IBM SecureWay Policy Director

Instalação e Uso

Versão 3 Release 0

IBM SecureWay Policy Director

Instalação e Uso

Versão 3 Release 0

Nota

Antes de utilizar estas informações e o produto suportado por elas, leia as informações gerais no Apêndice A, “Avisos” na página 77.

Primeira Edição (Outubro de 1999)

Esta edição aplica-se à Versão 3, release 0, modificação 0 do produto IBM SecureWay Policy Director e a todos os releases e modificações subseqüentes, até que seja indicado diferentemente em novas edições.

Esta edição substitui o IBM SecureWay Global Sign-On, Versão 2.0.200.

Índice

Sobre este manual

Este manual fornece informações sobre a instalação e configuração do produto IBM SecureWay Policy Director (Policy Director). Os servidores Policy Director podem ser instalados nos seguintes sistemas operacionais:

Microsoft Windows NT

AIX

Solaris

O cliente NetSEAT pode ser instalado nos seguintes sistemas operacionais:

Windows 95

Windows 98

Windows NT

Quem deve ler este manual

Este manual foi escrito para o administrador responsável pelo planejamento e instalação do Policy Director.

O administrador deve ter conhecimento sobre a instalação e a configuração do IBM DCE (Distributed Computing Environment) e LDAP (Lightweight Directory Access Protocol) do IBM SecureWay Directory. Os servidores IBM SecureWay Directory e IBM Distributed Computing Environment são utilizados pelo produto Policy Director e estão incluídos no produto Policy Director.

Organização deste manual

Este manual contém os seguintes capítulos:

O Capítulo 1, “Informações sobre o produto Policy Director” na página 1 fornece uma visão geral do produto Policy Director e seus componentes.

O Capítulo 2, “Requisitos do sistema” na página 11 fornece informações sobre o os requisitos de software e hardware que seu ambiente operacional deve atender.

O Capítulo 3, “Planejamento do Policy Director” na página 15 fornece informações para ajudar você a planejar, organizar e gerenciar o Policy Director.

O Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23 fornece informações sobre a instalação e configuração do produto IBM SecureWay Directory Versão 3.1.1 (LDAP) Client SDK e servidor, se você escolher o registro de usuário LDAP. Você deve instalar e configurar o servidor LDAP antes de instalar o produto Policy Director. Além disso, o servidor LDAP deve estar em execução antes da instalação do produto Policy Director.

O Capítulo 5, “Instalação do Policy Director para Windows” na página 35 descreve a instalação e a configuração do Policy Director no sistema operacional Windows NT.

O Capítulo 6, “Instalação do Policy Director para AIX” na página 47 descreve a instalação e a configuração do produto Policy Director no sistema operacional IBM AIX.

O Capítulo 7, “Instalação do Policy Director para Solaris” na página 61 descreve a instalação e a configuração do Policy Director no sistema operacional Sun Solaris.

O Capítulo 8, “Documentação Relacionada” na página 73 informa onde encontrar outras documentações referentes ao produto Policy Director e a documentação para produtos relacionados.

Novidades deste Release

Este release do produto Policy Director inclui os seguintes novos recursos:

Suporte para o produto IBM SecureWay Directory para armazenamento de informações de credenciais de usuário e de grupo.

As últimas atualizações sobre a especificação da API de Autorização do Open Group.

Capacidade de definir e editar credenciais de usuários de proxy IBM Firewall utilizando o Console de Gerenciamento do Policy Director.

Um serviço CAS (Credentials Acquisition Service) do Policy Director que fornece suporte para utilização de serviços de autenticação externos.

Suporte para autenticação baseada em certificado do cliente utilizando o novo CAS (Credentials Acquisition Service) do Policy Director.

A capacidade de criar seu próprio serviço CAS (Credentials Acquisition Service) personalizado utilizando a interface IDL (Interface Definition Language) entre WebSEAL e CAS do Policy Director. O produto Policy Director também fornece a estrutura de servidor geral que trabalha com funções do servidor CAS do Policy Director, como inicialização, registro do servidor e identificação de sinal.

A opção de utilizar um mecanismo de túnel SSL (Secure Sockets Layer) além do túnel GSS (Generic Security Services).

Utilize a interface da linha de comandos do Policy Director para gerenciar critérios de início de sessão e de senha.

Utilize o Console de Gerenciamento do Policy Director ou a interface de linha de comandos para gerenciar usuários únicos de início de sessão, grupos e recursos (destinos).

Uma ferramenta de gerenciamento de senha de recurso de início de sessão única baseada na Web.

Um processo de instalação integrada.

Preparação para o Ano 2000

Estes produtos estão preparados para o Ano 2000. Quando utilizados de acordo com sua documentação associada, eles são capazes de processar, fornecer e/ou receber corretamente os dados de data dentro ou entre os séculos vinte e vinte e um, contanto que todos os produtos (por exemplo, hardware, software e firmware) utilizados façam intercâmbio de dados com data, da maneira adequada.

Serviço e suporte

Entre em contato com a IBM para obter serviço e suporte referentes a todos os produtos incluídos na oferta IBM SecureWay FirstSecure. Alguns destes produtos podem fazer referência a suporte não-IBM. Se você adquirir estes produtos como

parte da oferta FirstSecure, entre em contato com a IBM para obter serviço e suporte.

