *Arquitetura do ZENworks Endpoint Security Management*



O Endpoint Security Client é responsável por assegurar o uso obrigatório das políticas de segurança distribuídas no sistema de pontos de extremidade. Agora, quando o Endpoint Security Client é instalado em todos os PCs da empresa, esses pontos de extremidade podem passar por fora do perímetro corporativo e manter sua segurança; os pontos de extremidade dentro do perímetro recebem verificações de segurança adicionais dentro do firewall do perímetro.

Cada componente de gerenciamento central é instalado separadamente (com exceção da instalação de servidor único). Consulte a Capítulo 3, “Executando uma instalação de Servidor Único” na página 17 para obter detalhes.

Os seguintes componentes são instalados em servidores protegidos dentro do perímetro corporativo:

- **Serviço de Distribuição de Política:** Responsável pela distribuição de políticas de segurança no Endpoint Security Client e pela recuperação de dados de relatório do Endpoint Security Client. O Serviço de Distribuição de Política pode ser implantado na DMZ, fora do firewall corporativo, para garantir atualizações regulares de política nos pontos de extremidade móveis.
- **Serviço de Gerenciamento:** Responsável pela atribuição de políticas de usuário e autenticação de componentes; pela recuperação de dados do gerador de relatórios; pela criação e disseminação de relatórios do ZENworks Endpoint Security Management; e pela criação e armazenamento de políticas de segurança.
- **Console de Gerenciamento:** A interface de usuário visível, executada diretamente no servidor que hospeda o Serviço de Gerenciamento ou em uma estação de trabalho que reside dentro do firewall corporativo com conexão com o servidor do Serviço de Gerenciamento. O Console de

Gerenciamento é usado para configurar o Serviço de Gerenciamento e para criar e gerenciar as políticas de segurança de usuários e grupos. As políticas são criadas, copiadas, editadas, disseminadas e apagadas no Console de Gerenciamento.

- **Client Location Assurance Service:** Fornece uma garantia criptográfica de que dispositivos com o Endpoint Security Client instalado realmente estejam em um local definido, conforme indicado por outros parâmetros de ambiente de rede existentes.

1.1 Requisitos do sistema

Requisitos do sistema do servidor	Requisitos do sistema de pontos de extremidade (cliente)
Sistemas operacionais:	**Sistemas operacionais:**
Microsoft&thrdmrk; Windows&thrdmrk; 2000 Server SP4 Microsoft Windows 2000 Advanced Server SP4 Windows 2003 Server	Windows XP SP1 Windows XP SP2 Windows 2000 SP4 Windows Vista SP1 (32 bits) Windows Server 2008 (32 bits)
Processador:	**Processador:**
Pentium&thrdmrk; de 3.0 GHz 4 HT (ou superior) Mínimo de 756 MB de RAM (é recomendável mais de 1 GB)	Pentium 3 de 600MHz (ou superior) RAM mínima de 128 MB (256 MB ou mais recomendados)
Espaço em disco:	**Espaço em disco:**
500 MB - sem banco de dados SQL Microsoft local 5 GB - com banco de dados SQL MS local (SCSI é recomendado)	5 MB exigidos, 5 MB adicionais recomendados para reportar dados
Software necessário:	**Software necessário:**
RDBMS suportado (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005) Serviços de Informações da Internet da Microsoft (configurado para SSL) Serviços de diretório suportados (eDirectory™ ou Active Directory&thrdmrk;) .NET framework 3.5 (apenas para os servidores e para o Console de Gerenciamento)	Windows 3.1 Installer Todas as atualizações do Windows devem estar em dia
Console de Gerenciamento independente:	
RDBMS suportado (SQL Server Standard, SQL Server Enterprise, Microsoft SQL Server 2000 SP4, SQL 2005, SQL Express)	

Os serviços de Distribuição de Política, Gerenciamento e Client Location Assurance exigem que uma conta local do ASP.NET 2.0 seja habilitada. Se a conta estiver desabilitada, os serviços não funcionarão corretamente.

1.2 Sobre os manuais do ZENworks Endpoint Security Management

Os manuais do ZENworks Endpoint Security Management fornecem três níveis de orientação para os usuários do produto.

- *Guia de Instalação do ESM:* Esse guia fornece instruções completas para a instalação dos componentes do ZENworks Endpoint Security Management e ajuda os administradores a colocar esses componentes em execução. Esse é o guia que você está lendo agora.
- *Guia de Administração do ZENworks Endpoint Security Management*: Esse guia foi escrito para os administradores do ZENworks Endpoint Security Management, que são responsáveis por gerenciar os serviços, criar políticas de segurança para a empresa, gerar e analisar dados de relatórios e fornecer solução de problemas para os usuários. Nesse manual, são fornecidas instruções para concluir essas tarefas.
- *Guia do Usuário do ZENworks Endpoint Security Client 3.5*: Esse guia foi escrito para instruir o usuário sobre o funcionamento do Endpoint Security Client. Esse guia pode ser enviado a todos os funcionários da empresa para ajudá-los a entender o Endpoint Security Client.

Instalando o ZENworks Endpoint Security Management

2

As seções a seguir contêm informações adicionais sobre a instalação do Novell® ZENworks® Endpoint Security Manager:

2.1 Informações de pré-instalação

O software de instalação do ZENworks Endpoint Security Management deve ser protegido fisicamente para evitar qualquer falsificação ou uso não-autorizado. Do mesmo modo, os administradores devem examinar as diretrizes de pré-instalação e instalação para garantir que o sistema do ZENworks Endpoint Security Management funcione sem interrupções ou que não fique vulnerável devido à proteção inadequada do hardware.

O administrador que está instalando este software deve ser o administrador principal dos servidores e do domínio. Se estiver usando certificados SSL corporativos, você também deverá utilizar o mesmo nome de usuário para criar o certificado de segurança raiz do SSL.

2.2 Pacotes de instalação

Quando a instalação é realizada pelo DVD, um programa de instalação master com uma interface do usuário simples é iniciado para orientar o administrador do ZENworks Endpoint Security Management durante o processo de instalação. Carregue o DVD de instalação em cada máquina para acessar o programa de instalação master e instalar os componentes desejados.

2.2.1 Sobre o programa de instalação master

Ao ser iniciado, o programa de instalação master exibe duas opções de menu: *Produtos* e *Documentação*.

O link *Produtos* abre o menu de instalação. Os itens de menu nessa tela iniciam o programa de instalação designado para cada componente. No caso do Endpoint Security Client 3.5 ou do Endpoint Security Client 4.0, uma opção adicional está disponível para iniciar a instalação no Modo de Administrador, o que ajudará o administrador do ZENworks Endpoint Security Management a criar um pacote MSI para facilitar a distribuição. (Consulte Capítulo 9.2, “Instalação MSI” na página 61.)

Para obter informações sobre a operação completa dos componentes do ZENworks Endpoint Security Management, consulte o *Guia de Administração do ZENworks Endpoint Security Management*, que pode ser obtido pelo link *Documentação*.

2.3 Opções de Instalação

Os componentes back end do ZENworks Endpoint Security Management podem ser instalados em instalações de Servidor Único ou em instalações de Vários Servidores. Instalações de Servidor Único são ideais para pequenas implantações que não exigem atualizações regulares de política. Instalações de Vários Servidores são ideais para grandes implantações que exigem atualizações regulares de política. Consulte Serviços Profissionais da Novell para determinar que tipo de instalação é melhor para você.

O Endpoint Security Client pode funcionar (quando necessário) sem conectividade com o Serviço de Distribuição de Política. Dessa maneira, um Console de Gerenciamento Independente pode ser instalado opcionalmente para fins de avaliação. A instalação desse modo de operação Não Gerenciado está descrita no Capítulo 11, "Instalação não gerenciada do ZENworks Endpoint Security Management" na página 75.

2.4 Ordem de instalação

O ZENworks Endpoint Security Management deve ser instalado na seguinte ordem:

1. Instalação de Servidor Único ou Instalação de Vários Servidores
   - Serviço de Distribuição de Política
   - Serviço de Gerenciamento
2. Console de Gerenciamento
3. Client Location Assurance Service
4. Endpoint Security Client 3.5 ou Endpoint Security Client 4.0

2.5 Antes de instalar o ZENworks Endpoint Security Management

Existem algumas questões que o administrador do ZENworks Endpoint Security Management deve considerar antes de iniciar a instalação:

Como os usuários receberão as políticas de segurança do ZENworks Endpoint Security Management?

As opções de distribuição de políticas baseiam-se no seguinte: os usuários podem receber uma atualização de política em qualquer lugar, inclusive fora da rede central; ou os usuários só podem receber uma atualização de política quando estão em (ou conectados por VPN a) uma rede protegida. Para as organizações que planejam atualizar com freqüência as políticas de segurança do ZENworks Endpoint Security Management, é recomendável uma instalação de Vários Servidores que coloque o Serviço de Distribuição de Política em um servidor Web fora da DMZ.

Quais tipos de implantações de servidor estão disponíveis para você?

Se sua organização tiver apenas alguns servidores disponíveis, poderá ser necessária uma implantação de instalação de Servidor Único. Se a disponibilidade do servidor não for um problema, deverão ser levados em consideração o tamanho da sua implantação de clientes e o número de usuários que trabalham fora do firewall.

Qual é a implantação de SQL Server disponível?

O ZENworks Endpoint Security Management cria três bancos de dados SQL na instalação. Se sua implantação for pequena, um único banco de dados SQL ou um banco de dados de servidor pode ser instalado nos servidores do Serviço de Gerenciamento e de Distribuição de Política. Para implantações grandes, um servidor de banco de dados SQL separado deve ser usado para receber os dados dos Serviços de Gerenciamento e de Distribuição de Política. Somente os seguintes tipos de RDBMS são permitidos:

- SQL Server Standard
- SQL Server Enterprise
- Microsoft SQL Server 2000 SP4

Em caso de instância nomeada, a configuração dos servidores deve ser a seguinte:

Provedor=sqloledb

Fonte de Dados=ServerName\InstanceName (esse tipo de definição é necessário para que o ZENworks Endpoint Security Management seja instalado)

Catálogo Inicial=Nome_do_banco_de_dados

Id do Usuário=Nome_de_usuário

Senha=Senha

Defina a SQL para o modo misto.

O nome de usuário e a senha usados na instalação não podem ser um usuário de domínio; devem ser um usuário SQL com direitos SysAdmin.

Você usará certificados existentes para estabelecer a comunicação SSL ou usará Certificados Auto-assinados da Novell?

Para recuperação de desastre e designs de failover, use certificados SSL da Autoridade de Certificação (VeriSign, GeoTrust, Thawte, etc.) corporativos, ou emitidos de outra forma, para implantações completas do ZENworks Endpoint Security Management. Quando você usa seus próprios certificados, os certificados de serviço Web e de CA raiz devem ser criados na máquina designada como o Serviço de Distribuição de Política e distribuídos para as máquinas apropriadas. Para criar uma Autoridade de Certificação Corporativa, consulte as instruções passo-a-passo para configurar corretamente a autoridade de certificação. Para obter essas instruções, visite o site da Microsoft.

Para avaliações ou pequenas implantações (menos de 100 usuários), use os certificados auto-assinados do ZENworks Endpoint Security Management. Os Certificados SSL da Novell são instalados nos servidores quando a instalação típica é executada.

Como você implantará os Endpoint Security Clients?

O software Endpoint Security Client pode ser implantado de forma individual em cada ponto de extremidade ou por meio de um servidor push MSI. As instruções sobre a criação de um pacote MSI podem ser encontradas no Capítulo 9.2, “Instalação MSI” na página 61.

Deseja que as políticas sejam baseadas em máquina ou em usuário?

As políticas podem ser distribuídas para uma única máquina, onde cada usuário que efetuar login receberá a mesma política, ou podem ser definidas para usuários individuais ou grupos.

Cada instalação possui diversos pré-requisitos. É recomendável que cada lista de verificação de pré-requisitos seja preenchida antes da execução da instalação dos componentes. Reveja as listas nas seguintes páginas:

- Capítulo 3, “Executando uma instalação de Servidor Único” na página 17
- Capítulo 5, “Executando a instalação do Serviço de Distribuição de Política” na página 23
- Capítulo 6, “Executando a instalação do Serviço de Gerenciamento” na página 31
- Capítulo 7, “Executando a instalação do Console de Gerenciamento” na página 43
- Capítulo 8, “Executando a instalação do Client Location Assurance Service” na página 55
- Capítulo 9, “Instalação do Endpoint Security Client 3.5” na página 59

Executando uma instalação de Servidor Único

3

A SSI (Single Server Installation - Instalação de Servidor Único) do ZENworks® Endpoint Security Management permite que o Serviço de Distribuição de Política e o Serviço de Gerenciamento coexistam no mesmo servidor, o que não é possível sem o uso dessa opção de instalação. Por motivos de segurança, o servidor deve ser distribuído dentro do firewall; os usuários só deverão receber atualizações de política quando estiverem dentro da infra-estrutura corporativa ou conectados por uma VPN.

A implantação da Instalação de Servidor Único em um PDC (Primary Domain Controller - Controlador de Domínio Primário) não é suportada por razões de segurança e funcionalidade.

Observa o: É recomendado que o Servidor SSI seja configurado (reforçado) para desativar todos os aplicativos, serviços, contas e outras opções desnecessárias para a funcionalidade destinada do servidor. As etapas envolvidas dependem das especificações do ambiente local e, portanto, não podem ser descritas antecipadamente. Os administradores são avisados para consultar a seção apropriada da página da Web de segurança Microsoft TechNet (http://www.microsoft.com/technet/security/default.mspx). Recomendações adicionais de controle de acesso são fornecidas no *Guia de Administração do ZENworks Endpoint Security Management*.

Para restringir o acesso a máquinas confiáveis, configure o diretório virtual e o IIS para ter ACLs. Consulte os artigos a seguir:

- Granting and Denying Access to Computers (Concedendo e negando o acesso a computadores) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (Restringir o acesso a site por endereço IP ou nome de domínio) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (FAQ do IIS: Restrições de endereço IP 2000 e nome de domínio) (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (Trabalhando com filtragem de pacotes do IIS) (http://www.15seconds.com/issue/011227.htm)

Por motivos de segurança, é altamente recomendável que as seguintes pastas padrão sejam removidas de qualquer instalação do IIS:

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Impressoras`

Também recomendamos o uso da ferramenta IIS Lockdown Tool 2.1 disponível em microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

A versão 2.1 é orientada por gabaritos fornecidos para os principais produtos Microsoft dependentes do IIS. Selecione o gabarito que melhor corresponda à função deste servidor. Em caso de dúvida, o gabarito de servidor Web Dinâmico é recomendado.

Antes de iniciar a instalação, verifique se os seguintes pré-requisitos são atendidos:

- ❑ Verifique se há acesso a um serviço de diretório suportado (eDirectory™, Active Directory ou Domínios NT). Domínios NT só são suportados quando o Serviço de Servidor Único está instalado em um Microsoft Windows 2000 Advanced Server (SP4).
- ❑ Se estiver realizando a implantação com um serviço eDirectory, verifique se o Novell Client™ está instalado no servidor e se pode autenticar corretamente no eDirectory. Crie uma senha de conta que nunca mude para usar na autenticação do Console de Gerenciamento. (Consulte a Seção 7.2.1, “Adicionando serviços do eDirectory” na página 47.)
- ❑ Para a resolução de nome de servidor do Endpoint Security Client para Servidor Único, verifique se os computadores de destino (em que o Endpoint Security Client está instalado) podem realizar ping no nome do servidor SSI. Se não obtiver êxito, você deverá resolver isso antes de continuar com a instalação. (Mude o nome do servidor SSI para FQDN/NETBIOS, mude AD para usar FQDN/NETBIOS, mude as configurações de DNS, modificando o arquivo host local nos computadores de destino para incluir as informações de MS corretas, etc.)
- ❑ Habilite ou instale o IIS (Serviços de Informações da Internet) da Microsoft e configure-o para aceitar Certificados SSL (Secure Socket Layer).

  Importante: Não marque a caixa de seleção *Exigir canal de segurança (SSL)* na página Comunicações de Segurança. (No utilitário Gerenciamento do Computador da Microsoft, expanda *Serviços e Aplicativos* > expanda *Gerenciador dos Serviços de Informações da Internet (ISS)* > expanda *Sites* > clique o botão direito do mouse em *Site Padrão* > clique em *Propriedades* > clique na guia *Segurança de Diretório* > clique no botão *Editar* na caixa de grupo Comunicações de segurança.) A habilitação dessa opção interrompe a comunicação entre o servidor e o cliente ZENworks Endpoint Security Management no ponto de extremidade.

- ❑ Se estiver usando seus próprios certificados SSL, verifique se o certificado de serviço Web e a CA raiz estão carregados na máquina e se o nome do servidor validado nas etapas anteriores (NETBIOS ou FQDN) corresponde ao valor *Emitido para* do certificado configurado no IIS.
- ❑ Se estiver usando seus próprios certificados ou se já tiver instalado o Certificado Auto-assinado da Novell, você também poderá validar o SSL experimentando o seguinte URL em uma máquina que tenha o Endpoint Security Client instalado:`https://`*`NOME_DO_SERVIDOR_SSI`*`/AuthenticationServer/UserService.asmx` (onde *NOME_DO_SERVIDOR_SSI* é o nome do servidor). Isso retornará dados válidos (uma página html), e não avisos de certificado. Todos os avisos de certificado devem ser resolvidos antes da instalação, a menos que você opte por usar Certificados Auto-assinados da Novell.
- ❑ Verifique o acesso a um RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise) suportado. Defina o banco de dados para o modo Misto.

3.1 Etapas de instalação

Selecione *Instalação de Servidor Único* no menu do programa de instalação master. Essa instalação combina as instalações do Serviço de Distribuição de Política e do Serviço de Gerenciamento. Para obter mais informações, consulte Capítulo 5, “Executando a instalação do Serviço de Distribuição de Política” na página 23 e Capítulo 6, “Executando a instalação do Serviço de Gerenciamento” na página 31.

Como suas instalações individuais, a configuração *Típica* instala os padrões dos serviços e os certificados SSL auto-assinados da Novell. *A instalação Personalizada permitirá ao administrador determinar os caminhos de diretório e usar uma autoridade de certificação de propriedade da empresa.*

3.2 Iniciando o serviço

A combinação dos Serviços de Distribuição e Gerenciamento é iniciada imediatamente após a instalação, sem que seja necessário reinicializar o servidor. Por meio do recurso Configuração, o Console de Gerenciamento é usado para gerenciar tanto o Serviço de Gerenciamento quanto o de Distribuição. Para obter mais informações, consulte o *Guia de Administração do ZENworks Endpoint Security Management*.

Depois que a instalação for concluída, o Console de Gerenciamento e o Client Location Assurance Service poderão ser instalados nesse servidor. Se quiser instalar o Console de Gerenciamento em uma máquina separada, copie a pasta ZENworks Endpoint Security Management Setup Files para a máquina designada do Console de Gerenciamento para concluir a instalação.

Continue na Capítulo 5, “Executando a instalação do Serviço de Distribuição de Política” na página 23.

Executando uma instalação de Vários Servidores

4

A instalação de Vários Servidores é recomendada para grandes implantações ou quando o Serviço de Distribuição de Política deve ser colocado fora do firewall corporativo para garantir que os usuários recebam atualizações regulares de política quando estiverem fora do perímetro. A instalação de Vários Servidores deve ser realizada em pelo menos dois servidores separados. Se tentar instalar o Serviço de Distribuição de Política e o Serviço de Gerenciamento separados no mesmo servidor, ocorrerá falha na instalação. Para obter mais informações sobre a instalação de servidor único, consulte o Capítulo 3, “Executando uma instalação de Servidor Único” na página 17.