Convenções

Este manual utiliza as seguintes convenções tipográficas:

Convenção	Significado
negrito	Elementos da interface do usuário como caixas de opções, botões e itens contidos nos quadros de listagens.
`monoespaçado`	Sintaxe, amostra de código e qualquer texto que o usuário precise digitar.
Itálico	Ênfase e primeira utilização de termos especiais que sejam relevantes ao produto Policy Director.
→	Mostra uma série de seleções de um menu. Por exemplo, clique em **Arquivo → Executar**, indica que você clique em **Arquivo** e depois em **Executar**.

Informações na Web

Informações sobre as atualizações de última hora no produto Policy Director estão disponíveis no seguinte endereço da Web:

`http://www.ibm.com/software/security/policy/library`

Informações sobre as atualizações em outros produtos IBM SecureWay FirstSecure estão disponíveis no seguinte endereço da Web:

`http://www.ibm.com/software/security/firstsecure/library`

Capítulo 1. Informações sobre o produto Policy Director

IBM SecureWay Policy Director (Policy Director) está disponível como um componente do IBM SecureWay FirstSecure ou como um produto independente.

O que é o IBM SecureWay FirstSecure?

IBM SecureWay FirstSecure (FirstSecure) é parte das soluções de segurança integradas da IBM. FirstSecure é um abrangente conjunto de produtos integrados que ajudam sua empresa a:

Estabelecer um ambiente e-business seguro.

Reduzir o custo total de propriedade de segurança, simplificando o planejamento da segurança.

Implementar o critério de segurança.

Criar um ambiente e-business eficaz.

Os produtos IBM SecureWay incluem:

Policy Director
IBM SecureWay Policy Director (Policy Director) fornece autenticação, autorização, segurança de dados e gerenciamento de recursos da Web.

Boundary Server
IBM SecureWay Boundary Server (Boundary Server) fornece as seguintes funções:

As principais funções do Firewall de filtro, proxy e gateway de nível de circuito

Uma conexão VPN (Virtual Private Network) ao IBM Firewall

Componentes para segurança na Internet

Uma solução de segurança de código móvel

Uma interface do usuário de configuração liga a função do usuário proxy do Policy Director ao produto Firewall do Boundary Server.

Intrusion Immunity
Intrusion Immunity fornece detecção de violação e proteção contra vírus.

Trust Authority
IBM SecureWay Trust Authority (Trust Authority) suporta padrões PKI (Public Key Infrastructure) para criptografia e interoperabilidade. O Trust Authority fornece suporte para segurança, renovação e revogação de certificados digitais. Estes certificados fornecem um meio de autenticar os usuários e assegurar comunicações confiáveis.

Toolbox
IBM SecureWay Toolbox (Toolbox) é um conjunto de APIs (Application Programming Interfaces) com o qual os programadores de aplicativos podem incorporar segurança no software. Você pode obter o recurso Toolbox como parte do programa FirstSecure. Tanto o Policy Director como o Toolbox incluem a biblioteca API do Policy Director e a documentação.

Como cada produto IBM SecureWay FirstSecure pode ser instalado separadamente, você pode planejar uma movimentação controlada em direção a um ambiente

seguro. Este recurso reduz a complexidade e o custo na proteção de seu ambiente e na disposição de velocidades dos aplicativos e recursos da Web.

Para obter mais informações sobre os componentes FirstSecure e uma lista de documentações do produto IBM SecureWay, consulte a documentação *Planning and Integration* do FirstSecure.

O que é IBM SecureWay Policy Director?

Policy Director é uma solução independente de gerenciamento de autorização e de segurança que fornece segurança de recursos extremidade-a-extremidade sobre intranets geograficamente dispersas e *extranets*. Uma *extranet* é uma rede VPN (Virtual Private Network) que utiliza recursos de controle de acesso e de segurança para restringir o uso de uma ou mais intranets conectadas à Internet aos assinantes selecionados.

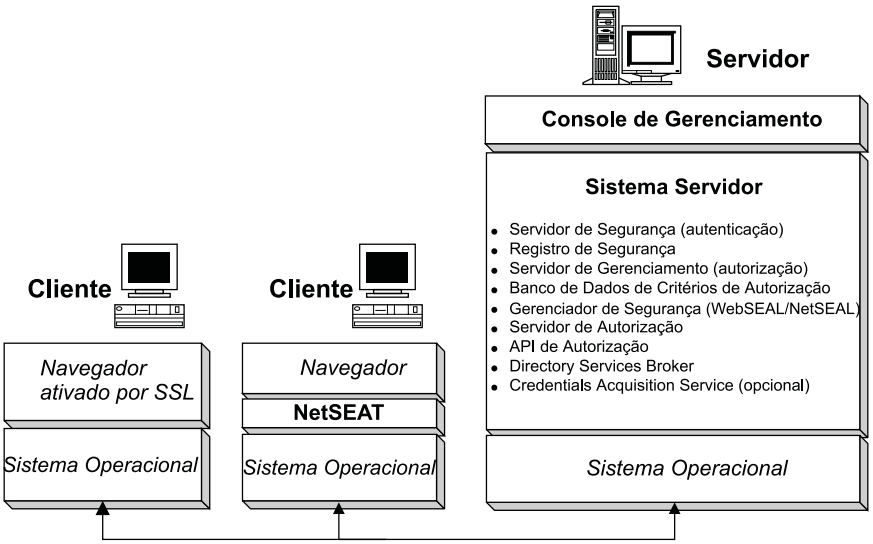
Policy Director fornece serviços de autenticação, autorização, segurança de dados e gerenciamento de recursos. Você pode utilizar o produto Policy Director em conjunto com aplicativos padrão baseados na Internet para criar intranets e extranets seguras e bem-gerenciadas.

Policy Director é executado nos sistemas operacionais Windows NT, AIX e Solaris.

Componentes do Policy Director

O produto Policy Director contém os seguintes componentes:

- Clientes e servidores LDAP (Lightweight Directory Access Protocol) e IBM DCE (Distributed Computing Environment) do IBM SecureWay Directory.
- Policy Director Base
- Servidor de Gerenciamento
- Gerenciador de Segurança, consistindo em WebSEAL e NetSEAL
- CAS (Credential Acquisition Service)
- Servidor de Autorização
- API (Application Programming Interface) de autorização
- Cliente NetSEAT
- Console de Gerenciamento
- DSB (Directory Services Broker)



Antes de instalar o produto Policy Director, você deve determinar os recursos de segurança e gerenciamento necessários para sua rede. Analise as seções a seguir para decidir os componentes necessários do Policy Director.

Servidores IBM SecureWay Directory e DCE

Os servidores IBM SecureWay Directory e IBM Distributed Computing Environment são utilizados pelo produto Policy Director e estão incluídos no produto Policy Director.

O Policy Director pode utilizar um registro de usuário LDAP ou um registro de usuário DCE. Será solicitado que você selecione o tipo de registro do usuário durante a instalação do Policy Director.

Se você pretende utilizar um registro do usuário LDAP, será necessário instalar um cliente LDAP e configurar um servidor LDAP antes de instalar o produto Policy Director. Siga as instruções no Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23. Se você pretende utilizar um registro de usuário DCE, poderá ignorar a seção sobre a instalação e configuração LDAP.

Servidor IBM SecureWay Directory

O produto SecureWay Directory fornece o protocolo LDAP (Lightweight Directory Access Protocol) para manter informações do diretório em uma localização central para armazenamento, atualizações, recuperação e intercâmbio. Se você utilizar o protocolo LDAP para seu registro de usuário, Policy Director utilizará LDAP para conceder autorização aos usuários.

Servidor IBM Distributed Computing Environment

O DCE (Distributed Computing Environment) inclui serviços e ferramentas que suportam a criação, a utilização e a manutenção de aplicações distribuídas em um ambiente de computação heterogêneo. O DCE forma o domínio seguro dentro do qual os servidores do Policy Director podem autenticar o usuário mutuamente e comunicar-se de maneira segura. No sistema operacional Windows NT, o cliente NetSeat opera como o cliente DCE.

Policy Director Base

O componente Policy Director Base (IVBase) é o software de referência comum utilizado por todos os componentes do Policy Director. Este componente é instalado automaticamente quando você instala outros componentes do Policy Director, exceto quando você instala o Console de Gerenciamento no Windows.

No AIX, o componente de Configuração SMIT (IV.Smit) é incluído como parte do pacote do IV.Base. Este pacote contém informações de configuração utilizadas pelo SMIT. Este pacote deve ser instalado em todos os servidores AIX.

Servidor de Gerenciamento

O servidor de Gerenciamento (IVMgr) é o servidor de autorização principal do domínio seguro inteiro. O servidor de Gerenciamento controla e mantém o banco de dados de critérios de autorização mestre. Todos os dados passam pelo servidor de Gerenciamento.

O servidor de Gerenciamento deve ser instalado em um computador no domínio seguro antes da instalação de quaisquer gerenciadores de segurança ou dos servidores de Autorização, mas não necessariamente no mesmo computador. Deve existir apenas uma instância do servidor de Gerenciamento instalada em um determinado domínio seguro.

Cada instância do servidor de Gerenciamento requer a instalação dos seguintes componentes no mesmo computador que o servidor de Gerenciamento:

- Cliente DCE
- Cliente LDAP (se você estiver utilizando o LDAP como seu registro de usuário)
- Policy Director Base
- Servidor de Gerenciamento

Gerenciador de Segurança

O Gerenciador de Segurança (IVNet) aplica critério de controle de acesso baseado em informações de um banco de dados de critérios de autorização em duplicata. O Gerenciador de Segurança inclui os seguintes componentes:

- WebSEAL para controle de acesso refinado de HTTP (Hypertext Transfer Protocol) e HTTPS (Secure Sockets Layer interface)
- NetSEAL para controle de acesso grosseiro de TCP/IP (Transmission Control Protocol/Internet Protocol)

Os componentes NetSEAL e WebSEAL são requeridos para configurar e ativar estas capacidades, que por padrão ficam inativas.