A instalação de Vários Servidores deve começar com a instalação do Serviço de Distribuição de Política em um servidor protegido dentro ou fora do firewall corporativo. Para obter mais informações, consulte Capítulo 5, “Executando a instalação do Serviço de Distribuição de Política” na página 23.

Depois que o Serviço de Distribuição de Política for instalado, a instalação do Serviço de Gerenciamento também deverá ser realizada. Para obter mais informações, consulte Capítulo 6, “Executando a instalação do Serviço de Gerenciamento” na página 31.

É recomendável que o Console de Gerenciamento também seja instalado nesse servidor. Para obter mais informações, consulte a Capítulo 7, “Executando a instalação do Console de Gerenciamento” na página 43.

Continue na Capítulo 5, “Executando a instalação do Serviço de Distribuição de Política” na página 23.

Executando a instalação do Serviço de Distribuição de Política

5

O servidor que está hospedando o Serviço de Distribuição de Política do ZENworks® Endpoint Security Management deve estar sempre acessível aos usuários, seja pela rede ou externamente na DMZ. Antes da instalação, verifique se o software necessário está instalado no servidor. (Consulte "Requisitos do sistema" na página 10.) Após selecionar o servidor, anote o nome do servidor, tanto o NETBIOS quanto o FQDN (nome completo do domínio).

A implantação do Serviço de Distribuição de Política em um PDC (Primary Domain Controller - Controlador de Domínio Primário) não é suportada por razões de segurança e funcionalidade.

Observa o: É recomendado que o Servidor SSI seja configurado (reforçado) para desativar todos os aplicativos, serviços, contas e outras opções desnecessárias para a funcionalidade destinada do servidor. As etapas envolvidas dependem das especificações do ambiente local e, portanto, não podem ser descritas antecipadamente. Os administradores são avisados para consultar a seção apropriada da página da Web de segurança Microsoft TechNet (http://www.microsoft.com/technet/security/default.mspx). Recomendações adicionais de controle de acesso são fornecidas no *Guia de Administração do ZENworks Endpoint Security Management*.

Para restringir o acesso a máquinas confiáveis, configure o diretório virtual e o IIS para ter ACLs. Consulte os artigos a seguir:

- Granting and Denying Access to Computers (Concedendo e negando o acesso a computadores) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (Restringir o acesso a site por endereço IP ou nome de domínio) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (FAQ do IIS: Restrições de endereço IP 2000 e nome de domínio) (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (Trabalhando com filtragem de pacotes do IIS) (http://www.15seconds.com/issue/011227.htm)

Por motivos de segurança, é altamente recomendável que as seguintes pastas padrão sejam removidas de qualquer instalação do IIS:

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Impressoras`

Também recomendamos o uso da ferramenta IIS Lockdown Tool 2.1 disponível em microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

A versão 2.1 é orientada por gabaritos fornecidos para os principais produtos Microsoft dependentes do IIS. Selecione o gabarito que melhor corresponda à função deste servidor. Em caso de dúvida, o gabarito de servidor Web Dinâmico é recomendado.

Verifique os seguintes pré-requisitos antes de iniciar a instalação:

- Verifique a resolução de nome do servidor MS (Serviço de Gerenciamento) para DS (Serviço de Distribuição de Política): confirme se o computador de destino em que o MS está instalado pode realizar ping no nome do servidor DS (NETBIOS se o DS for configurado dentro do firewall de rede ou FQDN se for instalado fora, na DMZ).
- Se você obtiver êxito, esse será o nome do servidor a ser inserido durante a instalação. Se não obtiver êxito, você deverá solucionar esse problema antes de continuar com a instalação.
- Verifique a resolução de nome do servidor Endpoint Security Client para DS: confirme se os clientes de pontos de extremidade (onde o Endpoint Security Client está instalado) podem realizar ping no mesmo nome de servidor DS usado anteriormente. Se não obtiver êxito, você deverá solucionar esse problema antes de continuar com a instalação.
- Habilite ou instale o IIS (Serviços de Informações da Internet) da Microsoft, verifique se o ASP.NET está habilitado e configure-o para aceitar Certificados SSL (Secure Socket Layer).

  Importante: Não marque a caixa de seleção *Exigir canal de segurança (SSL)* na página Comunicações de Segurança. (No utilitário Gerenciamento do Computador da Microsoft, expanda *Serviços e Aplicativos* > expanda *Gerenciador dos Serviços de Informações da Internet (ISS)* > expanda *Sites* > clique o botão direito do mouse em *Site Padrão* > clique em *Propriedades* > clique na guia *Segurança de Diretório* > clique no botão *Editar* na caixa de grupo Comunicações de segurança.) A habilitação dessa opção interrompe a comunicação entre o servidor e o cliente ZENworks Endpoint Security Management no ponto de extremidade.

- Se estiver usando seus próprios certificados SSL, verifique se o certificado de serviço Web está carregado na máquina e se o nome do servidor validado nas etapas anteriores (NETBIOS ou FQDN) corresponde ao valor *Emitido para* do certificado configurado no IIS.
- Se estiver usando seus próprios certificados SSL, valide o SSL do servidor MS para o servidor DS: abra um browser da Web no Serviço de Gerenciamento e digite o seguinte URL: `https://`*`NOMEDS`* (onde *NOMEDS* é o nome de servidor do DS). Isso retornará dados válidos, e não avisos de certificado (dados válidos podem ser "Página em Construção"). Todos os avisos de certificado devem ser resolvidos antes da instalação, a menos que você opte por usar Certificados Auto-assinados da Novell.
- Verifique o acesso a um RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL Server 2005) suportado. Defina o banco de dados para o modo Misto. Esse banco de dados deve estar hospedado no servidor Serviço de Gerenciamento ou em um servidor compartilhado protegido pelo firewall da empresa.

5.1 Etapas de instalação

Clique em *Instalação do Serviço de Distribuição de Política* no menu da interface de Instalação. A instalação do Serviço de Distribuição de Política é iniciada.

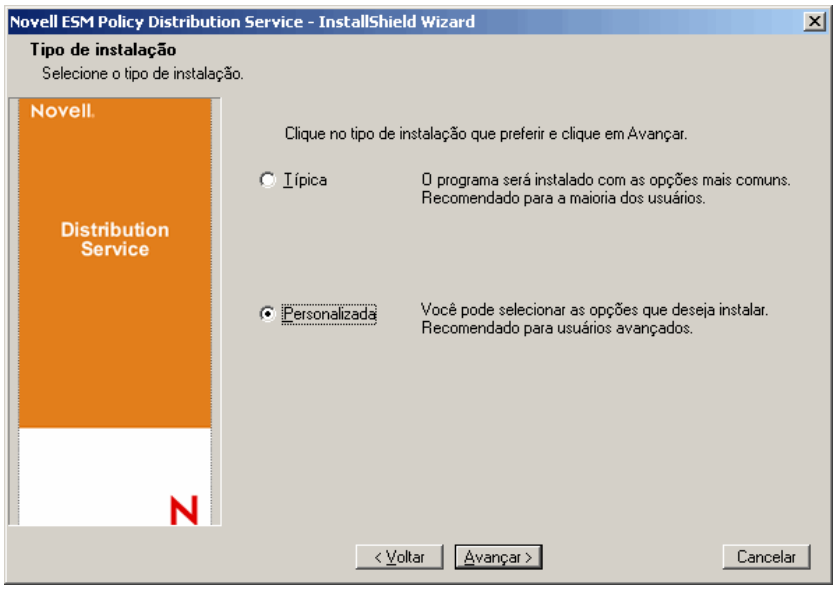
Na inicialização, o programa de instalação verifica se todos os softwares necessários estão presentes no servidor. Se algum software estiver ausente, ele será instalado automaticamente antes que a instalação prossiga para a tela de boas-vindas (talvez seja necessário aceitar os contratos de licença dos softwares adicionais). Se for necessário instalar o MDAC (Microsoft Data Access Components) 2.8, o servidor deverá ser reinicializado após instalação desse recurso e antes da conclusão da instalação do ZENworks Endpoint Security Management. Se você estiver usando o Windows 2003 Server, o ASP.NET 2.0 será configurado para ser executado pelo programa de instalação.

Após o início da instalação do Serviço de Distribuição de Política, siga estas etapas:

Observa o: As etapas a seguir descrevem o que você, o administrador, precisa fazer para concluir o processo de instalação. Os processos internos serão exibidos durante a instalação e não serão documentados aqui, a menos que haja uma ação ou uma informação específica que seja necessária para o êxito da instalação.

1. Clique em *Avançar* na tela de boas-vindas para continuar.
2. Aceite o Contrato de Licença e clique em *Avançar*.
3. Selecione a instalação *Típica* ou *Personalizada*.

Figura 5-1 *Selecionar instalação Típica ou Personalizada*



Ambos os caminhos de instalação são apresentados a seguir:

- Seção 5.1.1, “Instalação Típica” na página 25
- Seção 5.1.2, “Instalação Personalizada” na página 27

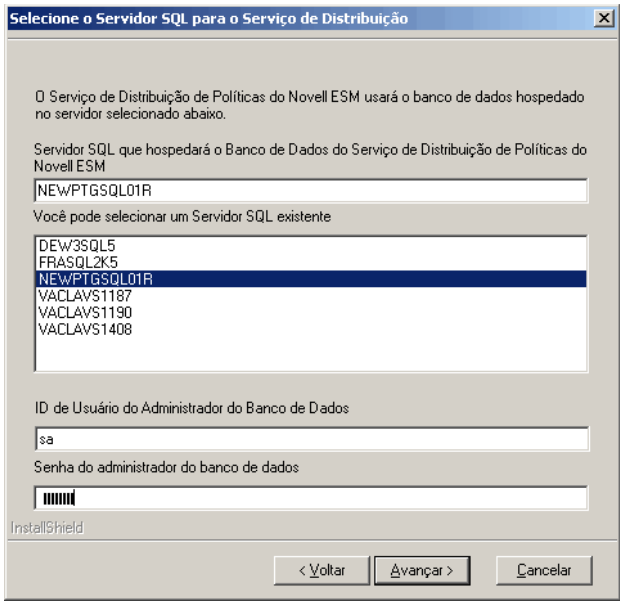
5.1.1 Instalação Típica

A instalação típica coloca os arquivos do software de Serviço de Distribuição de Política no diretório padrão: `\Arquivos de Programas\Novell\ESM Policy Distribution Service`. O nome do banco de dados SQL é atribuído como STDSDB. Os três arquivos do banco de dados SQL (data, index e log) são colocados em: `\Arquivos de Programas\Microsoft SQL Server\mssql\Data`.

1. Os Certificados SSL da Novell são criados para a instalação. Se quiser usar seus próprios certificados SSL, escolha a Instalação Personalizada. Esses certificados devem ser distribuídos para todos os usuários.
2. O programa de instalação detecta os bancos de dados SQL disponíveis na máquina e na rede. Selecione um banco de dados SQL protegido para o Serviço de Distribuição de Política e digite o nome e a senha do administrador do banco de dados (se a senha não tiver nenhum caractere, o

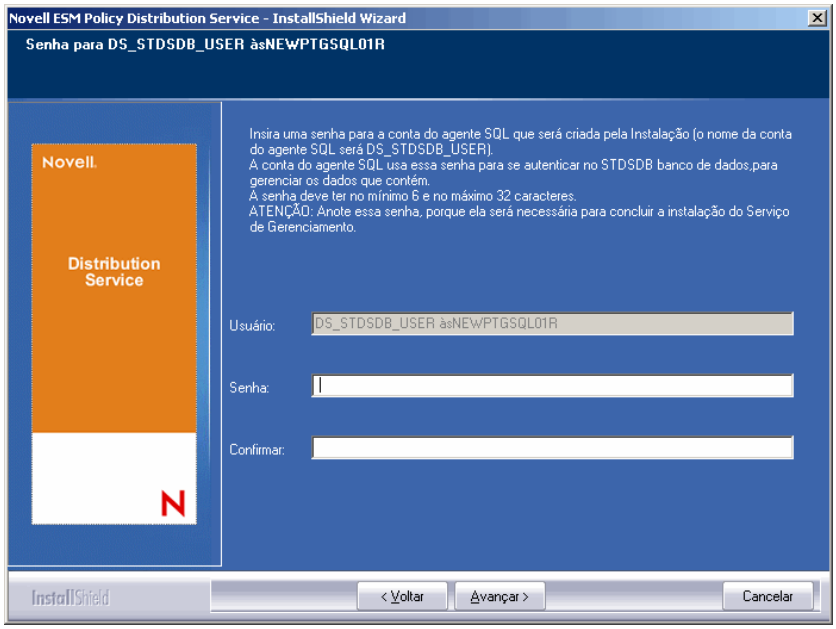
programa de instalação avisará sobre possível problema de segurança). O nome de usuário e a senha não podem ser um usuário de domínio; devem ser um usuário SQL com direitos SysAdmin.

Figura 5-2 *Selecionar SQL Server*



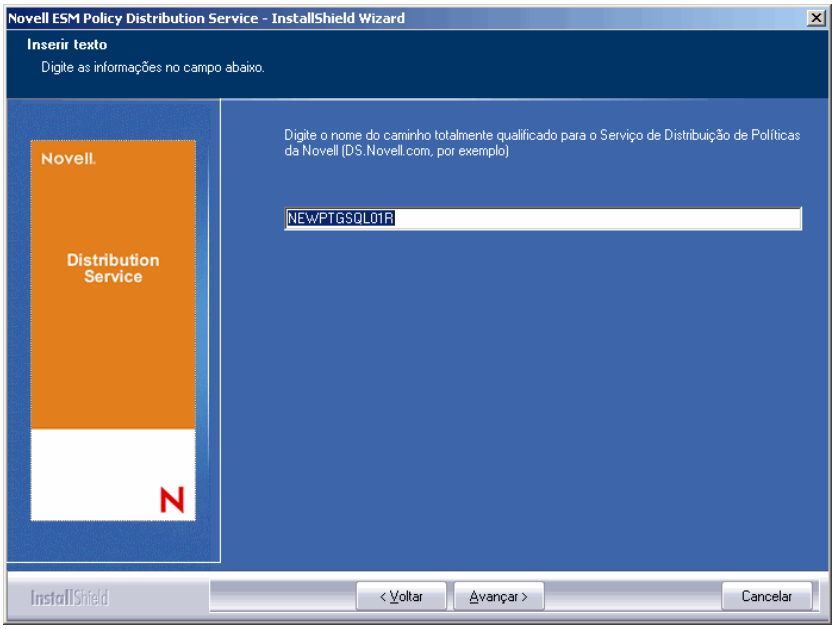
3 Especifique a senha do agente do Serviço de Distribuição de Política. Esses são o nome de usuário e a senha que o serviço usa para efetuar login no banco de dados SQL correspondente.

Figura 5-3 *Senha de SQL do serviço de distribuição*



4 Especifique o nome de domínio do Serviço de Distribuição de Política. Se o servidor residir fora do firewall corporativo, esse nome deverá ser o nome completo do domínio. Caso contrário, apenas o nome NETBIOS do servidor será exigido.

Figura 5-4 *Digitar nome de domínio do Serviço de Distribuição de Política*



5 Na tela Copiar Arquivos, clique em *Avançar* para iniciar a instalação.

6 A pasta `ESM Setup Files` é gerada no diretório de instalação. Ela contém um arquivo de `ID de Instalação` e o arquivo`ESM-DS.cer` (certificado SSL auto-assinado da Novell) exigidos pelo Serviço de Gerenciamento. Copie esse arquivo diretamente para a máquina designada como host do Serviço de Gerenciamento. Para fazer isso, use o netshare ou grave o arquivo em um disco ou em uma unidade USB e carregue-o manualmente no diretório de instalação do servidor.

7 O Serviço de Distribuição de Política está instalado. Clique em *Concluir* para fechar o programa de instalação e iniciar o monitor de desempenho.

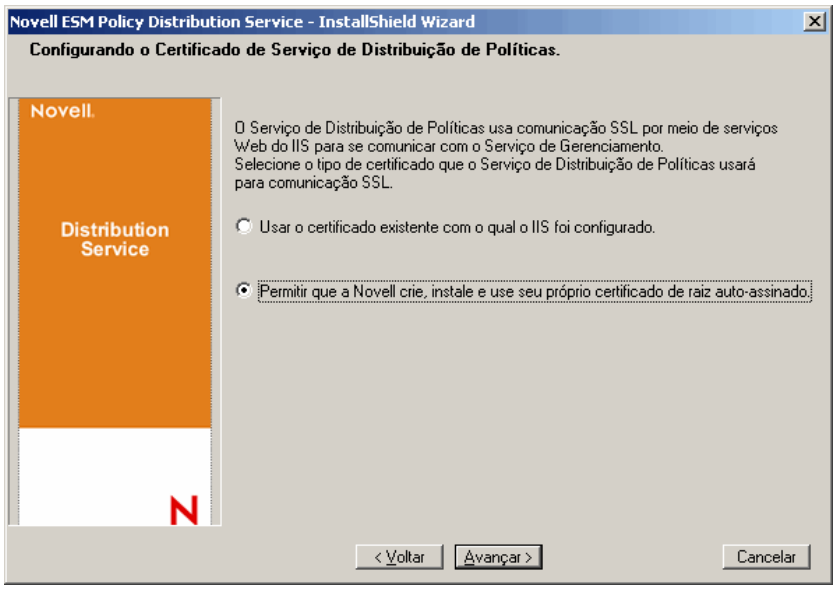
5.1.2 Instalação Personalizada

A instalação personalizada mostra os padrões usados na instalação típica e permite ao administrador especificar ou procurar outro diretório para colocar os arquivos do software.

O administrador pode optar entre instalar um certificado SSL auto-assinado da Novell ou usar um de seus próprios certificados.

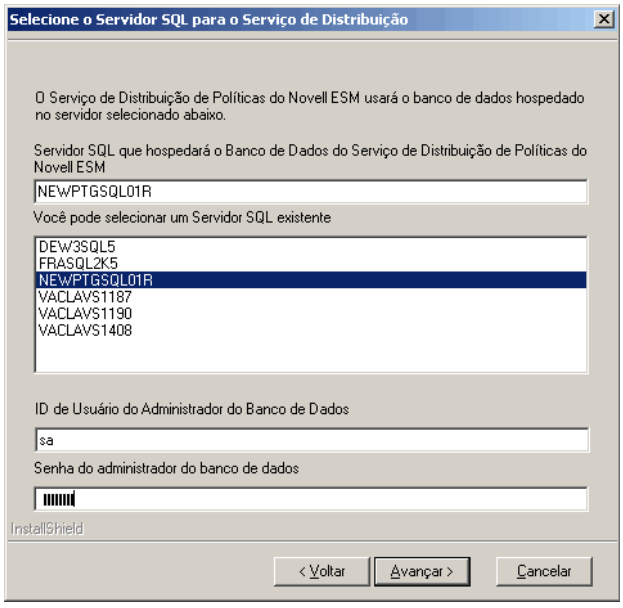
1 Um Certificado SSL é exigido para comunicação segura entre o Serviço de Distribuição de Política e o Serviço de Gerenciamento e entre o DS e todos os Novell Security Clients. Se você já tiver uma autoridade de certificação, clique em *Usar o certificado existente para o qual o IIS está configurado*. Se precisar de um certificado, clique em *Permitir que a Novell crie, instale e use seu próprio certificado raiz auto-assinado*. O programa de instalação cria os certificados e a autoridade de assinatura. Independentemente do tipo, esses certificados devem ser distribuídos para todos os usuários.

Figura 5-5 *Configurar a raiz confiável*



2 O programa de instalação detecta os bancos de dados SQL disponíveis na máquina e na rede. Selecione o banco de dados SQL protegido para o Serviço de Distribuição de Política e digite o nome e a senha do administrador do banco de dados (se a senha não tiver nenhum caractere, o programa de instalação avisará sobre possível problema de segurança). O nome de usuário e a senha não podem ser um usuário de domínio; devem ser um usuário SQL com direitos SysAdmin.