WebSEAL

WebSEAL (IVWeb) é o componente de servidor HTTP do Gerenciador de Segurança. O WebSEAL é um servidor da Web seguro que oferece suporte a clientes HTTP, HTTPS e NetSEAT. O WebSEAL combina com o CAS (Credential Acquisition Service) do Policy Director para oferecer suporte a autenticação baseada em certificado X.509 para um usuário do Policy Director.

NetSEAL

O NetSEAL (IVTrap) fornece controle de acesso grosseiro para servidores TCP/IP. O NetSEAL controla o acesso a um conjunto de portas configuradas em um servidor TCP/IP.

O conjunto de produtos Policy Director fornece segurança para a troca de dados de cliente/servidor na Internet e intranets privadas. Policy Director NetSEAL e Policy Director WebSEAL são produtos do lado do servidor que controlam e gerenciam os dados da rede dentro de domínios seguros definidos pelo DCE.

Servidor de Autorização

O servidor de Autorização (IVAcld) trata pedidos de autorização de aplicativos de terceiros que utilizam a API de Autorização do Policy Director em modo remoto. O servidor de Autorização deve ser instalado em pelo menos um computador no domínio seguro para aplicativos de terceiros.

Interface de programação do aplicativo de Autorização

O componente Policy Director Application Development Kit ou ADK (VAuthADK) inclui as APIs (Interface Programming Interface) de Autorização do Policy Director. A API permite gerar aplicativos que utilizem a autorização do Policy Director.

O ADK (Policy Director Application Development Kit) inclui um servidor de API de autorização (AuthAPI) que permite que os desenvolvedores gerem segurança e autorização do Policy Director diretamente em aplicativos da corporação. A API de autorização do Policy Director fornece acesso direto ao Serviço de Autorização do Policy Director. A utilização destas APIs de autorização significa que os desenvolvedores não precisam mais escrever códigos de autorização para cada aplicativo.

O ADK inclui programas C de amostra.

O ADK também contém o fonte para o servidor de demonstração CAS (Credential Acquisition Service) do Policy Director e o servidor de demonstração de serviço de autorização externa.

Cliente NetSEAT

O cliente NetSEAT do Policy Director é um cliente lightweight para Windows 95, Windows 98 ou Windows NT. O NetSEAT fornece canais de comunicação seguros para servidores Policy Director.

O software cliente NetSEAT permite que os clientes juntem domínios seguros e utilizem os serviços de segurança avançados que são oferecidos pelos servidores WebSEAL e NetSEAL. O NetSEAT protege todas as comunicações de uma rede de clientes, permitindo criptografia de extremidade a extremidade de todo o tráfego cliente/servidor e baseado na Web.

O NetSEAT fornece a capacidade de proteger tráfego TCP/IP como o gerado por serviços como Telnet e POP3. O NetSEAT permite que um administrador do sistema exerça controle grosseiro sobre as atividades de rede de uma estação de trabalho. Este controle é resultante da utilização da capacidade do domínio seguro de autenticar usuários e de atribuir privilégios de autorização a usuários e recursos.

Console de Gerenciamento

O Console de Gerenciamento (IVConsole) é um aplicativo gráfico baseado em Java utilizado para gerenciar critérios de segurança do domínio seguro do Policy Director. Através da utilização do Console de Gerenciamento, você pode executar tarefas administrativas no registro de contas e no banco de dados de critérios de autorização primária. O Console de Gerenciamento requer um cliente DCE para iniciar sessão no domínio seguro e executar RPCs (remote procedure calls) de gerenciamento seguro para os servidores de Gerenciamento do Policy Director. O Console de Gerenciamento utiliza serviços DCE lightweight (serviços de tempo de execução) fornecidos pelo cliente NetSEAT no Windows 95, Windows 98 ou Windows NT.

Directory Services Broker

O DSB (Directory Services Broker) é distribuído como parte do componente servidor de Gerenciamento. Os cliente Console de Gerenciamento e NetSEAT requerem um DSB no domínio seguro quando em execução em estação de trabalho Windows 95, Windows 98 ou Windows NT. Geralmente o DSB não requer nenhuma administração ou configuração após a instalação inicial.

Credentials Acquisition Service (opcional)

O CAS (Credentials Acquisition Service) é um componente configurado opcionalmente.

Aquisição de Credencial é o processo de transformação ou de mapeamento de informação de identidade específica fornecida por um mecanismo de autenticação em uma representação comum, e por todo o domínio, da identidade do cliente. Esta representação comum é denominada *credenciais do cliente*.

Quando a aquisição ou mapeamento de credenciais forem necessários, você deve configurar o CAS (Credential Acquisition Service) do Policy Director para ser utilizado com o servidor WebSEAL do Policy Director. Os usuários do Policy Director são automaticamente mapeados para credenciais pelo WebSEAL.

Os clientes que acessam o Policy Director utilizando certificados X.509 do lado cliente por ter as informações de *certificado* mapeadas para identidades do Policy Director através do Credentials Acquisition Service do Policy Director ou escrevendo seu próprio serviço de aquisição de credenciais.

Se você possuir usuários definidos em um outro registro externo, os nomes de usuários podem ser mapeados para as identidades do Policy Director através da utilização de um servidor CAS personalizado. Você pode escrever e personalizar seu próprio servidor CAS para fornecer uma solução específica para o domínio seguro e para processar informações de autenticação como: certificados de clientes, nomes de usuários ou tokens. O desenvolvedor ou o projetista do Credentials Acquisition Service do Policy Director determina completamente as especificações deste serviço de autenticação e mapeamento. O Policy Director armazena regras de mapeamento em um banco de dados externo ao Policy Director. O Policy Director fornece interface IDL (Interface Definition Language) entre o WebSEAL e o Service Acquisition Service do Policy Director. O Policy Director também fornece a estrutura de servidor geral que trata as funções de servidor do Credentials Acquisition Service do Policy Director como inicialização, registro de servidor e identificação de sinais. É responsabilidade do desenvolvedor do Credentials Acquisition Service do Policy Director estender a estrutura do serviço de aquisição

de credenciais para executar funções de mapeamento de identidade requeridas pelo aplicativo específico.

Para obter mais informações sobre cada um dos componentes do Policy Director, consulte o *Policy Director Administration Guide.*

Funcionamento do Policy Director

As seções a seguir mostram quatro cenários que demonstram utilizações típicas do Policy Director:

Um administrador utilizando o Console de Gerenciamento

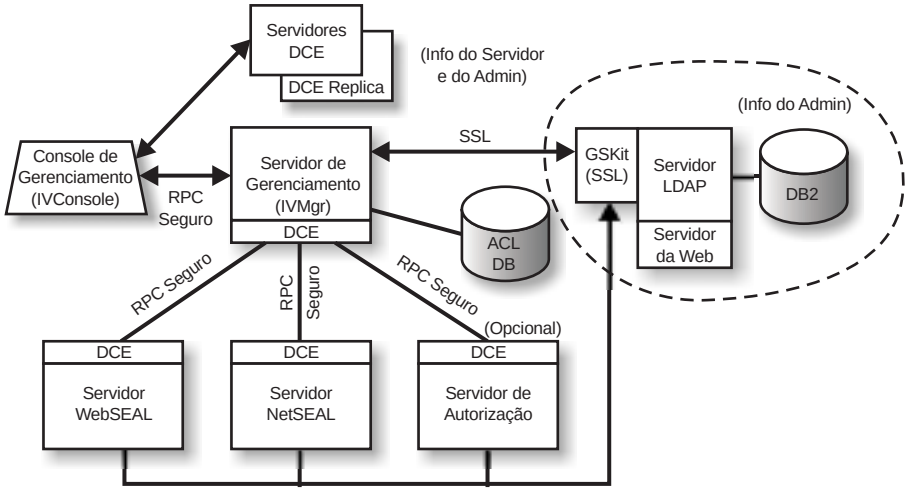
Um usuário acessando recursos protegidos da Web de um navegador da web

Um usuário acessando um servidor TCP/IP protegido utilizando um cliente NetSEAT

Um usuário acessando um servidor protegido de terceiros

Administração utilizando o Console de Gerenciamento

A figura a seguir mostra como os dados fluem quando um administrador está utilizando o Console de Gerenciamento para gerenciar o Policy Director. Os componentes LDAP, mostrados na linha pontilhada, são necessários apenas se você utilizar LDAP como seu registro de usuário.



Um administrador no Console de Gerenciamento autentica para o domínio seguro e recebe credenciais.

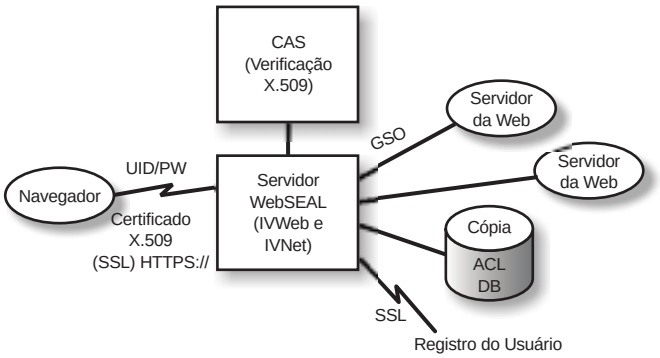
Quando o administrador gerencia usuários ou grupos do Console de Gerenciamento, o Console de Gerenciamento envia pedidos através de um RPC seguro para o servidor de Gerenciamento. O servidor de Gerenciamento envia as alterações correspondentes para o servidor LDAP através de uma conexão SSL que foi estabelecida previamente utilizando o DN (nome distinto) e a senha do servidor de Gerenciamento.

Quando o administrador adiciona, modifica ou aplica uma ACL (lista de controle de acesso), o Console de Gerenciamento envia os dados através de um RPC seguro para o servidor de Gerenciamento. O servidor de Gerenciamento armazena as alterações na cópia local do banco de dados ACL. Quando o banco de dados ACL é modificado, o servidor de Gerenciamento notifica todos os outros servidores

através de um RPC seguro que o banco de dados ACL foi alterado. Os servidores WebSEAL, NetSEAL e de Autorização também verificam periodicamente junto ao servidor de Gerenciamento para obter atualizações no banco de dados ACL.

Usuário acessando recursos protegidos da Web de um Navegador da web

A figura a seguir mostra como os dados fluem quando um usuário está acessando recursos protegidos da Web de um Navegador da web.