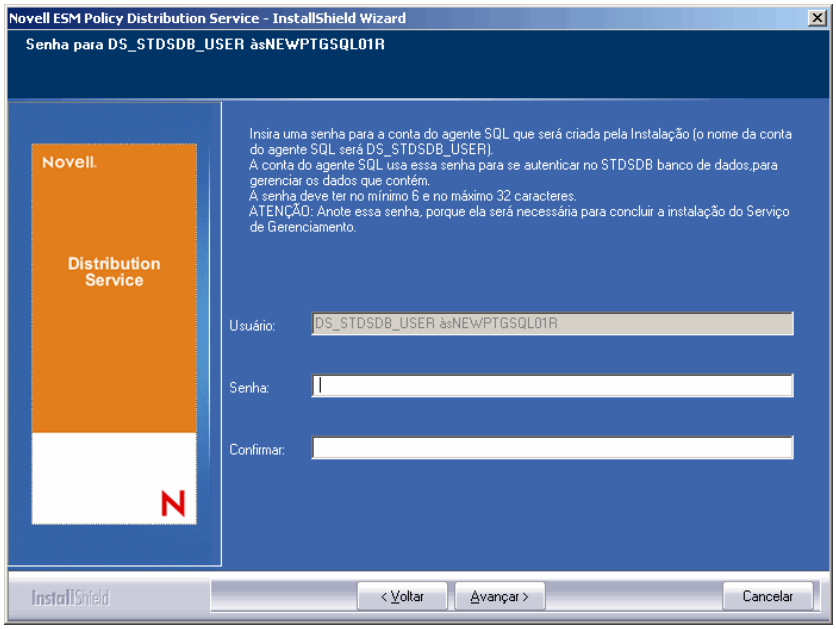
Figura 5-6 *Selecionar SQL Server*



3 Defina o nome do banco de dados (o padrão é digitado como STDSDB).

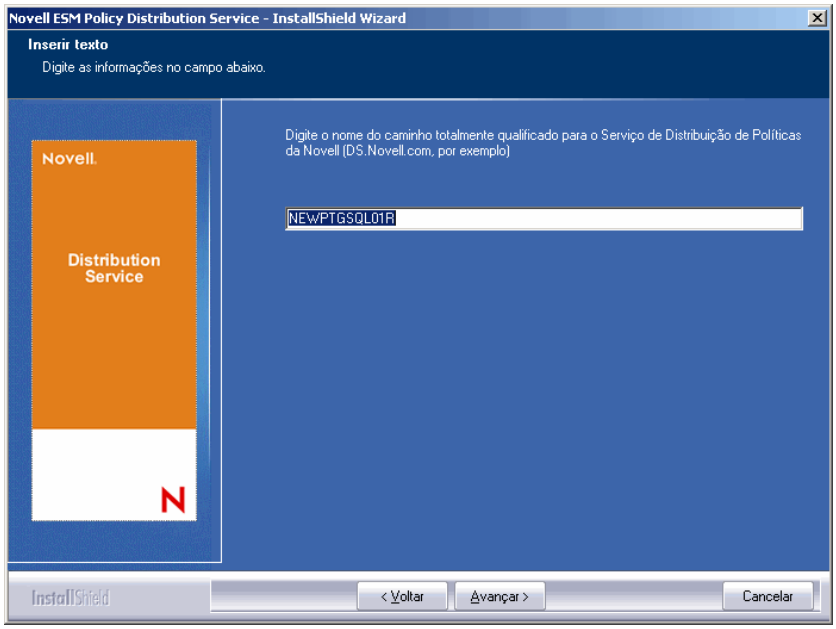
4 Especifique a senha do agente do Serviço de Distribuição de Política. Esses são o nome de usuário e a senha que o serviço usa para efetuar login no banco de dados SQL correspondente.

Figura 5-7 *Senha de SQL do serviço de distribuição*



5 Especifique o nome de domínio do Serviço de Distribuição de Política. Se o servidor residir fora do firewall corporativo, esse nome deverá ser o nome completo do domínio. Caso contrário, apenas o nome NETBIOS do servidor será exigido.

Figura 5-8 *Digitar nome de domínio do Serviço de Distribuição de Política*

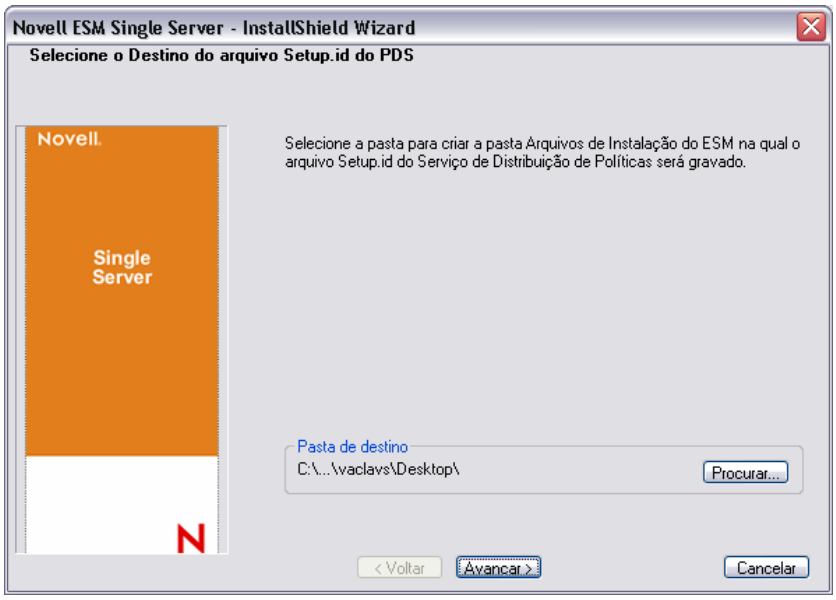


6 Na tela Copiar Arquivos, clique em *Avançar* para iniciar a instalação.

7 Especifique os caminhos para os arquivos data, index e log.

8 A pasta `ESM Setup Files` é gerada no diretório de instalação. Ela contém um arquivo de `ID de Instalação` e o arquivo`ESM-DS.cer` (certificado SSL auto-assinado da Novell, se selecionado) exigidos pelo Serviço de Gerenciamento. Use Procurar para designar onde esse arquivo deve ser gravado no servidor (o padrão é o diretório de instalação).

Figura 5-9 *Gravar arquivos de configuração*



9 Se você tiver optado por usar um certificado SSL da empresa, coloque uma cópia desse arquivo na pasta `ESM Setup Files`.

10 Copie toda a pasta `ESM Setup Files` diretamente na máquina designada como host do Serviço de Gerenciamento. Para fazer isso, use o netshare ou grave o arquivo em um disco ou em uma unidade USB e carregue-o manualmente para o diretório de instalação do servidor.

11 O Serviço de Distribuição de Política está instalado. Clique em *Concluir* para fechar o programa de instalação e iniciar o monitor de desempenho.

5.2 Iniciando o serviço

O Serviço de Distribuição de Política é iniciado logo após a instalação, sem a necessidade de reinicializar o servidor. O Console de Gerenciamento é usado para ajustar os horários de upload do Serviço de Distribuição utilizando a ferramenta de Configuração. Para obter mais informações, consulte o *Guia de Administração do ZENworks Endpoint Security Management*.

Continue na Capítulo 6, “Executando a instalação do Serviço de Gerenciamento” na página 31.

Executando a instalação do Serviço de Gerenciamento

6

O Serviço de Gerenciamento deve ser instalado em um servidor protegido pelo firewall e não pode compartilhar o mesmo servidor que o Serviço de Distribuição de Política (com a exceção de uma instalação de servidor único, consulte o Capítulo 3, "Executando uma instalação de Servidor Único" na página 17). Por motivos de segurança, o Serviço de Gerenciamento não deve ser instalado fora do firewall da rede. Após selecionar o servidor, anote o nome do servidor, tanto o NETBIOS quanto o FQDN (nome completo do domínio). A implantação do Serviço de Gerenciamento em um PDC (Primary Domain Controller - Controlador de Domínio Primário) não é suportada por razões de segurança e funcionalidade.

Observa o: É recomendado que o Servidor SSI seja configurado (reforçado) para desativar todos os aplicativos, serviços, contas e outras opções desnecessárias para a funcionalidade destinada do servidor. As etapas envolvidas dependem das especificações do ambiente local e, portanto, não podem ser descritas antecipadamente. Os administradores são avisados para consultar a seção apropriada da página da Web de segurança Microsoft TechNet (http://www.microsoft.com/technet/security/default.mspx). Recomendações adicionais de controle de acesso são fornecidas no *Guia de Administração do ZENworks Endpoint Security Management*.

Para restringir o acesso a máquinas confiáveis, configure o diretório virtual e o IIS para ter ACLs. Consulte os artigos a seguir:

- Granting and Denying Access to Computers (Concedendo e negando o acesso a computadores) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (Restringir o acesso a site por endereço IP ou nome de domínio) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (FAQ do IIS: Restrições de endereço IP 2000 e nome de domínio) (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (Trabalhando com filtragem de pacotes do IIS) (http://www.15seconds.com/issue/011227.htm)

Por motivos de segurança, é altamente recomendável que as seguintes pastas padrão sejam removidas de qualquer instalação do IIS:

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Impressoras`

Também recomendamos o uso da ferramenta IIS Lockdown Tool 2.1 disponível em microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

A versão 2.1 é orientada por gabaritos fornecidos para os principais produtos Microsoft dependentes do IIS. Selecione o gabarito que melhor corresponda à função deste servidor. Em caso de dúvida, o gabarito de servidor Web Dinâmico é recomendado.

Antes de iniciar a instalação, verifique se os seguintes pré-requisitos são atendidos:

- Verifique o acesso a um serviço de diretório suportado (eDirectory, Active Directory ou Domínios NT*). * = Suportado somente quando o Serviço de Gerenciamento é instalado em um servidor Microsoft Windows 2000 Advanced (SP4).
- Se estiver realizando a implantação com um serviço eDirectory™, verifique se o Novell Client™ está instalado no servidor e se pode autenticar corretamente no eDirectory. Crie uma senha de conta que nunca mude para usar na autenticação do Console de Gerenciamento. (Consulte a Seção 7.2.1, "Adicionando serviços do eDirectory" na página 47.)
- Verifique a resolução de nome de servidor Endpoint Security Client para MS: confirme se os computadores de destino (onde o Endpoint Security Client está instalado) podem realizar ping no nome do servidor MS. Se você obtiver êxito, esse será o valor inserido na instalação. Se não obtiver êxito, você deverá resolver isso antes de continuar com a instalação.
- Habilite ou instale o IIS (Serviços de Informações da Internet) da Microsoft, verifique se o ASP.NET está habilitado e configure-o para aceitar Certificados SSL (Secure Socket Layer).

  Importante: Não marque a caixa de seleção *Exigir canal de segurança (SSL)* na página Comunicações de Segurança. (No utilitário Gerenciamento do Computador da Microsoft, expanda *Serviços e Aplicativos* > expanda *Gerenciador dos Serviços de Informações da Internet (ISS)* > expanda *Sites* > clique o botão direito do mouse em *Site Padrão* > clique em *Propriedades* > clique na guia *Segurança de Diretório* > clique no botão *Editar* na caixa de grupo Comunicações de segurança.) A habilitação dessa opção interrompe a comunicação entre o servidor e o cliente ZENworks Endpoint Security Management no ponto de extremidade.

- Se estiver usando seus próprios certificados SSL, verifique se a CA raiz está carregada na máquina e se o nome do servidor validado nas etapas anteriores (NETBIOS ou FQDN) corresponde ao valor *Emitido para* do certificado configurado no IIS.
- Se estiver usando seus próprios certificados ou se já tiver instalado o Certificado Auto-assinado da Novell, você também poderá validar o SSL experimentando o seguinte URL em uma máquina que tenha o Endpoint Security Client instalado:`https://`*`NOME_DO_SERVIDOR_MS`*`/AuthenticationServer/UserService.asmx` (onde *NOME_DO_SERVIDOR_MS* é o nome do servidor). Isso retornará dados válidos (uma página html), e não avisos de certificado. Todos os avisos de certificado devem ser resolvidos antes da instalação.
- Verifique o acesso a um RDBMS (Microsoft SQL Server 2000 SP4, SQL Server Standard, SQL Server Enterprise, SQL 2005) suportado. Defina o banco de dados para o modo Misto.
- Copie o diretório `ESM Setup Files` que contém o ID de Instalação do Serviço de Distribuição de Política e o Certificado SSL Raiz para o Serviço de Distribuição de Política no diretório de instalação desse servidor.

6.1 Etapas de instalação

Clique em *Instalação do Serviço de Gerenciamento* no menu da interface de Instalação. A instalação do Serviço de Gerenciamento é iniciada.

Na inicialização, o programa de instalação verifica se todos os softwares necessários estão presentes no servidor. Se algum software estiver ausente, ele será instalado automaticamente antes que a instalação prossiga para a tela de boas-vindas (talvez seja necessário aceitar os contratos de licença dos softwares adicionais). Se for necessário instalar o MDAC (Microsoft Data Access Components)

2.8, o servidor deverá ser reinicializado após instalação desse recurso e antes da conclusão da instalação do ZENworks Endpoint Security Management. Se você estiver usando o Windows 2003 Server, o ASP.NET 2.0 deverá ser configurado para ser executado pelo programa de instalação.

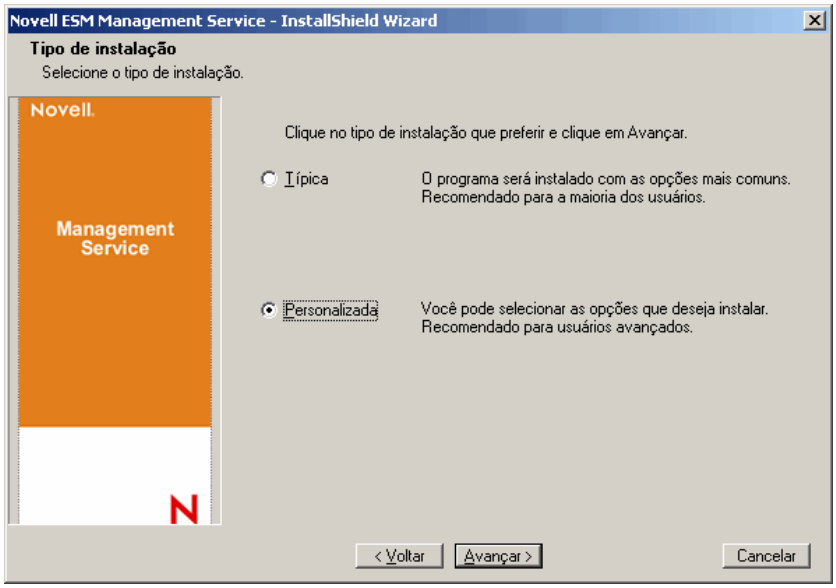
Após o início da instalação do Serviço de Gerenciamento, siga estas etapas:

Observa o: As etapas a seguir descrevem o que você, o administrador, precisa fazer para concluir o processo de instalação. Os processos internos serão exibidos durante a instalação e não serão documentados aqui, a menos que haja uma ação ou uma informação específica que seja necessária para o êxito da instalação.

---

1. Clique em *Avançar* na tela de boas-vindas para continuar.
2. Aceite o Contrato de Licença e clique em *Avançar*.
3. Selecione a instalação *Típica* ou *Personalizada*.

Figura 6-1 *Selecionar Típica ou Personalizada*



Ambos os caminhos de instalação são apresentados a seguir:

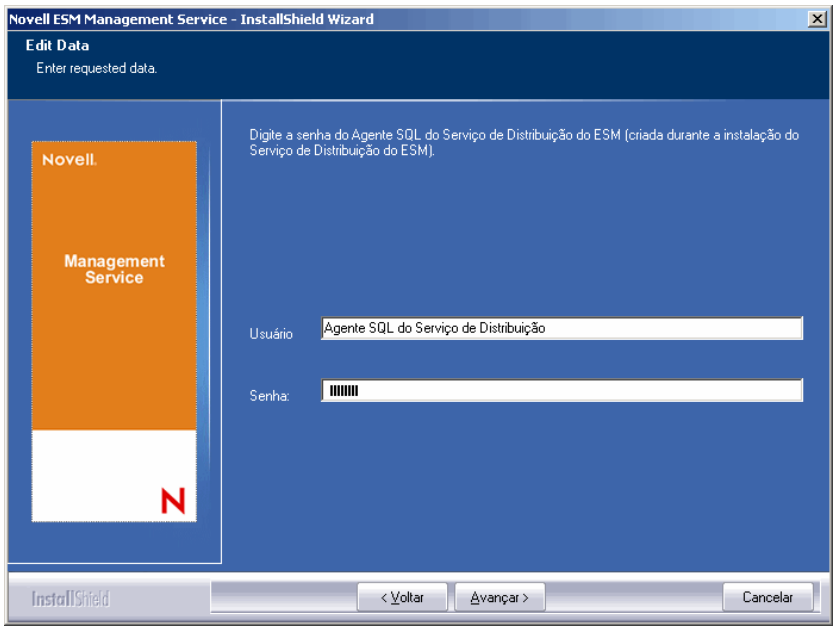
- Seção 6.1.1, “Instalação Típica” na página 33
- Seção 6.1.2, “Instalação Personalizada” na página 37

6.1.1 Instalação Típica

A instalação típica coloca os arquivos do software de Serviço de Gerenciamento no diretório padrão: `\Arquivos de Programas\Novell\Serviço de Gerenciamento do ESM`. O nome do banco de dados SQL é atribuído como STMSDB. Os três arquivos do banco de dados SQL (data, index e log) são colocados em: `\Arquivos de Programas\Microsoft SQL Server\mssql\Data`.

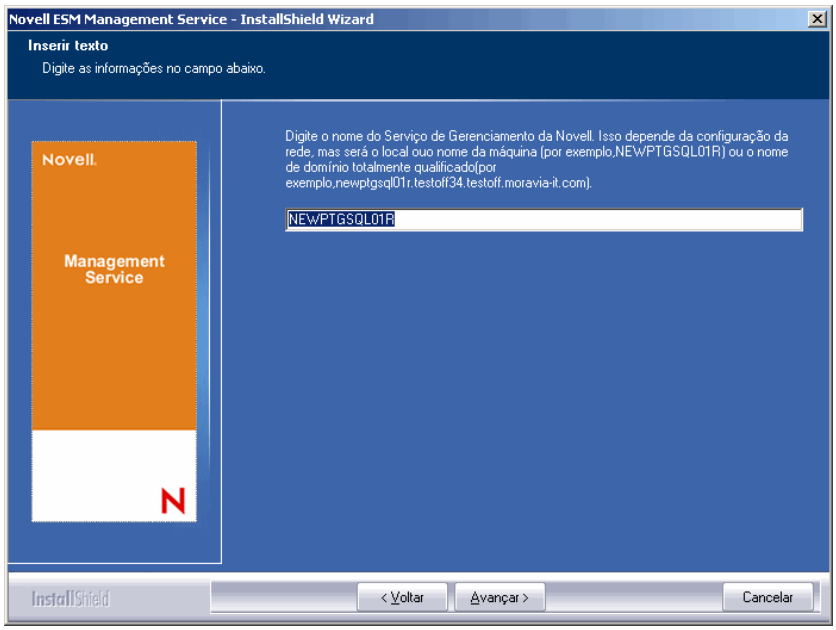
1. Especifique a senha do agente do Serviço de Distribuição de Política criada durante a instalação de Distribuição de Política.