Quando o usuário tenta acessar um página protegida da Web, o navegador ativado por SSL entra em contato com o servidor WebSEAL. Se o WebSEAL estiver configurado para autenticação baseada em certificado de cliente, o WebSEAL pede um certificado X.509 do navegador. Quando o WebSEAL recebe o certificado do navegador, ele passa o certificado para o servidor CAS. O CAS tenta mapear o certificado recebido para uma identidade de usuário entendida pelo Policy Director. Dentro do arquivo de configuração do CAS, o administrador do Policy Director pode criar uma tabela que é utilizada para associar um DN de certificado ao DN de um usuário do Policy Director. Quando o CAS é chamado pelo WebSEAL com um certificado, ele primeiro extrai o DN do certificado e pesquisa uma correspondência na tabela. Se uma correspondência é encontrada, o CAS retorna o DN do usuário do Policy Director para o WebSEAL. O WebSEAL utiliza este DN para identificar o usuário do Policy Director. Se uma correspondência não for encontrada, o CAS retorna o DN do certificado para o WebSEAL. Neste caso o DN no certificado é utilizado para identificar o usuário do Policy Director. O servidor WebSEAL utiliza o DN retornado para recuperar as credenciais do usuário.

Para obter mais informações sobre certificados X.509, consulte o seguinte endereço da Web:

`http://www.ietf.org`

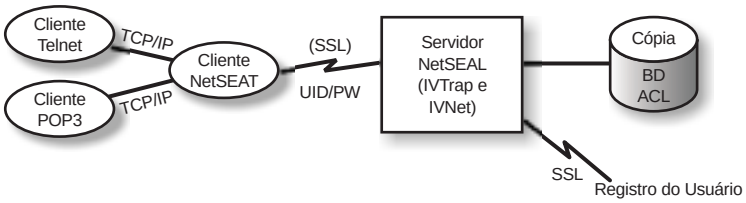
Quando o WebSEAL conclui a autenticação do usuário com êxito, o WebSEAL utiliza a duplicata local do banco de dados ACL para decidir se o usuário está autorizado a acessar o objeto da Web na forma solicitada.

Se a conexão entre o servidor WebSEAL e o servidor back-end que contém o recurso que está sendo acessado for uma junção GSO (Global Sign On), o WebSEAL procura as credenciais GSO daquela junção no LDAP e passa o nome do usuário e a senha para o servidor da Web.

Para obter informações sobre gerenciamento de recursos GSO e grupos de recursos GSO, consulte as informações do Console de Gerenciamento no *Policy Director Administration Guide.*

Usuário acessando um servidor TCP/IP protegido utilizando um cliente NetSEAT

A figura a seguir mostra como é o fluxo de dados quando um usuário está acessando um servidor protegido TCP/IP utilizando um cliente NetSEAT.



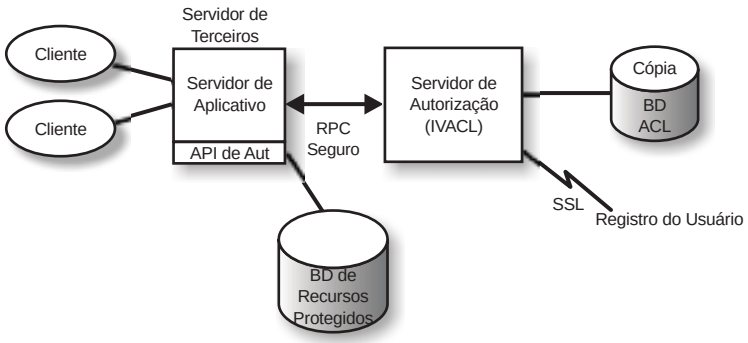
O usuário no cliente Telnet executa telnet para um servidor protegido NetSEAL, que identifica que o usuário está solicitando acesso. O NetSEAL solicita o nome e a senha do usuário e verifica a identidade do usuário provendo-se das informações do usuário e comparando-as com o valor armazenado no registro do usuário. O NetSEAL verifica se o usuário pode acessar o computador através da porta especificada.

O NetSEAT redireciona pedidos de maneira transparente para servidores Policy Director seguros, enviando as informações através do túnel SSL seguro. O NetSEAT utiliza suas informações de configuração para reconhecer pedidos para um servidor seguro a partir de aplicativos TCP/IP genéricos como Telnet, POP3 ou HTTP. O NetSEAT utiliza autenticação básica através de SSL para estabelecer a identidade e as credenciais do usuário NetSEAT. Depois que a autorização é estabelecida, o SSL seguro encapsula e conclui a transação solicitada de acordo com as definições de segurança aplicáveis.

Por exemplo, quando um Navegador da web pede acesso a um serviço ou recurso protegido pelo Gerenciador de Segurança do Policy Director, o NetSEAT intercepta o pedido de maneira transparente e direciona-o para o servidor apropriado. Se este for o primeiro pedido para o Policy Director e for necessária autenticação, o NetSEAT apresenta uma caixa de diálogo de início de sessão ao usuário. Quando um usuário já foi autenticado, o Policy Director anexa de maneira transparente as credenciais apropriadas à cada pedido futuro para informação. Este processo permite um ambiente de um único início de sessão para todos os aplicativos Winsock gerenciados pelo Policy Director. Adicionalmente, o Policy Director utiliza estas credenciais para determinar se o usuário pode acessar o recurso protegido do Policy Director solicitado.