Figura 6-2 *Digite a senha de SQL.*



2 Especifique o nome do servidor que hospedará o Serviço de Gerenciamento.

Figura 6-3 *Digitar nome do servidor do MS*

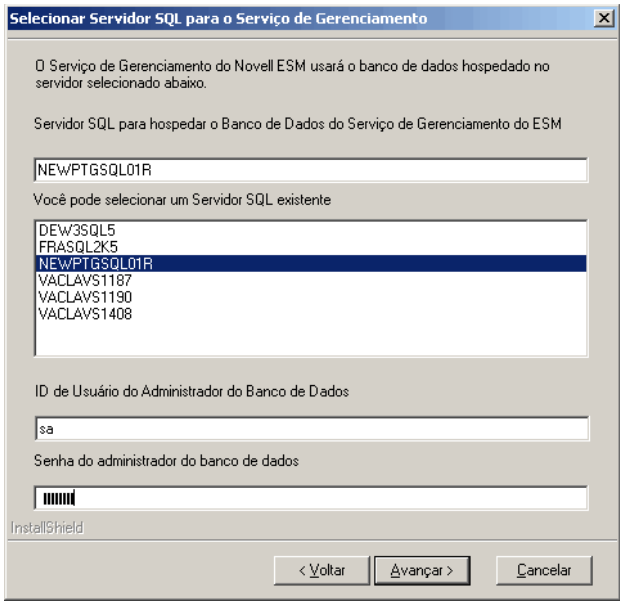


3 Os Certificados SSL da Novell são criados para a instalação. Se quiser usar seus próprios certificados SSL, execute a Instalação Personalizada. Esses certificados devem ser distribuídos para todos os usuários.

4 O programa de instalação detecta os bancos de dados SQL disponíveis na máquina e na rede. Selecione o banco de dados SQL para o Serviço de Gerenciamento e especifique o nome de usuário e a senha do administrador do banco de dados (se a senha não tiver nenhum caractere, o

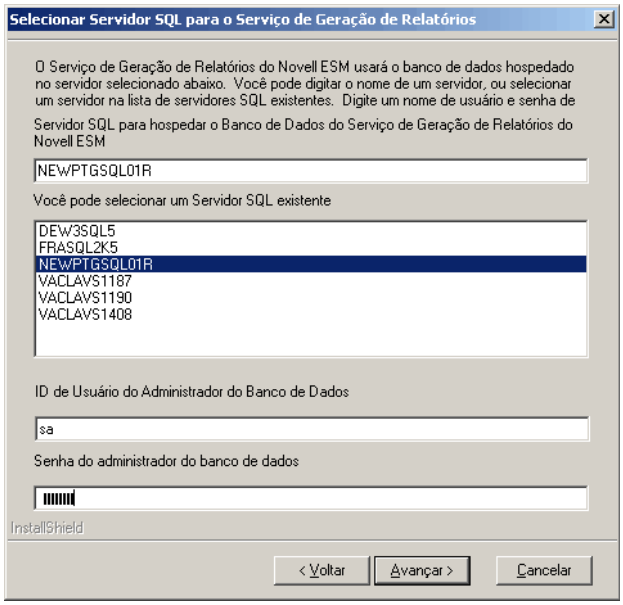
programa de instalação avisará sobre o possível problema de segurança). O nome de usuário e a senha não podem ser um usuário de domínio; devem ser um usuário SQL com direitos SysAdmin.

Figura 6-4 *Selecionar o banco de dados SQL do MS*



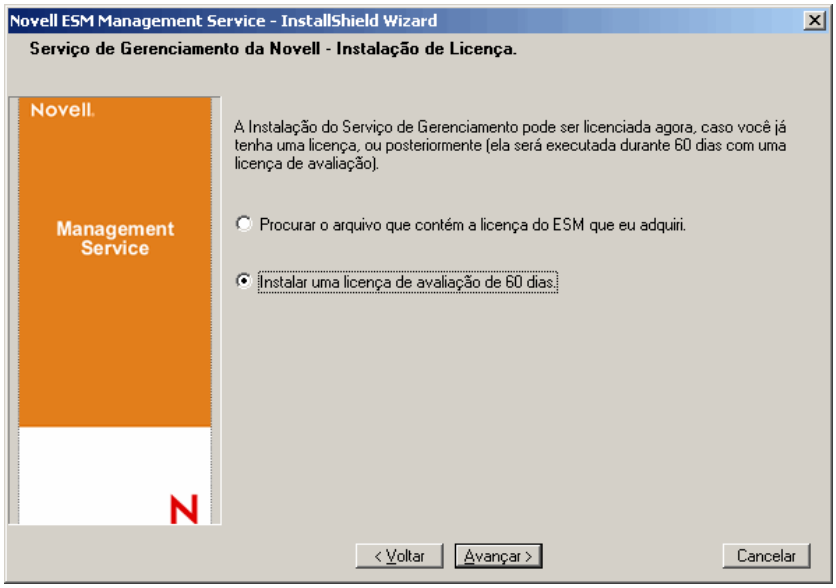
5 Selecione o banco de dados SQL para o Serviço de Geração de Relatórios e especifique a senha do administrador do banco de dados para esse banco de dados. Se você planeja capturar e armazenar um grande número de relatórios, é recomendado que o banco de dados Serviço de Geração de Relatórios possua seu próprio servidor SQL.

Figura 6-5 *Selecionar o banco de dados de Serviço de Geração de Relatórios*



6 Se você já tiver adquirido o ZENworks Endpoint Security Management, um arquivo de licença separado será fornecido. Copie o arquivo de licença para este servidor e procure-o (consulte a página de instruções fornecida com seu arquivo de Licença para obter mais detalhes). Caso ainda não tenha adquirido uma licença do ZENworks Endpoint Security Management, selecione a opção *Licença de Avaliação de 60 Dias* para continuar.

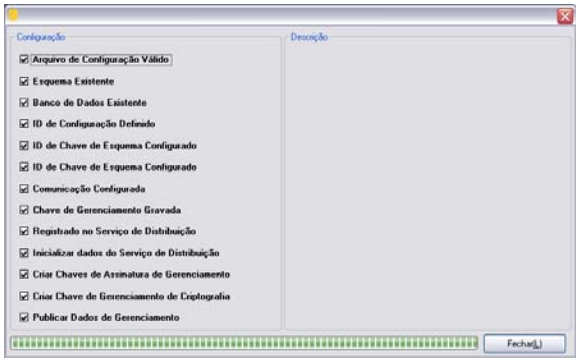
Figura 6-6 *Procurar o arquivo de licença da Novell*



7 Na tela Copiar Arquivos, clique em *Avançar* para iniciar a instalação.

8 O Serviço de Gerenciamento executa uma verificação de comunicação nos bancos de dados SQL e no Serviço de Distribuição de Política. Se não for possível verificar a comunicação, o programa de instalação notificará você sobre o problema. Para que a instalação seja bem-sucedida, todas as caixas devem ser marcadas.

Figura 6-7 *Verificação da comunicação*



9 Ignore a Etapa 10 e a Etapa 11 se estiver instalando com o eDirectory como serviço de diretório.

10 Se a instalação estiver ocorrendo em um servidor membro de um domínio que possua um serviço de diretório do Active Directory ou de Domínios NT, o programa de instalação detectará e adicionará automaticamente os seguintes dados à instalação, usando uma conexão segura e apenas leitura:

- Nome de domínio raiz ou nome da máquina
- Nome do administrador de domínio ou uma conta de recurso com permissões de leitura apropriadas

11 Especifique a senha do administrador no espaço fornecido e clique em *Testar para verificar se a conexão pode ser estabelecida*. Se o teste for bem-sucedido, clique em *Gravar*. Se o teste falhar ou se o domínio correto não for detectado, você deverá adicionar esse domínio manualmente por meio do Console de Gerenciamento. (Consulte a Seção 7.2.1, “Adicionando serviços do eDirectory” na página 47.)

Observa o: A senha digitada deve ser definida para não expirar e essa conta também não deve ser desabilitada nunca.

---

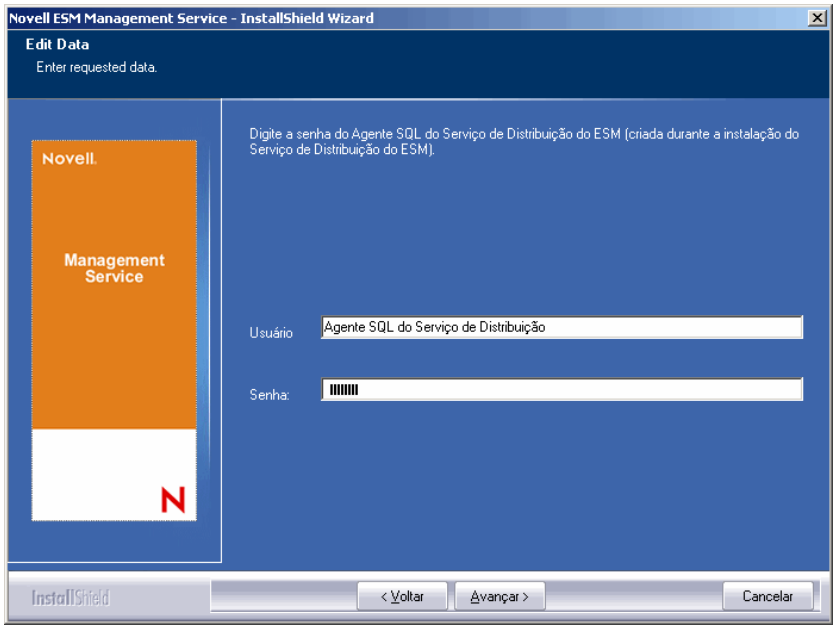
12 O Serviço de Gerenciamento está instalado. Clique em *Concluído* para fechar as verificações de comunicação e, em seguida, clique em *Concluir* para fechar o programa de instalação.

6.1.2 Instalação Personalizada

A instalação personalizada mostra os padrões usados na instalação típica e permiti ao administrador digitar ou procurar outro local.

1 Especifique a senha do agente do Serviço de Distribuição de Política criada durante a instalação de Distribuição de Política.

Figura 6-8 *Digite a senha de SQL.*

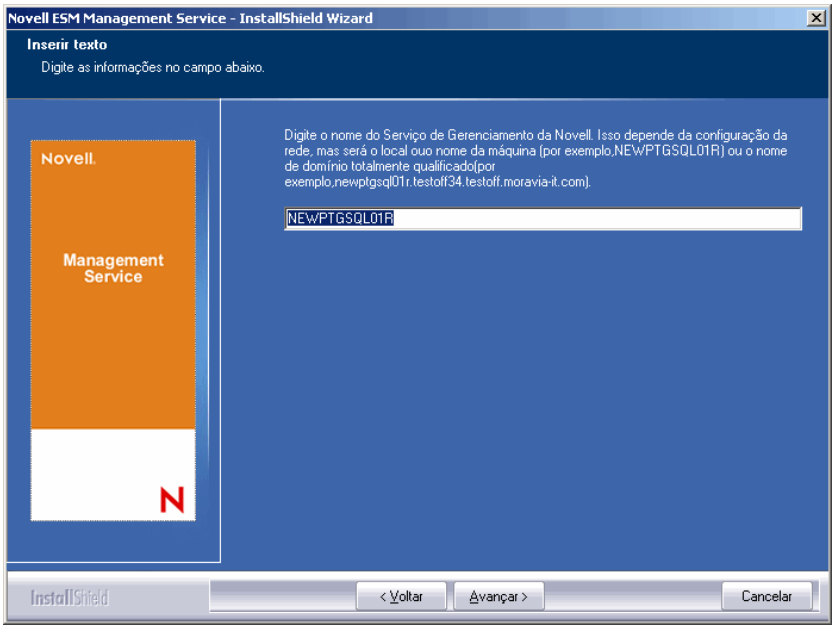


2 Selecione o tipo do Certificado SSL usado para a instalação do Serviço de Distribuição de Política. Se você tiver usado uma autoridade de certificação existente (corporativa), clique em *O Serviço de Distribuição da Novell usou um certificado com o qual o IIS já está configurado*.

Se o programa de instalação do Serviço de Distribuição tiver criado um certificado da Novell, clique em *O Serviço de Distribuição da Novell instalou um certificado raiz auto-assinado da Novell*.

3 Especifique o nome do servidor que hospedará o Serviço de Gerenciamento.

Figura 6-9 *Digitar nome do servidor MS*

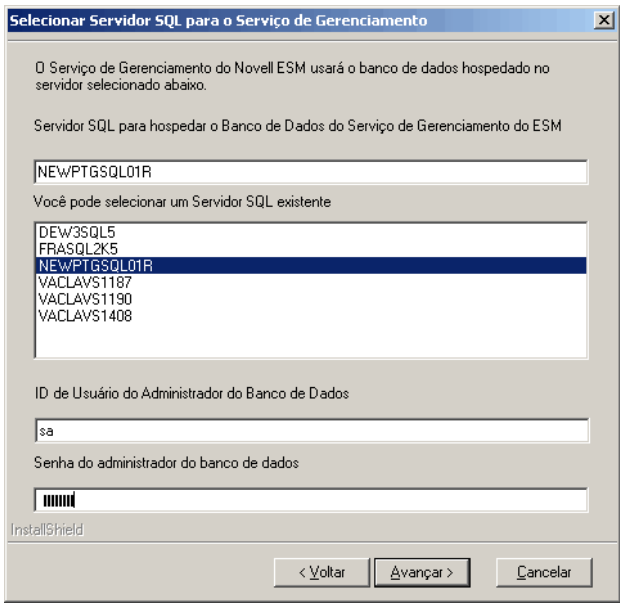


4 É necessário ter um Certificado SSL para obter uma comunicação segura entre o Serviço de Gerenciamento e todos os Endpoint Security Clients. Se você já possuir uma autoridade de certificação, clique em *Usar o certificado existente para o qual o IIS está configurado*. Se precisar de um certificado, clique em *Permitir que a Novell crie, instale e use seu próprio certificado raiz auto-assinado*. O programa de instalação cria os certificados e a autoridade de assinatura. Independentemente do tipo, esses certificados devem ser distribuídos para todos os usuários.

5 Ao selecionar certificados da Novell, defina onde o certificado pode ser gravado para facilitar a distribuição (o padrão é o diretório de instalação).

6 O programa de instalação detecta os bancos de dados SQL disponíveis na máquina e na rede. Selecione o banco de dados SQL para o Serviço de Gerenciamento e especifique o nome de usuário e a senha do administrador do banco de dados (se a senha não tiver nenhum caractere, o programa de instalação avisará sobre o possível problema de segurança). O nome de usuário e a senha não podem ser um usuário de domínio; devem ser um usuário SQL com direitos SysAdmin.

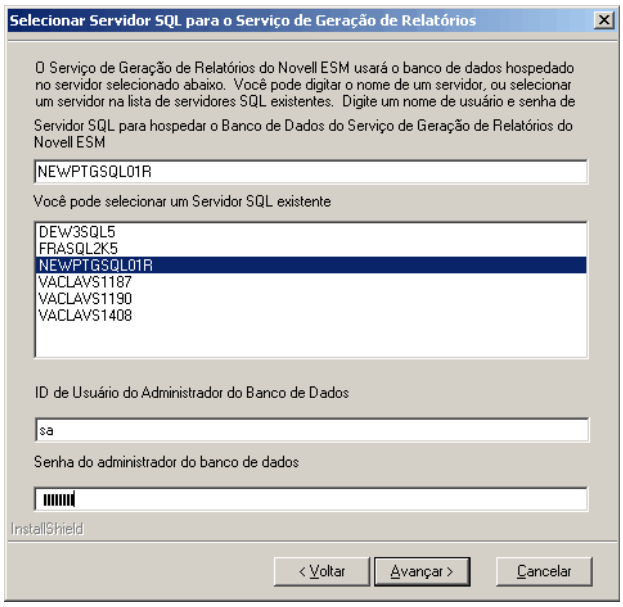
Figura 6-10 *Selecionar o banco de dados SQL do MS*



7 Defina o nome do banco de dados (o padrão é inserido como STMSDB).

8 Selecione o banco de dados SQL para o Serviço de Geração de Relatórios e especifique a senha do administrador do banco de dados para esse banco de dados.

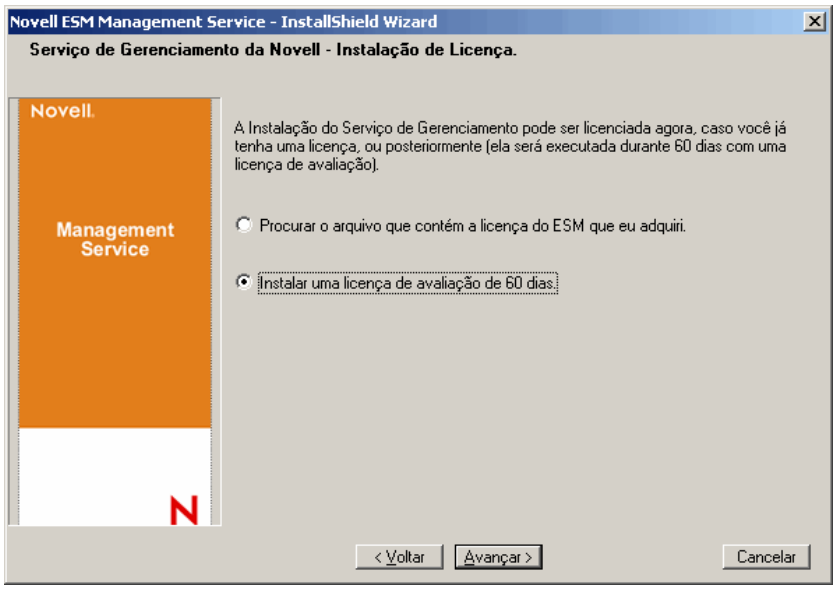
Figura 6-11 *Selecionar o banco de dados de Serviço de Geração de Relatórios*



9 Defina o nome do banco de dados (o padrão é digitado como STRSDB).

10 Se você já tiver adquirido o ZENworks Endpoint Security Management, um arquivo de licença separado será fornecido. Copie o arquivo de licença para este servidor e procure-o (consulte a página de instruções fornecida com seu arquivo de Licença para obter mais detalhes). Caso ainda não tenha adquirido uma licença do ZENworks Endpoint Security Management, selecione a opção *Licença de Avaliação de 60 Dias* para continuar.

Figura 6-12 *Procurar o arquivo de licença da Novell*



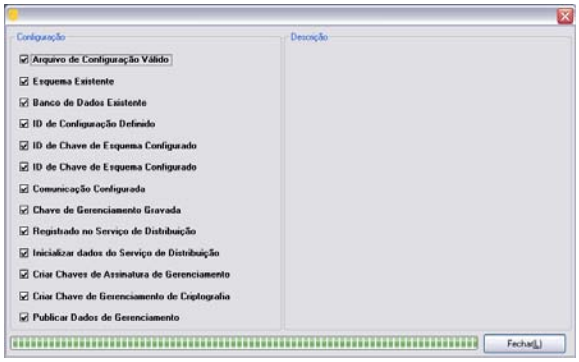
11 Na tela Copiar Arquivos, clique em *Avançar* para iniciar a instalação.

12 Selecione os caminhos de arquivo para os arquivos data, index e log do banco de dados do Serviço de Gerenciamento.

13 Selecione os caminhos para os arquivos data, index e log do banco de dados do Serviço de Geração de Relatórios.

14 O Serviço de Gerenciamento executa uma verificação de comunicação nos bancos de dados SQL e no Serviço de Distribuição de Política. Se não for possível verificar a comunicação, o programa de instalação notificará você sobre o problema. Para que a instalação seja bem-sucedida, todas as caixas devem ser marcadas.

Figura 6-13 *Verificação da comunicação*



15 Ignore a Etapa 16 e a Etapa 17 se estiver instalando com o eDirectory como serviço de diretório.

16 Se a instalação estiver ocorrendo em um servidor membro de um domínio que possua um serviço de diretório do Active Directory ou de Domínios NT, o programa de instalação detectará e adicionará automaticamente os seguintes dados à instalação, usando uma conexão segura e apenas leitura:

- Nome de domínio raiz ou nome da máquina
- Nome do administrador de domínio ou uma conta de recurso com permissões de leitura apropriadas

17 Especifique a senha do administrador no espaço fornecido e clique em *Testar para verificar se a conexão pode ser estabelecida*. Se o teste for bem-sucedido, clique em *Gravar*. Se o teste falhar ou se o domínio correto não for detectado, você deverá adicionar esse domínio manualmente por meio do Console de Gerenciamento. (Consulte a Seção 7.2.1, “Adicionando serviços do eDirectory” na página 47.)

Observa o: A senha especificada deve ser configurada para não expirar e a conta nunca deve ser desabilitada.

---

18 O Serviço de Gerenciamento está instalado. Clique em *Concluído* para fechar as verificações de comunicação e, em seguida, clique em *Concluir* para fechar o programa de instalação.

6.2 Iniciando o serviço

O Serviço de Gerenciamento inicia imediatamente após a instalação, sem a necessidade de reinicialização do servidor. O Console de Gerenciamento é utilizado para gerenciar os dados do Serviço de Gerenciamento. (Consulte o *Guia de Administração do ZENworks Endpoint Security Management*.)

A Novell recomenda a instalação do Console de Gerenciamento nesse servidor. Se você estiver instalando o Console de Gerenciamento em uma máquina separada, copie o diretório `ESM Setup Files` para a máquina que hospedará o Console de Gerenciamento. Para isso, use um netshare ou grave o arquivo em um disco ou em uma unidade USB.

Continue na Capítulo 7, “Executando a instalação do Console de Gerenciamento” na página 43.

Executando a instalação do Console de Gerenciamento

7

O Console de Gerenciamento pode ser instalado no servidor do Serviço de Gerenciamento ou em um PC protegido que tenha comunicação direta com o servidor do Serviço de Gerenciamento. É possível configurar várias instalações do Console de Gerenciamento para se comunicar com um único Serviço de Gerenciamento; entretanto, é altamente recomendável que o acesso ao Console de Gerenciamento seja limitado a usuários selecionados.

Por motivos de segurança, recomendamos que o Console de Gerenciamento seja instalado diretamente no servidor do Serviço de Gerenciamento.

Se quiser instalar o Console de Gerenciamento em uma estação de trabalho separada, verifique se os seguintes pré-requisitos são atendidos antes de iniciar a instalação:

- Verifique se o dispositivo no qual você deseja instalar o Console de Gerenciamento atende aos seguintes requisitos:
  - Windows XP SP1, Windows XP SP2 ou Windows 2000 SP4.
  - É recomendável usar um processador de 1.0 GHz, com um mínimo de 256 MB de RAM e 100 MB de espaço em disco disponível.
- Copie para o PC a pasta `ESM Setup Files` que contém os Certificados Raiz SSL do Serviço de Distribuição de Política e do Serviço de Gerenciamento, juntamente com o arquivo `STInstParam.id`.
- Se estiver instalando o Console de Gerenciamento no servidor do Serviço de Gerenciamento, verifique se a versão do Microsoft Internet Explorer é 5.5 ou superior.

7.1 Etapas de instalação

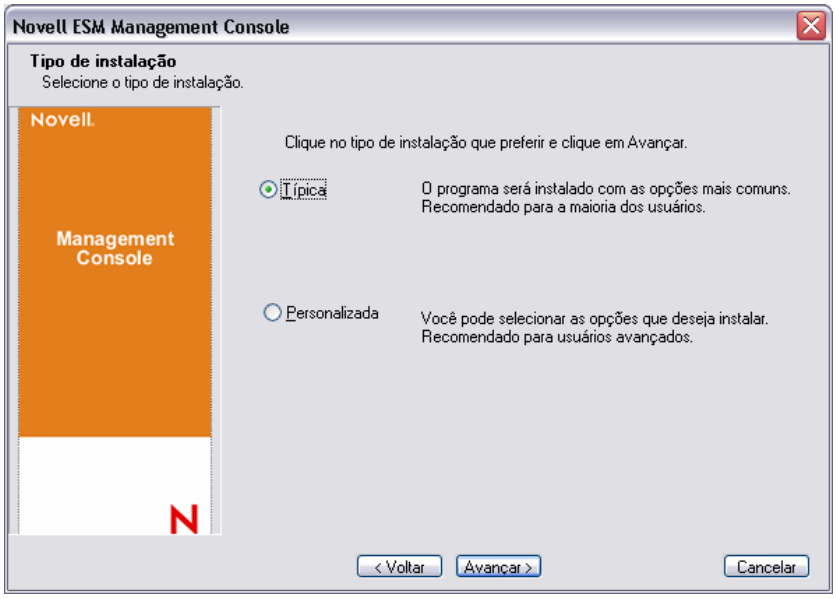
Clique em *Instalação do Console de Gerenciamento* no menu da interface de Instalação.

Na inicialização, o programa de instalação verifica se o .NET Framework 3.5 e o WSE 2.0 SP2 necessários estão presentes na máquina. Se um ou ambos estiverem ausentes, eles serão instalados automaticamente antes de a instalação prosseguir para a tela de boas-vindas. (Será necessário aceitar o contrato de licença para .NET 3.5.)

Para instalar os Consoles de Gerenciamento:

1. Clique em *Avançar* para continuar.
2. Aceite o Contrato de Licença e clique em *Avançar*.
3. Selecione a instalação *Típica* ou *Personalizada*.

Figura 7-1 *Selecionar Típica ou Personalizada*



Ambos os caminhos de instalação são apresentados a seguir:

- Seção 7.1.1, “Instalação Típica” na página 44
- Seção 7.1.2, “Instalação Personalizada” na página 44

7.1.1 Instalação Típica

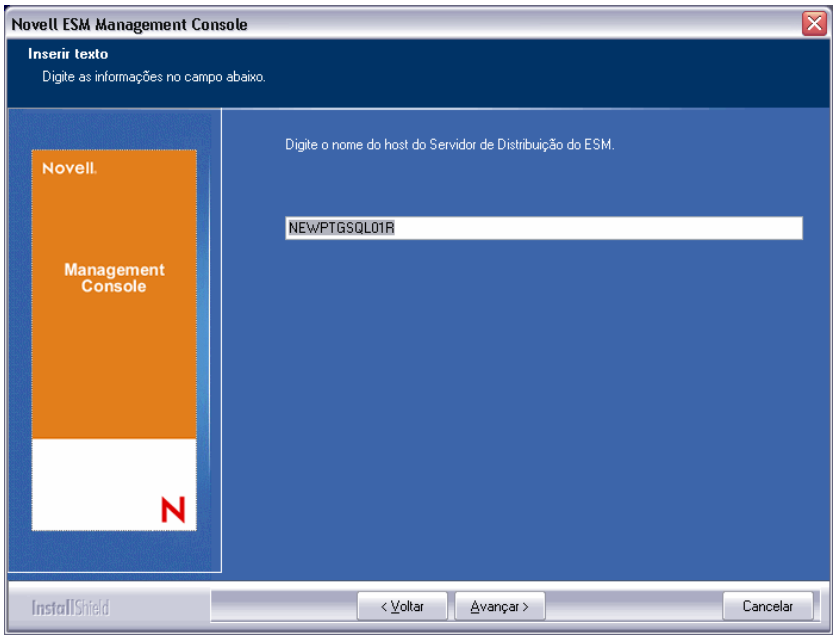
A instalação típica usa todos os servidores padrão e as informações sobre SSL contidas no arquivo `STInstParam.id`. O diretório padrão dessa instalação é: `\Arquivos de Programas\Novell\Console de Gerenciamento do ESM`. Não são necessárias seleções adicionais para a instalação do Console de Gerenciamento, contanto que o diretório `ESM Setup Files` esteja na máquina.

7.1.2 Instalação Personalizada

A instalação personalizada exibe os padrões de `STInstParam.id` usados na instalação típica e permite que o administrador mude essas informações.

1 Especifique o nome de host do Serviço de Distribuição de Política (esse nome deverá ser o nome completo do domínio se o Servidor de Distribuição for implantado fora do firewall corporativo).

Figura 7-2 *Digite o nome do host do Serviço de Distribuição.*

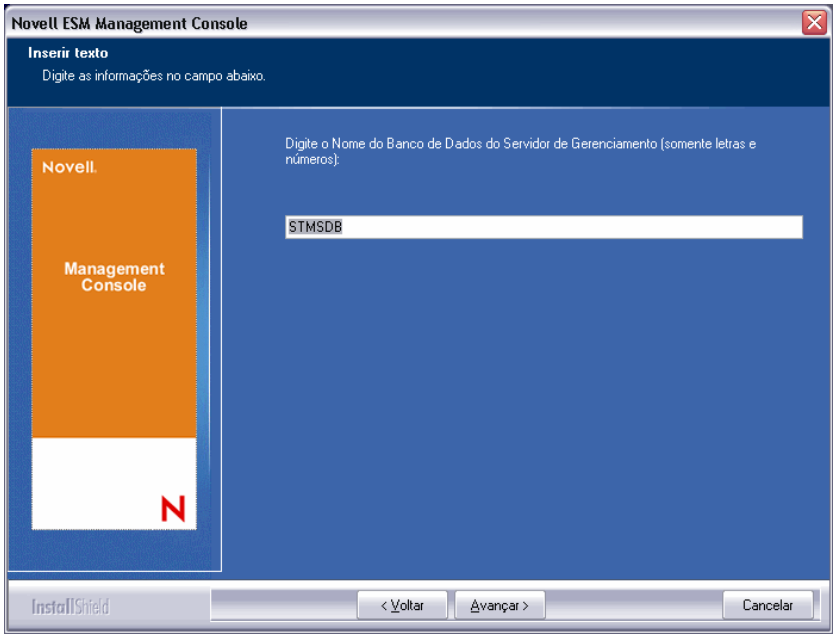


2 Especifique o nome de host do Serviço de Gerenciamento.

3 Especifique o nome de host de banco de dados SQL do Serviço de Gerenciamento.

4 Especifique o nome do banco de dados SQL do Serviço de Gerenciamento.

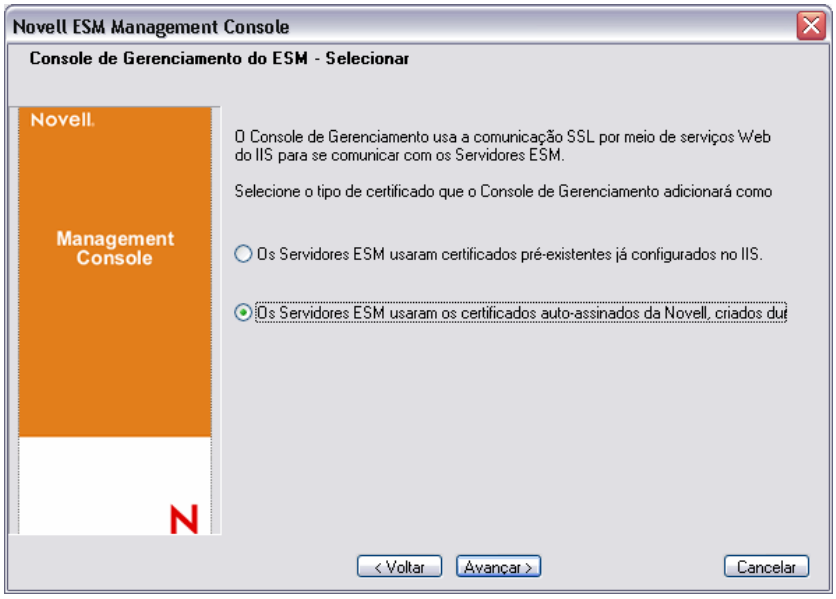
Figura 7-3 *Digite o nome do banco de dados SQL do MS.*



5 Especifique o nome de usuário e a senha do SA do SQL identificados durante a instalação do Serviço de Gerenciamento.

6 Selecione o tipo de Certificado SSL instalado no Serviço de Distribuição de Política e no Serviço de Gerenciamento.

Figura 7-4 *Selecionar certificados do servidor*



7 Selecione o diretório no qual o Console de Gerenciamento está instalado. O local padrão é `\Arquivos de Programas\Novell\Console de Gerenciamento do ESM`.

Depois de instalar o ZENworks Endpoint Security Management, você deverá criar e configurar um serviço de diretório antes de começar a gerenciar dispositivos no sistema.

O Assistente de Nova Configuração de Serviço de Diretório permite criar uma configuração do serviço de diretório que defina o escopo das instalações do Endpoint Security Client. A nova configuração usa o serviço de diretório existente para definir a divisa lógica das instalações de cliente baseadas em usuário e em computador.

O assistente orienta você através do processo de seleção do serviço de diretório e dos contextos em que residem as contas de cliente atuais e futuras.

Além disso, o assistente permite sincronizar as entradas de diretório incluídas na nova configuração. Essa sincronização é executada em segundo plano para que você possa começar a usar imediatamente sua nova configuração.

Depois que você instalar o ZENworks Endpoint Security Management, o Assistente de Nova Configuração de Serviço de Diretório será exibido automaticamente. Para obter mais informações sobre como criar e configurar o serviço de diretório, consulte "Configurando o serviço de diretório" no *Guia de Administração do ZENworks Endpoint Security Management*.

7.2 Iniciando o console

Para abrir a janela de login do Console de Gerenciamento, clique em *Iniciar* > *Todos os Programas* > *Novell* > *Console de Gerenciamento do ESM* > *Console de Gerenciamento*.

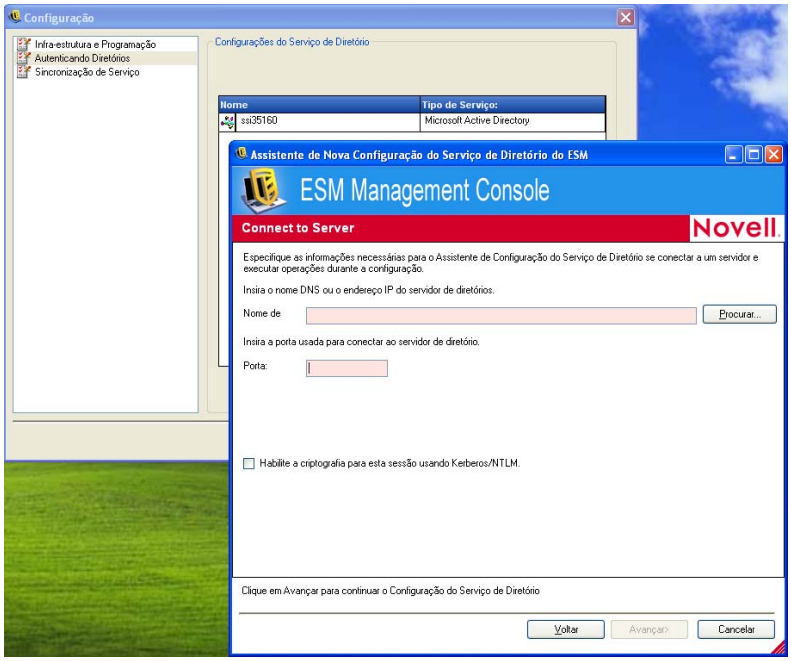
Para efetuar login no Console de Gerenciamento, digite o nome e a senha do administrador. Antes de digitar o nome de usuário e a senha, você deve estabelecer conexão com o domínio do serviço de diretório. (Consulte a Seção 7.2.1, "Adicionando serviços do eDirectory" na página 47.) O nome fornecido deve ser o nome de um usuário do domínio do Serviço de Gerenciamento.

Figura 7-5 *Login no Console de Gerenciamento do ZENworks Endpoint Security Management*

7.2.1 Adicionando serviços do eDirectory

1 Na tela de login, clique no botão *Opções* para exibir a janela Configuração.

Figura 7-6 *Autenticação de Diretórios*



2 Digite um nome amigável para o Serviço de Diretório e selecione eDirectory na lista suspensa *Tipo de Serviço*.

3 No campo *Host/DN*, especifique o endereço IP do servidor eDirectory e o nome de árvore sob a árvore *Domínio*.

4 Marque a opção *Disponível para Autenticação do Usuário* para mostrar o domínio no menu suspenso de login.

5 Desmarque *Autenticação Segura* nas opções de *Conexão de Serviço*.

6 Especifique o nome da Conta usando o formato LDAP. Por exemplo, em "cn=admin,o=acmeserver", cn é o usuário e o é o objeto em que a conta do usuário está armazenada.

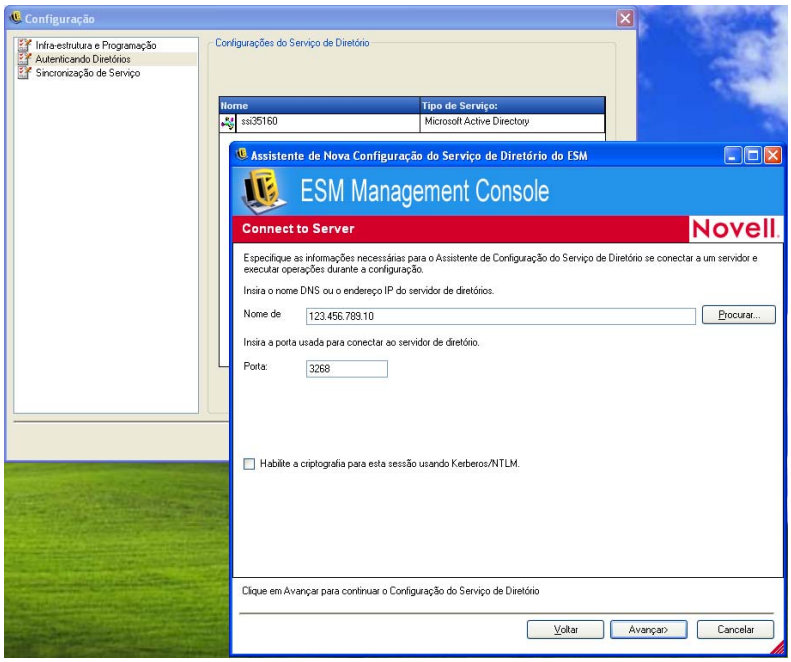
7 Especifique a senha da conta.

Observa o: A senha deve ser configurada para não expirar e a conta nunca deve ser desabilitada.

---

8 Clique em *Testar* para verificar a comunicação com o serviço de diretório. Se a comunicação não puder ser estabelecida, o usuário será notificado do erro. Qualquer informação imprecisa será corrigida, quando possível, pela interface durante o teste.

Figura 7-7 *Tela Diretório Concluído*



9 Clique em *Gravar* para adicionar esse serviço de diretório ao banco de dados e, em seguida, clique em *Novo* para adicionar outro serviço de diretório ao banco de dados.

10 Clique em *OK* ou em *Cancelar* para sair da janela Configuração e retornar à tela de login.

Consulte o *Guia de Administração do ZENworks Endpoint Security Management* para obter informações sobre como configurar a escuta para serviços de diretório adicionais, incluindo os serviços do Active Directory e de Domínios NT suportados.

7.2.2 Definindo as configurações de permissão do Console de Gerenciamento

A opção *Permissões* está localizada no menu *Ferramentas* do Console de Gerenciamento. Essa opção só pode ser acessada pelo administrador principal do Serviço de Gerenciamento e pelos usuários que receberam permissões de acesso desse administrador. Esse controle não está disponível quando o Console de Gerenciamento Independente é executado. Consulte o Capítulo 11, “Instalação não gerenciada do ZENworks Endpoint Security Management” na página 75 para obter mais detalhes.

As configurações de permissão definem qual usuário ou grupo de usuários terão permissão para acessar o Console de Gerenciamento, Publicar Políticas e Mudar Configurações de Permissão.

Durante a instalação do Servidor de Gerenciamento, o nome de um administrador ou de uma Conta de Recurso é digitado no formulário de configuração. Depois que um teste é realizado com êxito e as informações do usuário são gravadas, as permissões são concedidas automaticamente a esse usuário.

Após a instalação do Console de Gerenciamento, todos os grupos de usuários do domínio receberão permissão total. O usuário do recurso deve remover as permissões de todos os grupos e usuários, exceto daqueles que devem ter acesso. O usuário do recurso pode configurar permissões adicionais para os usuários indicados. Estes são os resultados das permissões concedidas:

- **Acesso ao Console de Gerenciamento:** O usuário pode ver políticas e componentes, e também editar políticas existentes. Os usuários que receberam apenas esse privilégio não poderão adicionar nem apagar políticas, e as opções de publicação e de permissões estarão indisponíveis.
- **Publicar Política:** O usuário só pode publicar políticas para outros usuários e grupos designados.
- **Mudar Permissão:** O usuário pode acessar e mudar configurações de permissão de outros usuários já definidos ou conceder permissões a novos usuários.
- **Criar Políticas:** O usuário pode criar novas políticas no Console de Gerenciamento.
- **Apagar políticas:** O usuário pode apagar qualquer política do Console de Gerenciamento.

Observa o: Por motivos de segurança, somente o usuário do recurso ou alguns poucos administradores devem ter as permissões Mudar Permissão e Apagar Políticas.

As seções a seguir contêm mais informações:

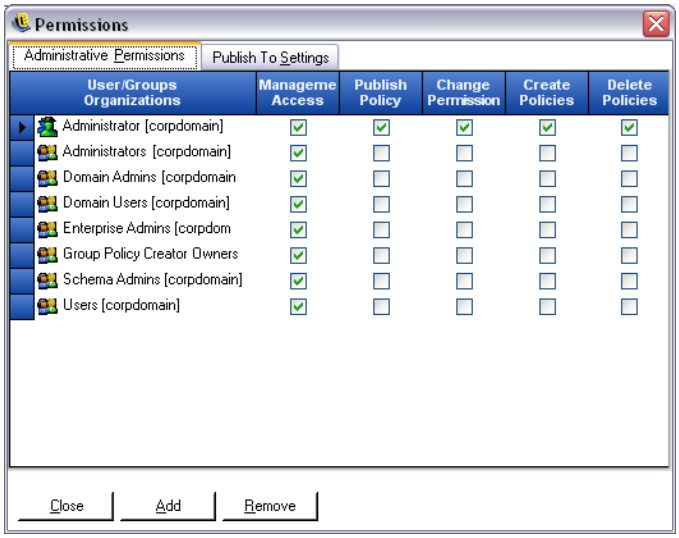
- “Configurando permissões administrativas” na página 49
- “Definindo as Configurações de Publicar Para” na página 51

Configurando permissões administrativas

1 Clique em *Ferramentas* > *Permissões*.

Os grupos associados a este domínio são mostrados.

Figura 7-8 *Janela Configurações de Permissão do Console de Gerenciamento*



Observa o: Por padrão, são concedidas permissões totais a todos os grupos no Console de Gerenciamento. Os administradores devem desmarcar imediatamente qualquer e todas as tarefas de política de grupos não-autorizados. Para remover o acesso ao console, basta desmarcar essa permissão.

---

2 (Opcional) Para carregar usuários e novos grupos nessa lista:

2a Clique no botão *Adicionar*, na parte inferior da tela, para exibir a tabela Organização.

Figura 7-9 *Tabela Organização de Configurações de Permissão*

2b Selecione os usuários e os grupos apropriados na lista. Use a tecla Ctrl ou Shift para selecionar vários usuários.

2c Depois de selecionar todos os usuários e grupos, clique no botão *OK* para adicioná-los à grade do formulário Permissões.

3 Atribua permissões aos usuários e grupos disponíveis.

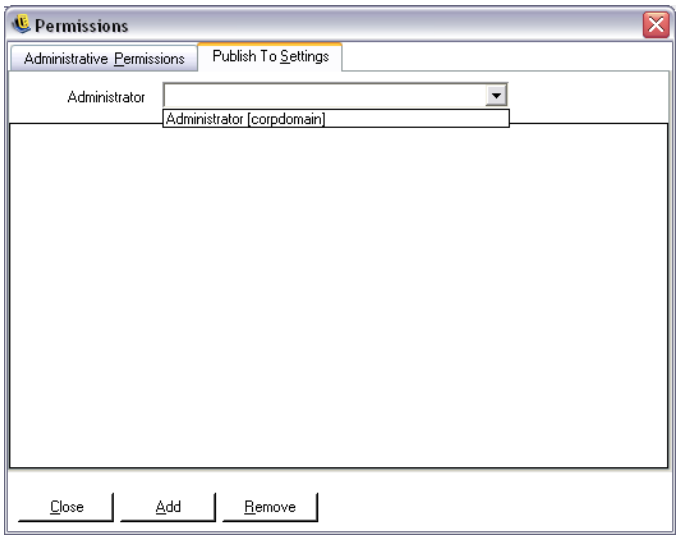
Para remover um usuário ou um grupo escolhido, selecione o nome correspondente e, em seguida, clique em *Remover*.

Definindo as Configurações de Publicar Para

Os usuários e os grupos que tiverem a opção *Publicar Política* marcada deverão ser usuários ou grupos designados para publicação. Para definir as Configurações de Publicar Para:

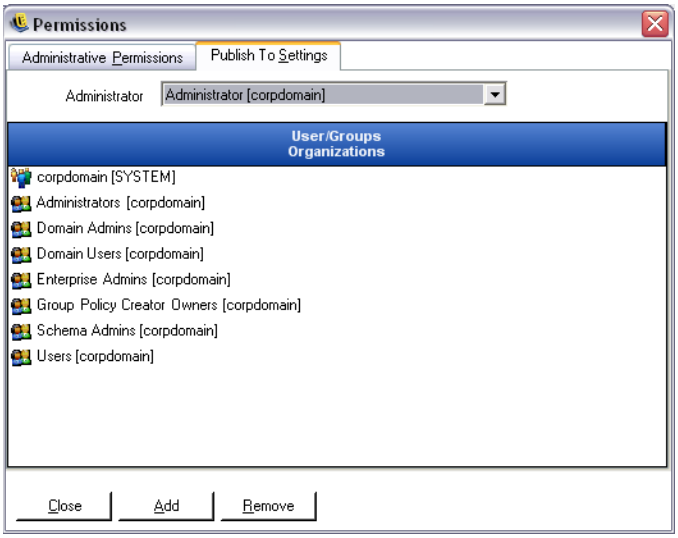
1. Clique na guia *Configurações de Publicar Para*.
2. Na lista suspensa, selecione os usuários e os grupos que receberam a permissão Publicar.

Figura 7-10 *Configurações de Publicar Para*



3. Para designar usuários e grupos e esse usuário ou grupo:
   - **3a** Clique no botão *Adicionar*, na parte inferior da tela, para exibir a tabela Organização.
   - **3b** Selecione os usuários e os grupos apropriados na lista. Use as teclas Ctrl e Shift para selecionar vários usuários.
   - **3c** Quando todos os usuários ou grupos tiverem sido selecionados, clique no botão *OK*.

Figura 7-11 *Lista Publicar Para*



Para remover um usuário ou um grupo escolhido, selecione o nome correspondente na lista e, em seguida, clique em *Remover*.

As configurações de permissão são implementadas imediatamente. Dessa forma, o administrador só precisará clicar em *Fechar* e aceitar as mudanças para retornar ao editor.

Quando um novo serviço de diretório é adicionado, a Conta de Recurso recebe configurações de permissão totais, conforme descrito anteriormente.

7.2.3 Publicando uma política

Para publicar uma política de segurança com as configurações padrão:

1. Clique em *Criar Nova Política*.
2. Dê um nome para a política e, em seguida, clique em *Criar*.
3. Grave a política e clique na guia *Publicar*.
4. Como os usuários do Endpoint Security Client devem registrar entrada para serem exibidos na árvore, você deve selecionar o topo da árvore à esquerda e, em seguida, clicar duas vezes para preencher o campo de publicação com todos os usuários e grupos atuais.
5. Clique em *Publicar* para enviar a política para o Serviço de Distribuição de Política.

A política gerada dessa maneira tem as seguintes características:

- Uma localização única (Desconhecida) é criada.
- Unidades de CD/DVD ROM são permitidas.
- Dispositivos de armazenamento removíveis são permitidos.
- Todas as portas de comunicação (incluindo Wi-Fi) são permitidas.
- A Configuração de Firewall Tudo Adaptável (todo o tráfego de saída que passar pelas portas de rede é permitido; todo o tráfego de entrada não solicitado que passar pelas portas de rede é proibido) é incluída.

Para obter informações sobre como criar uma política de segurança mais robusta, consulte o *Guia de Administração do ZENworks Endpoint Security Management*.

Continue na Capítulo 8, “Executando a instalação do Client Location Assurance Service” na página 55.

7.3 Instalando o Leitor USB

O Leitor USB da Novell é fornecido no pacote de instalação. Ele ajuda o administrador na criação de listas de dispositivos USB permitidos.

Para instalar o leitor:

1. Clique em *Instalar* para iniciar a instalação.
2. Na tela de boas-vindas, clique em *Avançar* para continuar.
3. Aceite o contrato de licença e clique em *Avançar*.
4. Na tela de informações do cliente, especifique as informações da organização e o nome de usuário apropriados e determine se o acesso ao software deve ser permitido a qualquer pessoa neste computador ou apenas ao usuário especificado.
5. Clique em *Instalar*.
6. Clique em *Concluir*.

Para obter mais informações sobre como usar o Leitor USB, consulte o *Guia de Administração do ZENworks Endpoint Security Management*.

Executando a instalação do Client Location Assurance Service

8

Este servidor só deverá ficar acessível quando o usuário entrar em um ambiente de rede controlado, para garantir que ele esteja realmente no ambiente identificado pelo ZENworks® Security Client. Instruções sobre configurações de failover e redundâncias podem ser encontradas a seguir. Se desejar, você poderá optar por implantar o CLAS (Client Location Assurance Service) no mesmo servidor que hospeda a Instalação de Servidor Único ou a instalação do Serviço de Gerenciamento de vários servidores.

Instale o CLAS em um servidor que os pontos de extremidade só conseguirão detectar quando estiverem em um ambiente de rede que exija verificação criptográfica.

A implantação do CLAS em um PDC (Primary Domain Controller - Controlador de Domínio Primário) não é suportada por razões de segurança e funcionalidade.

Observa o: É recomendado que o Servidor SSI seja configurado (reforçado) para desativar todos os aplicativos, serviços, contas e outras opções desnecessárias para a funcionalidade destinada do servidor. As etapas envolvidas dependem das especificações do ambiente local e, portanto, não podem ser descritas antecipadamente. Os administradores são avisados para consultar a seção apropriada da página da Web de segurança Microsoft TechNet (http://www.microsoft.com/technet/security/default.mspx). Recomendações adicionais de controle de acesso são fornecidas no *Guia de Administração do ZENworks Endpoint Security Management*.

Para restringir o acesso a máquinas confiáveis, configure o diretório virtual e o IIS para ter ACLs. Consulte os artigos a seguir:

- Granting and Denying Access to Computers (Concedendo e negando o acesso a computadores) (http://www.microsoft.com/technet/prodtechnol/windows2000serv/default.mspx)
- Restrict Site Access by IP Address or Domain Name (Restringir o acesso a site por endereço IP ou nome de domínio) (http://support.microsoft.com/default.aspx?scid=kb%3BEN-US%3BQ324066)
- IIS FAQ: 2000 IP address and domain name restrictions (FAQ do IIS: Restrições de endereço IP 2000 e nome de domínio) (http://www.iisfaq.com/default.aspx?View=A136&P=109)
- Working With IIS Packet Filtering (Trabalhando com filtragem de pacotes do IIS) (http://www.15seconds.com/issue/011227.htm)

Por motivos de segurança, é altamente recomendável que as seguintes pastas padrão sejam removidas de qualquer instalação do IIS:

- `IISHelp`
- `IISAdmin`
- `Scripts`
- `Impressoras`

Também recomendamos o uso da ferramenta IIS Lockdown Tool 2.1 disponível em microsoft.com (http://www.microsoft.com/technet/security/tools/locktool.mspx).

A versão 2.1 é orientada por gabaritos fornecidos para os principais produtos Microsoft dependentes do IIS. Selecione o gabarito que melhor corresponda à função deste servidor. Em caso de dúvida, o gabarito de servidor Web Dinâmico é recomendado.

Antes de iniciar a instalação, verifique se os seguintes pré-requisitos são atendidos:

- ❑ Verifique a resolução de nome do servidor MS (Serviço de Gerenciamento) para DS (Serviço de Distribuição de Política): confirme se o computador de destino em que o MS está instalado pode realizar ping no nome do servidor DS (NETBIOS se o DS for configurado dentro do firewall de rede ou FQDN se for instalado fora, na DMZ).
- ❑ Habilite ou instale o IIS (Serviços de Informações da Internet) da Microsoft e verifique se o ASP.NET está habilitado.

  Importante: Não marque a caixa de seleção *Exigir canal de segurança (SSL)* na página Comunicações de Segurança. (No utilitário Gerenciamento do Computador da Microsoft, expanda *Serviços e Aplicativos* > expanda *Gerenciador dos Serviços de Informações da Internet (ISS)* > expanda *Sites* > clique o botão direito do mouse em *Site Padrão* > clique em *Propriedades* > clique na guia *Segurança de Diretório* > clique no botão *Editar* na caixa de grupo Comunicações de segurança.) A habilitação dessa opção interrompe a comunicação entre o servidor e o cliente ZENworks Endpoint Security Management no ponto de extremidade.

Clique em *Instalação do Client Location Assurance Service* no menu da interface de Instalação. A instalação do CLAS é iniciada.

Na inicialização, o programa de instalação verifica se todos os softwares necessários estão presentes no servidor. Se algum software estiver ausente, ele será instalado automaticamente antes que a instalação prossiga para a tela de boas-vindas (talvez seja necessário aceitar os contratos de licença dos softwares adicionais). Se o MDAC (Microsoft Data Access Components) 2.8 não estiver instalado, o servidor deverá ser reinicializado após instalação desse recurso e antes da conclusão da instalação do ZENworks Endpoint Security Management. Se você estiver usando o Windows 2003 Server, o ASP.NET 2.0 será configurado para ser executado pelo programa de instalação.

8.1 Etapas de instalação

Para instalar o CLAS e gerar uma chave de licença:

1. Clique em *Avançar* na tela de boas-vindas para continuar.
2. Aceite o Contrato de Licença e clique em *Avançar*.
3. A instalação copiará os arquivos para o diretório padrão: `\Arquivos de Programas\Novell\ESM CLAS`.
4. A instalação do Client Location Assurance Service gera duas chaves: a privatekey (chave privada) e a publickey (chave pública). O arquivo publickey pode ser armazenado na área de trabalho ou em um diretório diferente. Se você quiser armazenar o arquivo publickey em um diretório diferente, clique em *Sim* e procure a pasta desejada. Clique em *Não* para aceitar o padrão e armazenar o arquivo publickey com o arquivo privatekey.
5. Clique em *Concluir* para fechar o programa de instalação.

A chave pública deve ser acessível ao Serviço de Gerenciamento.

8.2 Instalações de failover do CLAS

Várias iterações do CLAS podem ser instaladas em servidores por toda a empresa para proteger criptograficamente vários locais da empresa ou assegurar que, caso o servidor CLAS principal fique inativo, o local possa permanecer protegido.

No segundo caso, a chave privada é localizada com base no URL, não no endereço IP. Assim, um bloco de servidores pode ser configurado para compartilhar um único URL. O CLAS pode ser instalado em um único servidor e, em seguida, a imagem desse servidor pode ser copiada para cada servidor adicional. O CLAS também pode ser instalado em cada servidor separadamente; as chaves privada e pública serão copiadas para os outros servidores. Todos os servidores de um bloco de URLs devem ter as mesmas chaves privada e pública.

8.3 Transferindo a chave pública para o serviço de gerenciamento

Depois de concluída a instalação, a chave pública gerada, que é transferida pela política de segurança para o Endpoint Security Client, será armazenada no diretório `\Arquivos de Programas\Novell\Novell ESM CLAS` no servidor. A chave pública é identificada pelo nome de arquivo `publickey`. Esse nome de arquivo pode ser alterado para qualquer outro desejado.

O arquivo publickey deve ser copiado e transferido para o Serviço de Gerenciamento (qualquer lugar do serviço). Isso permite que o Console de Gerenciamento acesse e distribua a chave para todos os Endpoint Security Clients por meio de uma política de segurança. O arquivo `publickey` também pode ser carregado em um PC que esteja executando um Console de Gerenciamento do ZENworks Endpoint Security Management.

Continue na Capítulo 9, “Instalação do Endpoint Security Client 3.5” na página 59.

Instalação do Endpoint Security Client 3.5

9

Use o Novell ZENworks Endpoint Security Client 3.5 para clientes Windows XP (SP1 e SP2) e Windows 2000 SP4. No menu da interface de Instalação, clique no programa de instalação apropriado do *ZENworks Security Client*. A instalação do Endpoint Security Client é iniciada. As páginas a seguir descrevem o processo de instalação Básica e MSI.

- A Instalação Básica instala o Endpoint Security Client 3.5 apenas na máquina atual.
- A Instalação MSI inicia o programa de instalação no modo Administrativo (`/a`) e cria um Pacote MSI do software. Em seguida, esse pacote pode ser aplicado ou de outra forma disponibilizado em um local de rede especificado, com as entradas de usuário necessárias pré-configuradas. Isso permite que usuários individuais instalem o software com os valores de servidor predefinidos.

9.1 Instalação Básica do Endpoint Security Client 3.5

Esse procedimento instala o Endpoint Security Client 3.5 apenas na máquina atual.

Verifique se todos os patches de segurança do software antivírus e da Microsoft estão instalados e atualizados.

Instale os Certificados Raiz SSL do Serviço de Gerenciamento na máquina local (`ESM-MS.cer` ou o certificado corporativo).

Observa o: Recomendamos que o software antivírus/spyware que esteja interagindo com as funções de registro válidas seja encerrado durante a instalação do Endpoint Security Client 3.5.

---

1. Clique em *Avançar* na tela de boas-vindas para continuar.
2. Aceite o Contrato de Licença e clique em *Avançar*.
3. Digite uma senha de instalação. Isso impede que o usuário desinstale o Endpoint Security Client 3.5 em *Adicionar ou Remover Programas* (recomendável).

Figura 9-1 *Senha de desinstalação*

4 Selecione como as políticas serão recebidas (do Serviço de Distribuição para clientes gerenciados ou recuperados localmente para uma configuração não gerenciada [consulte Capítulo 11, “Instalação não gerenciada do ZENworks Endpoint Security Management” na página 75 para obter detalhes sobre configuração não gerenciada]).

Figura 9-2 *Configurações de gerenciamento*

5 Especifique as informações do Serviço de Gerenciamento.

6 Determine se as políticas devem ser recebidas para usuários ou para a máquina (políticas baseadas em máquina).

Figura 9-3 *Políticas baseadas em usuário ou em máquina*

7 Clique em *Instalar*.

Após a instalação do software, o usuário será solicitado a reiniciar a máquina.

Observa o: Como alternativa, antes de executar a instalação, você poderá copiar o certificado do Serviço de Gerenciamento em um pasta co-localizada com o arquivo `setup.exe`. Esse procedimento instala automaticamente o certificado na máquina (por exemplo, para todos os usuários). Esse processo também pode ser executado com o arquivo `dat` da licença da Novell.

9.2 Instalação MSI

Esse procedimento cria um Pacote MSI para o Endpoint Security Client 3.5. Esse pacote é usado por um administrador do sistema para publicar a instalação para um grupo de usuários por meio de uma política do Active Directory ou de outros métodos de distribuição de software.

Para criar o pacote MSI:

Se você estiver executando a instalação a partir do CD ou do programa de instalação master ISO e não pretender executar nenhuma variável de linha de comando (consulte a Seção 9.2.1, “Variáveis de linha de comando” na página 64):

1 Insira o CD e aguarde o programa de instalação master ser iniciado.
2 Clique em *Instalação do Produto*.
3 Clique em *Security Client*.
4 Clique em *Criar Pacote MSI do ZSC*.

Se estiver usando apenas o arquivo `setup.exe` para a instalação (o executável pode ser encontrado no CD em `D:\ESM32\ZSC`), comece da seguinte maneira:

1 Clique o botão direito do mouse no arquivo `setup.exe`.
2 Selecione *Criar Atalho*.
3 Clique o botão direito do mouse no atalho e, em seguida, clique em *Propriedades*.
4 No fim do campo Destino, depois das aspas, insira um espaço e digite `/a`.

Por exemplo: "`C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a`

Diversas variáveis de linha de comando estão disponíveis para a instalação do MSI. Consulte a Seção 9.2.1, “Variáveis de linha de comando” na página 64 para obter mais detalhes.

5 Clique em *OK*.

6 Clique duas vezes no atalho para iniciar o programa de instalação MSI.

Quando a instalação for iniciada:

1 Clique em *PRÓXIMO* na tela de boas-vindas para continuar.

2 Aceite o Contrato de Licença e clique em *Avançar*.

3 Selecione se uma senha de desinstalação é exigida (recomendado) e digite a senha.

4 Selecione como as políticas serão recebidas (do Serviço de Distribuição para clientes gerenciados, recuperadas localmente para uma configuração não gerenciada). Se a configuração gerenciada for selecionada:

- Especifique as informações do Serviço de Gerenciamento (nome FQDN ou NETBIOS, dependendo do que foi inserido na instalação do Serviço de Gerenciamento).
- Determine se as políticas serão baseadas em usuário ou em máquina.

5 (Opcional) Se desejar ser notificado caso ocorram falhas na instalação, especifique um endereço de e-mail no campo fornecido.

6 Especifique a localização de rede na qual a imagem MSI será criada ou clique no botão *Mudar* para procurar essa localização.

Figura 9-4 *Selecione Local de Rede para Imagem MSI.*

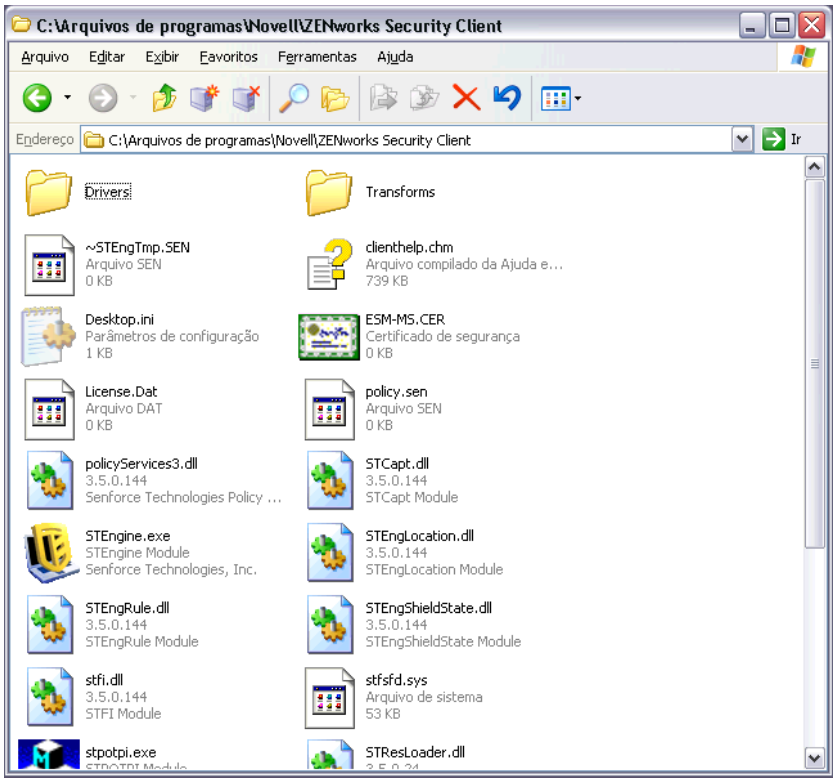
7 Clique em *Instalar* para criar a imagem MSI.

8 Procure a imagem MSI criada e abra a pasta "`\Arquivos de programa\Novell\ZENworks Security Client\`".

9 Copie o certificado SSL do Serviço de Gerenciamento (`ESM-MS.cer` ou o certificado corporativo) e a Chave de Licença da Novell para essa pasta, substituindo os arquivos padrão de 0 KB existentes na pasta. O certificado SSL do ESM-MS está disponível na pasta

`ZENworks Endpoint Security Management Setup Files`. A chave de licença é enviada por e-mail separadamente (se você estiver usando uma versão de avaliação de 30 dias, nenhuma chave de licença será necessária nesse momento).

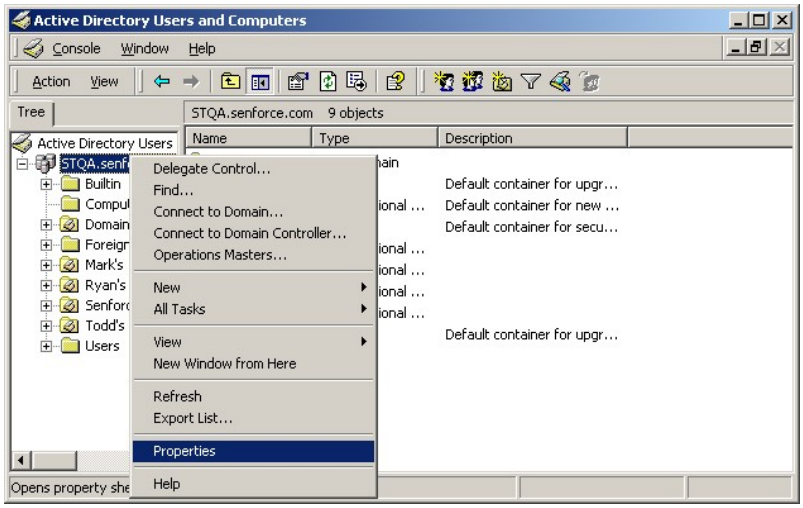
Figura 9-5 *Substituir os arquivos padrão no pacote MSI*



Para definir o pacote MSI a ser aplicado a grupos de usuários como uma Política de Grupo:

1 Abra *Ferramentas Administrativas - Usuários e Computadores do Active Directory* e, em seguida, abra *Domínio Raiz* ou *Propriedades da OU*.

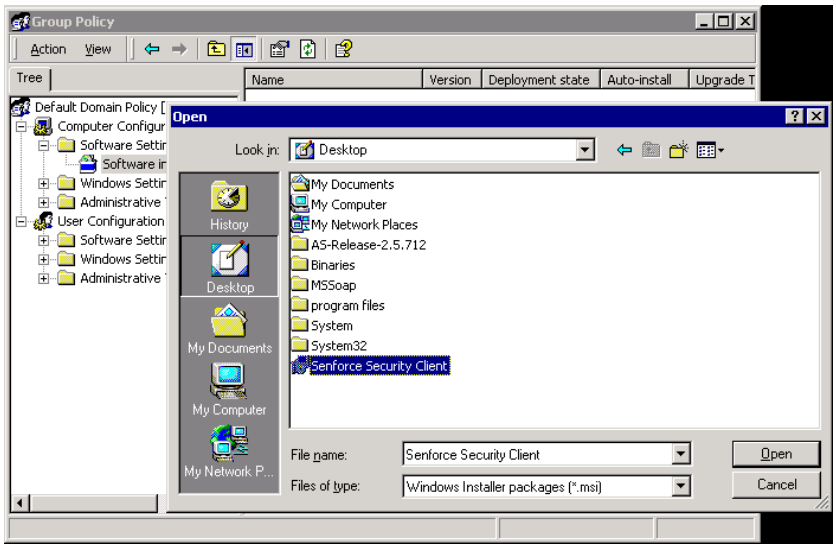
Figura 9-6 *Abra Propriedades em Domínio Raiz ou OU.*



2 Clique na guia *Política de Grupo* e em *Editar*.

3 Adicione o Pacote MSI à Configuração do Computador.

Figura 9-7 *Selecione o pacote MSI a ser adicionado.*



9.2.1 Variáveis de linha de comando

Opções de variáveis de linha de comando estão disponíveis para a instalação MSI. Essas variáveis devem ser definidas no atalho executável configurado para ser executado no modo de administrador. Para usar uma variável, a seguinte linha de comando deve ser digitada no atalho MSI:

`"...\setup.exe" /a /V"variáveis"`. Digite qualquer um dos comandos a seguir entre aspas. Separe diversas variáveis com um único espaço.

Exemplo: `setup.exe /a /V"STDRV=stateful STBGL=1"` cria um pacote MSI em que o Endpoint Security Client 3.5 será inicializado em Todos com Informações de Estado com o uso obrigatório da lista de permissões assegurado.

Observa o: Reinicializar com informações de estado pode causar alguns problemas de interoperabilidade (atrasos de endereço DHCP, problemas de interoperabilidade da rede da Novell, etc.).

As seguintes variáveis de linha de comando estão disponíveis:

Tabela 9-1 *Variáveis de linha de comando*

Variável de linha de comando	Descrição	Notas
STDRV=stateful	Driver NDIS all stateful no momento da inicialização.	Muda o estado padrão do driver NDIS de Tudo Aberto para Todos com Informações de Estado, permitindo o tráfego total da rede no momento da inicialização, até que o Endpoint Security Client 3.5 tenha determinado sua localização.
/qn	Instalação silenciosa.	Use para suprimir o processo de Instalação MSI típico. O Endpoint Security Client 3.5 será ativado na próxima reinicialização do usuário.
STRBR=ReallySuppress	Nenhuma reinicialização após conclusão da instalação.	A aplicação do uso obrigatório da segurança e a autodefesa do cliente não estarão completamente funcionais até que a primeira reinicialização seja realizada.
STBGL=1	A aplicação do uso obrigatório da lista de permissões exata no controle de aplicativo.	Uma política DEVE ser criada para identificar o aplicativo na lista de permissões e distribuída com essa política.
STUPGRADE=1	Faz upgrade do Endpoint Security Client 3.5.	Use para fazer upgrade do Endpoint Security Client 3.5.
STUNINSTALL=1	Desinstala o Endpoint Security Client 3.5.	Use para desinstalar o Endpoint Security Client 3.5.
STUIP=”a senha”	Desinstala com senha.	Use quando uma senha de desinstalação estiver ativa.
STNMS=”Nome do MS”	Muda o nome do Serviço de Gerenciamento.	Muda o nome do Serviço de Gerenciamento do Endpoint Security Client 3.5.
POLICYTYPE=1	Muda o Endpoint Security Client 3.5 para políticas baseadas em máquina.	Use para mudar Endpoint Security Clients instalados pelo MSI para aceitar políticas baseadas em máquina, em vez de políticas baseadas em usuário.
POLICYTYPE=2	Muda o Endpoint Security Client 3.5 para políticas baseadas em usuário.	Use para mudar Endpoint Security Clients instalados pelo MSI para aceitar políticas baseadas em usuário, em vez de políticas baseadas em máquina.
STVA=”Nome do adaptador”	Adiciona o adaptador virtual.	Use para ativar o controle de políticas com um adaptador virtual.

Variável de linha de comando	Descrição	Notas
/L*v c:\log.txt	Ativa o registro.	Use para ativar o registro na instalação. Caso contrário, isso deverá ser feito com as ferramentas de Diagnósticos do Endpoint Security Client. (Consulte o Manual do Administrador.)

9.2.2 Distribuindo uma política com o pacote MSI

A política padrão fornecida na instalação MSI pode ser substituída por uma política configurada pela empresa. Para aplicar uma política específica com a imagem MSI:

1. Crie uma política para ser distribuída a todos os usuários por meio do Console de Gerenciamento. (Consulte o *Guia de Administração do ZENworks Endpoint Security Management* para obter detalhes sobre Criação de Política.)
2. Exporte a política e grave-a como `policy.sen`.

   Observa o: Todas as políticas distribuídas dessa maneira (não gerenciadas) devem ser denominadas `policy.sen` para que o Endpoint Security Client 3.5 as aceite. As políticas que não forem denominadas `policy.sen` não serão implementadas pelo Endpoint Security Client 3.5.
3. Abra a pasta para a qual a política foi exportada e copie os arquivos `policy.sen` e `setup.sen`.
4. Procure a imagem MSI criada e abra a pasta `"\Arquivos de Programas\Novell\ZENworks Security Client\"`.
5. Cole os arquivos `policy.sen` e `setup.sen` na pasta. Isso substituirá os arquivos `policy.sen` e `setup.sen` padrão.

9.2.3 Instalação do usuário do Endpoint Security Client 3.5 a partir do MSI

Quando o usuário se autenticar novamente no domínio (reinicializando a máquina), o pacote de instalação do MSI será executado antes do login. Depois que a instalação do MSI for concluída, a máquina será reinicializada e o usuário poderá efetuar login. O Endpoint Security Client 3.5 está instalado e em execução na máquina.

9.3 Executando o Endpoint Security Client 3.5

O Endpoint Security Client 3.5 é executado automaticamente na inicialização do sistema. Para obter mais informações sobre o Endpoint Security Client 3.5, consulte o *Guia do Usuário do ZENworks Endpoint Security Client 3.5*.

O Guia do Usuário pode ser distribuído a todos os usuários para ajudá-los a compreender melhor o funcionamento de seu novo software de segurança de ponto de extremidade.

Instalação do ZENworks Endpoint Security Client 4.0

10

O Novell® ZENworks® Endpoint Security Client 4.0 é uma versão cliente que suporta o Microsoft Windows Vista com Support Pack 1 executado no modo de 32 bits e o Windows Server 2008 executado no modo de 32 bits. O Endpoint Security Client 4.0 usa o ZENworks Endpoint Security Management 3.5 Server e o Console de Gerenciamento. Agora você pode gerenciar o Windows XP com o cliente 3.5 e o Windows Vista com o cliente 4.0.

As páginas a seguir descrevem o processo de instalação Básica e MSI.

A Instalação Básica instala o Endpoint Security Client 4.0 apenas na máquina atual.

A Instalação MSI inicia o programa de instalação no modo Administrativo (`/a`) e cria um pacote MSI do software. Em seguida, esse pacote pode ser aplicado ou de outra forma disponibilizado em um local de rede especificado, com as entradas de usuário necessárias pré-configuradas. Isso permite que usuários individuais instalem o software com valores de servidor predefinidos.

10.1 Instalação Básica do Endpoint Security Client 4.0

Esse procedimento instala o ZENworks Endpoint Security Client 4.0 apenas na máquina atual.

Antes de começar:

- Verifique se todos os patches de segurança do software antivírus e da Microsoft estão instalados e atualizados. O software Endpoint Security Client 4.0 pode ser instalado no Windows Vista Support Pack 1 e no Windows Server 2008, ambos executados no modo de 32 bits.
- A Novell recomenda que o software antivírus/spyware que esteja interagindo com as funções de registro válidas seja encerrado durante a instalação do Endpoint Security Client 4.0.
- O Endpoint Security Client Gerenciado requer comunicação SSL com o componente ZENworks Endpoint Security Management Service. Se você tiver selecionado “certificados auto-assinados” durante a instalação do Serviço de Gerenciamento ou do Servidor Único, o ponto de extremidade que estiver executando o Security Client deverá ter o certificado instalado no contexto apropriado (de preferência no contexto do computador local).

  Para fazer isso automaticamente, coloque o arquivo `ESM-MS.cer` na mesma pasta que o arquivo `Setup.exe` do programa de instalação do Endpoint Security Client. Como alternativa, você pode copiar toda a pasta `ESM Setup Files` da instalação do Serviço de Gerenciamento (ou da instalação do Servidor Único) para a pasta que contém o arquivo `Setup.exe` do programa de instalação do Endpoint Security Client (verifique se o arquivo

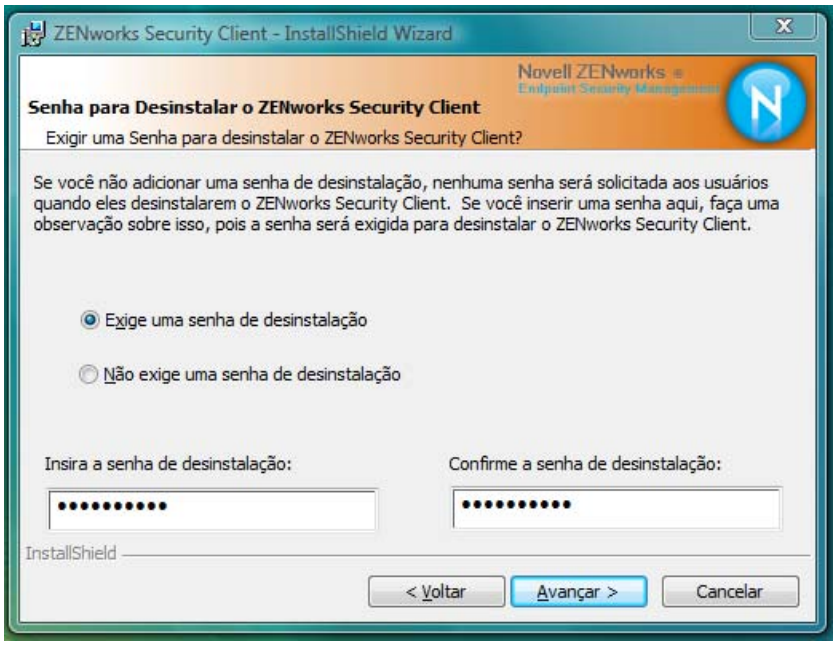
`ESM-MS.cert` está na pasta `ESM Setup Files` e se o nome da pasta é `ESM Setup Files`). Esse procedimento instala automaticamente o certificado na máquina (por exemplo, para todos os usuários). Esse processo também pode ser executado com o arquivo `dat` da licença da Novell.

No menu da interface de Instalação, selecione o diretório do programa de instalação apropriado do *ZENworks Security Client*.

1. Clique duas vezes em `Setup.exe` para iniciar o processo de instalação.
2. Escolha o idioma da instalação e clique em *OK*.

   Estas são as opções de idioma:

   - Chinês simplificado
   - Chinês tradicional
   - Inglês (padrão)
   - Francês
   - Alemão
   - Italiano
   - Japonês
   - Português
   - Espanhol tradicional
3. O Endpoint Security Client 4.0 exige que você instale o Microsoft Web Services Enhancements (WSE) 2.0 com Service Pack 3 e o Microsoft Visual C++ 2008 antes de instalar o cliente. Se o processo de instalação não detectar esses componentes, a tela a seguir será exibida. Clique em *Instalar* para instalar esses requisitos.
4. Caso ainda não o tenha feito, desative os softwares antivírus e anti-spyware antes de clicar em *Avançar* na tela de boas-vindas.
5. Aceite o Contrato de Licença e clique em *Avançar*.

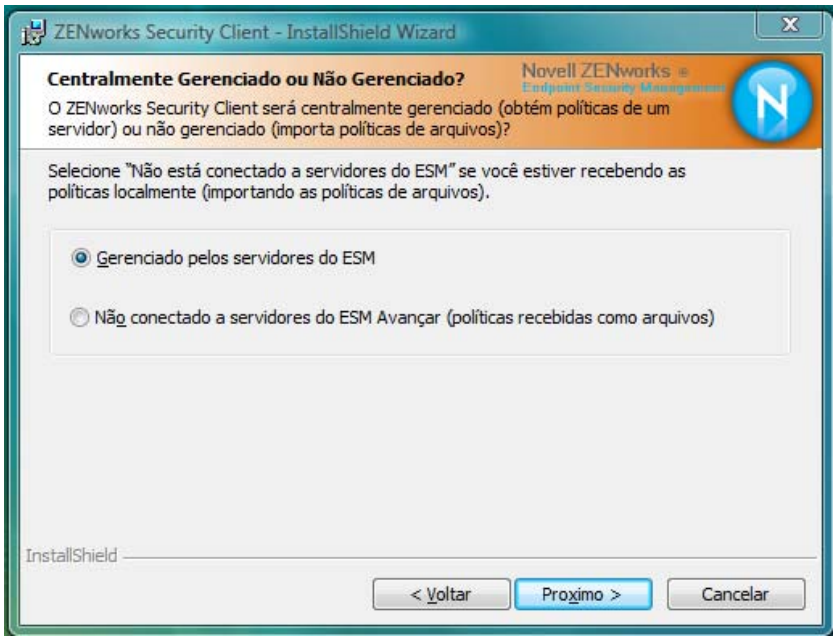


6 Selecione *Requer uma senha de desinstalação*. Isso impede que o usuário desinstale o Endpoint Security Client 4.0 (recomendável).

7 Adicione uma senha de desinstalação, confirme a senha e clique em *Avançar*.

8 Selecione um tipo de política (uma Política Baseada em Usuário, em que cada usuário possui uma política individual, ou uma Política Baseada em Computador, em que uma única política é utilizada para todos os usuários). Clique em *Avançar*.

Observa o: Selecione Política Baseada em Usuário se sua rede utilizar o eDirectory como Serviço de Diretório. O eDirectory não suporta políticas baseadas em computador.



9 Selecione o modo de recebimento das políticas — gerenciadas por meio de servidores ESM para clientes gerenciados ou recuperadas localmente para uma configuração não gerenciada (independente). Clique em *Avançar*.

   Para obter detalhes sobre instalações não gerenciadas, consulte Capítulo 11, "Instalação não gerenciada do ZENworks Endpoint Security Management" na página 75.

10 (Opcional) Se tiver selecionado *Gerenciado por servidores do ESM* na Etapa 9, digite o nome do servidor que suporta o Serviço de Gerenciamento.

   O nome do servidor inserido deve ser igual ao nome de "Emitido para" fornecido no certificado raiz confiável usado no servidor em que você instalou o Servidor Único ou o Serviço de Gerenciamento do ZENworks Endpoint. Esse nome é o nome NETBIOS ou FQDN (nome completo do domínio) do servidor que está executando o componente Serviço de Gerenciamento do ZENworks Endpoint. Depois de inserir o nome, clique em *Avançar*.

11 Clique em *Instalar* para iniciar a instalação.

12 Após a instalação do software, reinicie a máquina ao ser solicitado.

   Para obter uma lista dos recursos que não estão disponíveis no Cliente 4.0 para Vista, consulte Seção 10.4, "Recursos não suportados no Endpoint Security Client 4.0" na página 74.

10.2 Instalação MSI

Esse procedimento cria um pacote MSI para o Endpoint Security Client 4.0. Esse pacote é usado por um administrador do sistema para publicar a instalação para um grupo de usuários por meio de uma política do Active Directory ou de outros métodos de distribuição de software.

10.2.1 Usando o programa de instalação master

Se você estiver executando a instalação a partir do CD ou do programa de instalação master ISO e não pretender executar nenhuma variável de linha de comando:

1 Insira o CD e aguarde o programa de instalação master ser iniciado.

2 Clique em *Instalação do Produto*.

3 Clique em *Security Client*.

4 Clique em *Criar Pacote MSI do ZSC*.

5 Continue em Seção 10.2.3, "Concluindo a instalação" na página 71.

10.2.2 Usando o arquivo Setup.exe

Se estiver usando apenas o arquivo `setup.exe` para instalação:

1 Clique o botão direito do mouse no arquivo `setup.exe`.

   O executável pode ser encontrado no CD, em `D:\ESM32\ZSC`.

2 Selecione *Criar Atalho*.

3 Clique o botão direito do mouse no atalho e, em seguida, clique em *Propriedades*.

4 No final do campo *Destino*, depois das aspas, pressione a barra de espaço uma vez para inserir um espaço e digite `/a`.

Por exemplo: `"C:\Documents and Settings\euser\Desktop\CL-Release-3.2.455\setup.exe" /a`

Há diversas variáveis de linha de comando disponíveis para a instalação MSI. Consulte Seção 9.2.1, “Variáveis de linha de comando” na página 64 para obter mais detalhes.

5 Clique em *OK*.

6 Clique duas vezes no atalho para iniciar o programa de instalação MSI.

7 Continue em Seção 10.2.3, “Concluindo a instalação” na página 71.

10.2.3 Concluindo a instalação

Conclua Usando o programa de instalação master ou Usando o arquivo Setup.exe e, em seguida, use este procedimento para finalizar a instalação do cliente.

1 Clique em *AVANÇAR* na tela de boas-vindas para continuar.

2 Selecione *Requer uma senha de desinstalação* (recomendável) e digite a senha. Clique em *Avançar*.

Observa o: Se desinstalar o Endpoint Security Client por meio de um pacote MSI, você deverá especificar a senha de desinstalação usando as propriedade do MSI. (Consulte Tabela 10-1 na página 72.)

---

3 Selecione um tipo de política (uma Política Baseada em Usuário, em que cada usuário possui uma política individual, ou uma Política Baseada em Computador, em que uma única política é utilizada para todos os usuários). Clique em *Avançar*.

Observa o: Selecione Política Baseada em Usuário se sua rede utilizar o eDirectory como Serviço de Diretório. O eDirectory não suporta políticas baseadas em computador.

---

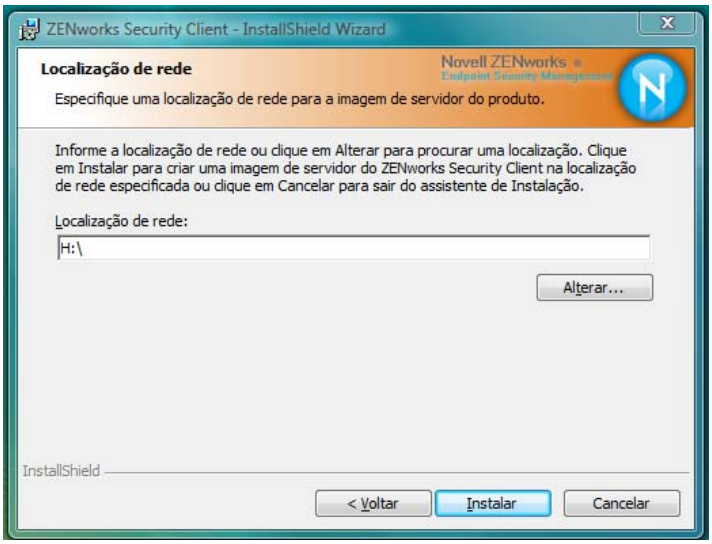
4 Selecione o modo de recebimento das políticas — gerenciadas por meio de servidores ESM para clientes gerenciados ou recuperadas localmente para uma configuração não gerenciada (independente).

5 (Opcional) Se tiver selecionado *Gerenciado por servidores do ESM* na Etapa 4:

- O nome do servidor inserido deve ser igual ao nome de “Emitido para” fornecido no certificado raiz confiável usado no servidor em que você instalou o Servidor Único ou o Serviço de Gerenciamento do ZENworks Endpoint. Esse nome é o nome NETBIOS ou FQDN (nome completo do domínio) do servidor que está executando o componente Serviço de Gerenciamento do ZENworks Endpoint.

6 (Opcional) Se desejar ser notificado caso ocorram falhas na instalação, especifique um endereço de e-mail no campo fornecido.

7 Especifique o local de rede em que deseja criar a imagem MSI ou clique no botão *Mudar* para procurar e selecionar o local.



8 Clique em *Instalar* para criar a imagem MSI. Clique em *Concluir* para fechar o programa de instalação.

9 Procure o local onde a imagem MSI foi criada e abra a pasta `\Arquivos de Programas\Novell ZENworks\Endpoint Security Client\`.

10 Copie o certificado SSL do Serviço de Gerenciamento (`ESM-MS.cer` ou o certificado corporativo) e a chave de licença da Novell para essa pasta, substituindo os arquivos padrão de 0 KB existentes na pasta.

O certificado SSL do ESM-MS está disponível na pasta `ZENworks Endpoint Security Management Setup Files`. A chave de licença é enviada separadamente por e-mail. Se estiver usando a avaliação de 60 dias, você não precisará de nenhuma chave de licença.

10.2.4 Variáveis de linha de comando

Há opções de variáveis de linha de comando disponíveis para instalações MSI. Essas variáveis devem ser definidas no atalho do executável configurado para ser executado no modo de administrador. Para usar uma variável, a seguinte linha de comando deve ser digitada no atalho MSI:

`"...\setup.exe" /a /V"variáveis"`. Digite qualquer um dos comandos a seguir entre aspas. Separe diversas variáveis com um único espaço.

As seguintes variáveis de linha de comando estão disponíveis:

Tabela 10-1 *Variáveis de linha de comando*

Variável de linha de comando	Descrição	Notas
/qn	Instalação silenciosa.	Suprime o processo de instalação MSI típica. O Endpoint Security Client será ativado na próxima reinicialização do usuário.

Variável de linha de comando	Descrição	Notas
SESMSG=1	Mostra ao usuário final uma mensagem informando que a criptografia dos arquivos localizados em “Safe Harbors” não poderá ser removida automaticamente se uma Política de Criptografia for implantada.	Para tornar a desinstalação “silenciosa”, o valor padrão é 0 (não exibir mensagens).
STRBR=ReallySuppress	Nenhuma reinicialização após conclusão da instalação.	O uso obrigatório de segurança e a autodefesa do cliente só estarão completamente funcionais depois que a primeira reinicialização for realizada.
STUPGRADE=1	Faz upgrade do Endpoint Security Client 4.0.	Faz upgrade do Endpoint Security Client 4.0.
STUNINSTALL=1	Desinstala o Endpoint Security Client 4.0.	Desinstala o Endpoint Security Client 4.0.
STUIP=”a senha”	Desinstalar com senha	Use essa variável quando uma senha de desinstalação estiver ativa.
STNMS=”Nome do MS”	Muda o nome do Serviço de Gerenciamento.	Muda o nome do Serviço de Gerenciamento do Endpoint Security Client 4.0.
POLICYTYPE=1	Muda o Endpoint Security Client 4.0 para políticas baseadas em máquina.	Muda os Endpoint Security Clients instalados por MSI para aceitar políticas baseadas em máquina em vez de políticas baseadas em usuário.
POLICYTYPE=2	Muda o Endpoint Security Client 4.0 para políticas baseadas em usuário.	Muda os Clientes ZENworks Security 4.0 para Vista instalados pelo MSI para aceitar políticas baseadas em usuário em vez de políticas baseadas em máquina.
STVA=”Nome do adaptador”	Adiciona um adaptador virtual.	Ativa o controle de políticas sobre um adaptador virtual.
/L*v c:\log.txt	Ativa o registro.	Ativa o registro na instalação. Se não usar essa variável, você deverá utilizar as ferramentas de Diagnóstico do Endpoint Security Client para fazer o registro.

10.2.5 Distribuindo uma política com o pacote MSI

A política padrão fornecida na instalação MSI pode ser substituída por uma política configurada pela empresa. Para aplicar uma política específica com a imagem MSI:

1 Crie uma política para ser distribuída a todos os usuários por meio do Console de Gerenciamento. (Consulte o *Guia de Administração do ZENworks Endpoint Security Management* para obter detalhes sobre Criação de Política.)

2 Exporte a política e renomeie-a como `policy.sen`.

   Todas as políticas distribuídas dessa maneira (não gerenciadas) devem ser denominadas `policy.sen` para que o Endpoint Security Client 4.0 as aceite. As políticas que não forem denominadas `policy.sen` não serão implementadas pelo Endpoint Security Client 4.0.

3 Abra a pasta para a qual a política foi exportada e copie os arquivos `policy.sen` e `setup.sen`.

4 Procure a imagem MSI criada e abra a pasta `\Arquivos de Programas\Novell ZENworks\Endpoint Security Client\`.

5 Cole os arquivos `policy.sen` e `setup.sen` na pasta. Isso substituirá os arquivos `policy.sen` e `setup.sen` padrão.

10.3 Executando o Endpoint Security Client 4.0

O Endpoint Security Client 4.0 é executado automaticamente na inicialização do sistema. Para obter mais informações sobre o Endpoint Security Client 4.0, consulte o *Guia do Usuário do ZENworks Endpoint Security Client 4.0*.

O Guia do Usuário pode ser distribuído a todos os usuários para ajudá-los a compreender melhor o funcionamento de seu novo software de segurança de ponto de extremidade.

10.4 Recursos não suportados no Endpoint Security Client 4.0

Estes são alguns dos recursos não suportados ou parcialmente suportados no Endpoint Security Client 4.0:

- Autodefesa do cliente.
- Suporte a modems.
- Criação de scripts.
- Alteração manual de firewalls em um local.
- Exibição de vários firewalls em um local. Apenas o firewall padrão está disponível.
- Regras de integridade.
- Bloqueio de aplicativos.
- As informações de ícone da área de notificação, exibidas quando o usuário passa o mouse sobre o ícone, sofreram mudanças. Agora, o ícone só mostra informações sobre Política e Localização.
- Conectividade USB.
- Gerenciamento de chave Wi-Fi.
- As conexões com fio não têm mais valor que as conexões sem fio.
- Atualizações do Endpoint Security Client (por política).
- Tempo de espera de autenticação da VPN.
- Reprodução automática para controle de dispositivo de armazenamento.
- Entradas do catálogo telefônico no ambiente de rede.

Instalação não gerenciada do ZENworks Endpoint Security Management

11

Uma empresa pode executar o ZENworks® Security Client e o Console de Gerenciamento de modo não gerenciado (sem conexão com o Serviço de Distribuição de Política ou com o Serviço de Gerenciamento). Isso está disponível como uma opção de instalação, destinada principalmente para a configuração de avaliações simples. Essa opção também é ideal para empresas com pouco ou nenhum espaço de servidor, ou com necessidades básicas de segurança. Entretanto, atualizações rápidas de política e Gerador de Relatórios de Conformidade não estão disponíveis nessa configuração.

11.1 Instalação do Endpoint Security Client não gerenciado

Para instalar um Endpoint Security Client não gerenciado, siga as instruções contidas no Capítulo 9, “Instalação do Endpoint Security Client 3.5” na página 59 e selecione a opção *Não Conectado a Servidores do ZENworks Endpoint Security Management (políticas recebidas como arquivos)*. O programa da instalação ignora as perguntas relacionadas aos nomes dos servidores e instala o Endpoint Security Client nessa máquina (também é possível criar um pacote MSI para um Endpoint Security Client Não Gerenciado).

Figura 11-1 *Selecione "Não Conectado a Servidores do ZENworks Endpoint Security Management"*

11.2 Console de Gerenciamento Independente

Essa configuração permite que um Console de Gerenciamento do ZENworks Endpoint Security Management seja instalado e crie políticas sem estabelecer uma conexão com um Serviço de Gerenciamento externo nem distribuir políticas por meio do Serviço de Distribuição de Política.

Selecione *Instalação do Console de Gerenciamento Independente* no menu Programa de Instalação Master e siga as instruções no Capítulo 7, "Executando a instalação do Console de Gerenciamento" na página 43 para a instalação.

No início do processo, um banco de dados SQL é instalado (se houver um na máquina, o programa de instalação configurará os bancos de dados apropriados). Depois que o banco de dados é instalado, o processo de instalação é interrompido. Reinicie a máquina para ativar o banco de dados SQL. Após a reinicialização, ative a instalação novamente para continuar.

A maioria das funcionalidades de política está disponível para implantação, com exceção do Gerador de Relatórios. Todos os arquivos de política exportados devem ser distribuídos para o diretório `\Arquivos de Programas\Novell\ZENworks Security Client\` do Endpoint Security Client.

11.3 Distribuindo políticas não gerenciadas

Para distribuir políticas não gerenciadas:

1. Localize e copie em uma pasta separada o arquivo `setup.sen` do Console de Gerenciamento.

   O arquivo `setup.sen` é gerado durante a instalação do Console de Gerenciamento e colocado no diretório `\Arquivos de Programas\Novell\Console de Gerenciamento do ESM\`.

2. Crie uma política no Console de Gerenciamento (para obter mais informações, consulte o *Guia de Administração do ZENworks Endpoint Security Management*).

3. Use o comando *Export* para exportar a política para a mesma pasta que contém o arquivo `setup.sen`. Todas as políticas distribuídas devem ser denominadas `policy.sen` para que o Endpoint Security Client as aceite.

4. Distribua os arquivos `policy.sen` e `setup.sen`. Esses arquivos devem ser copiados no diretório `\Arquivos de Programas\Novell\ZENworks Security Client\` de todos os clientes não gerenciados.

   O arquivo `setup.sen` só precisa ser copiado para os dispositivos não gerenciados uma vez, com a primeira política. Depois disso, somente as novas políticas precisam ser distribuídas.

Se um Endpoint Security Client Não Gerenciado for instalado na mesma máquina que o Console de Gerenciamento Independente, o arquivo `setup.sen` também deverá ser copiado no diretório `\Arquivos de Programas\Novell\ZENworks Security Client`. Se o Endpoint Security Client Não Gerenciado for instalado na máquina após o Editor Independente, o arquivo deverá ser transferido manualmente, conforme descrito acima.

Se você clicar no botão *Publicar*, a política será publicada imediatamente para o Endpoint Security Client não gerenciado dessa máquina. Para fornecer políticas a vários usuários não gerenciados, use o recurso Export, conforme descrito acima.

Atualizações da documentação

A

Esta seção contém informações sobre as mudanças do conteúdo da documentação feitas neste *Guia de Instalação do Novell ZENworks Endpoint Security Management* após o lançamento inicial para a versão 3.5. As mudanças estão listadas de acordo com a data de publicação.

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.

A documentação foi atualizada nas seguintes datas:

- Seção A.1, “5 de janeiro de 2009” na página 77

A.1 5 de janeiro de 2009

Foram feitas atualizações nas seguintes seções:

Local	Atualização
Todas as seções	O nome do cliente mudou em todo o guia. Oficialmente, ele agora é chamado de Novell ZENworks Endpoint Security Client. Em seus respectivos capítulos, os clientes são chamados Endpoint Security Client 3.5 (para Windows XP) e Endpoint Security Client 4.0 (para Windows Vista).
Seção 1.1, “Requisitos do sistema” na página 10	Requisitos do sistema adicionais para o novo cliente Vista e o Console de Gerenciamento independente.
Capítulo 9, “Instalação do Endpoint Security Client 3.5” na página 59	Informações adicionais e mudança de nome indicando que o Endpoint Security Client 3.5 é para Windows XP.
Capítulo 10, “Instalação do ZENworks Endpoint Security Client 4.0” na página 67	Capítulo adicional sobre o Endpoint Security Client 4.0 (para Windows Vista).