Usuário acessando um servidor protegido de terceiros

A figura a seguir mostra como é o fluxo de dados quando um usuário está acessando um servidor de terceiros protegido.



Quando um cliente tenta acessar dados protegidos em um servidor protegido de terceiros, o servidor de terceiros autentica o usuário e mapeia o usuário para um usuário Policy Director. O servidor do aplicativo passa as informações do usuário Policy Director para o servidor de Autorização, que contacta o LDAP (ou outro produto, como o DCE, utilizado para registro de usuários) e recupera as credenciais do usuário. O servidor de aplicativo então passa as credencias, o nome do objeto que o usuário deseja acessar e a operação que o usuário deseja executar para o servidor de Autorização, que retorna uma indicação sobre se a operação deve ser permitida. O servidor do aplicativo então permite ou nega o acesso.

Conteúdo do pacote do Policy Director

O produto IBM SecureWay Policy Director, Versão 3.0, é fornecido em cinco CDs. Os títulos e o conteúdo dos CDs são mostrados na tabela a seguir.

Título do CD	**Conteúdo**
IBM SecureWay Policy Director Versão 3.0	IBM Policy Director Versão 3.0
IBM SecureWay Policy Director Security Services	IBM DCE para AIX Versão 2.2 IBM DCE para Windows NT Versão 2.2 Transarc DCE para Solaris Versão 2.0
IBM SecureWay Directory Versão 3.1.1 para AIX	IBM SecureWay Directory Versão 3.1.1 IBM DB2 Versão 5.2 com Fix Pack 7 IBM Global Security Kit SSL Runtime Toolkit Versão 3.0.1 (GSKit)
IBM SecureWay Directory Versão 3.1.1 para NT	IBM SecureWay Directory Versão 3.1.1 IBM DB2 Versão 5.2 com Fix Pack 7 IBM Global Security Kit SSL Runtime Toolkit Versão 3.0.1 (GSKit)
IBM SecureWay Directory Versão 3.1.1 para Solaris	IBM SecureWay Directory Versão 3.1.1 IBM DB2 Versão 5.2 com Fix Pack 8 IBM Global Security Kit SSL Runtime Toolkit Versão 3.0.1 (GSKit)

Capítulo 2. Requisitos do sistema

Seu ambiente operacional deve atender aos requisitos de software e de hardware discutidos nas seções a seguir. Para obter as informações mais recentes sobre os requisitos do sistema, consulte o arquivo README do Policy Director. O arquivo README contém informações que substituem as informações nas publicações do produto.

Para obter o arquivo README mais recente, acesse a página da biblioteca do site da Web do IBM SecureWay Policy Director.

`http://www.ibm.com/software/security/policy/library`

Antes de instalar o DCE, LDAP NetSEAT e os componentes de servidor do Policy Director, certifique-se de que você possui o hardware e o software necessários, listados nas seções a seguir.

Requisitos de hardware

Utilização de memória, gerenciamento de buffer e de cache e estruturas de controle são escaláveis. No entanto, os requisitos fundamentais de seu sistema operacional de base, os requisitos dos clientes DCE e LDAP de pré-requisito e os requisitos de seus aplicativos de cliente ditam os requisitos mínimos de espaço em disco e memória de sua configuração.

Os requisitos de hardware do servidor Policy Director são os seguintes:

Plataforma	Espaço Mínimo em Disco	Memória Mínima
Servidor Windows NT com 80468 Intel ou compatível com Intel de 133 MHz ou superior	16 MB	64 MB
Servidor AIX, hardware que execute o AIX 4.3.1	16 MB	64 MB
Servidor Solaris, com hardware que execute o Solaris 2.6	16 MB	64 MB

Os requisitos de hardware para o cliente Policy Director são os seguintes:

Plataforma	Espaço Mínimo em Disco	Memória Mínima
Cliente Windows NT, com 80486 Intel ou compatível com Intel de 133 MHz ou superior	16 MB	32 MB
Servidor AIX, hardware que execute o AIX 4.3.1	16 MB	32 MB
Servidor Solaris, com hardware que execute o Solaris 2.6	16 MB	24 MB

Requisitos de software

Ao planejar a instalação do Policy Director, certifique-se de que você possui as versões corretas dos sistemas operacionais e outros pré-requisitos de software,

mostrados nas seções a seguir. A seguir estão os requisitos do sistema operacional para servidores Policy Director, o cliente NetSEAT e o Console de Gerenciamento:

Servidores do Policy Director

Os servidores do Policy Director podem ser instalados nos seguintes sistemas operacionais:

Servidor Windows NT Versão 4.0 com Service Pack 4 ou superior

AIX Versão 4.3.1 ou superior

Sun Solaris Versão 2.6

Clientes NetSEAT

Os clientes NetSEAT do Policy Director podem ser instalados nos seguintes sistemas operacionais:

Windows NT Versão 4.0 com Service Pack 4 ou superior

Windows 98

Windows 95

Console de Gerenciamento

O Console de Gerenciamento do Policy Director pode ser instalada nos seguintes sistemas operacionais:

Servidor Windows NT, Versão 4.0, com Service Pack 4 ou superior

Windows NT, Windows 95 ou Windows 98

AIX Versão 4.3.1 ou superior, incluindo Java Runtime 1.1.6 ou superior

Sun Solaris Versão 2.6

Outros requisitos de software

O Policy Director requer um servidor DCE e, se você estiver utilizando LDAP como seu registro de usuário, um servidor LDAP. Um servidor (LDAP ou DCE) deve estar instalado em pelo menos um computador no domínio seguro. Os clientes DCE e LDAP e os servidores são fornecidos como parte do produto Policy Director. Você pode instalá-los antes de instalar o Policy Director ou utilizar uma instalação existente do DCE e do LDAP que estejam no nível correto.

Windows NT e AIX

Nas plataformas Windows NT e AIX, os servidores Policy Director requerem o seguinte software:

IBM DCE para Windows NT Versão 2.2 ou superior para servidores Windows NT ou IBM DCE para AIX Versão 2.2 ou superior para servidores AIX.

IBM SecureWay Directory Versão 3.1.1 (LDAP), que inclua o DB2 Versão 5.2, Fix Pack 7. O LDAP é necessário apenas se você estiver utilizando o LDAP para seu registro de usuário.

SSL (Secure Sockets Layer) Versão 3.0 ou superior.

CAS (Credentials Acquisition Service) e WebSEAL do Policy Director requerem um dos seguintes Navegadores da web:

— Microsoft Internet Explorer Versão 4 ou superior

— Netscape Communicator Versão 4.5 ou superior

— Netscape Navigator Versão 4.5 ou superior

Para clientes Policy Director no Windows 95 apenas, você deve ter o Winsock Versão 2.0 ou superior.

Solaris

Na plataforma Solaris, os servidores Policy Director requerem o seguinte software:

Transarc DCE Versão 2.0.

IBM SecureWay Directory (LDAP) Versão 3.1.1, que inclua DB2 Versão 5.2, Fix PackPacote de Correção 8. O LDAP é necessário apenas se você estiver utilizando LDAP para seu registro de usuário.

Secure Sockets Layer Versão 3.0 ou superior.

CAS e WebSEAL do Policy Director requerem um dos seguintes Navegadores da web:

- Microsoft Internet Explorer Versão 4 ou superior
- Netscape Communicator Versão 4.5 ou superior
- Netscape Navigator Versão 4.5 ou superior

Capítulo 3. Planejamento do Policy Director

As seções a seguir fornecem as informações necessárias para a preparação e o planejamento da instalação e configuração do Policy Director. Certifique-se de ler Capítulo 1, “Informações sobre o produto Policy Director” na página 1 e decidir quais os componentes do Policy Director você precisa antes de planejar sua instalação.

Configurações comuns

As configurações mostradas nesta seção podem ajudá-lo a determinar a configuração apropriada para sua rede. Utilize a tabela em “Componentes requeridos para configurações comuns” na página 16 para determinar os componentes necessários para sua configuração. Em seguida, selecione estes componentes durante a instalação do Policy Director. Observe que o WebSEAL e o NetSEAL podem ser instalados em qualquer computador. Algumas configurações comuns de componentes do Policy Director são mostradas na lista a seguir:

Servidor de Gerenciamento apenas
: Um servidor que executa uma única instância do servidor de Gerenciamento para o domínio seguro. Neste cenário, o servidor de Gerenciamento reside por si mesmo em seu próprio sistema. O servidor de Gerenciamento mantém o banco de dados de autorizações mestre do domínio seguro, replica este banco de dados por todo o domínio seguro e mantém informações de localização sobre outros computadores de servidores do Policy Director no domínio seguro.

Gerenciador de Segurança com servidor WebSEAL
: Dois componentes formam o WebSEAL — o Gerenciador de Segurança (IVNet) e o WebSEAL (IVWeb). Um servidor WebSEAL protege um espaço da Web. O WebSEAL oferece suporte a servidores back-end para alta disponibilidade e tolerância a falhas através de *junções inteligentes* ou junções.

Gerenciador de Segurança com servidor NetSEAL
: Dois componentes formam o NetSEAL — o Gerenciador de Segurança (IVNet) e o NetSEAL (IVTrap). Um servidor NetSEAL protege uma rede privada virtual (VPN) e fornece controle de acesso para legacy e serviços de rede de terceiros.

Gerenciador de Segurança com servidor WebSEAL e NetSEAL
: Um combinação de servidor WebSEAL e NetSEAL.

Servidor de Autorização
: Um servidor que fornece acesso ao serviço de autorização do Policy Director para aplicativos de terceiros, utilizando a API de Autorização do Policy Director.

Servidor de Autorização e ADK
: Um servidor que fornece um ambiente de desenvolvimento para desenvolvedores que desejem construir aplicativos de terceiros que utilizam a API de Autorização do Policy Director para chamar o serviço de autorização.

Console de Gerenciamento
Um aplicativo gráfico baseado em Java utilizado para gerenciar critérios de segurança para o domínio seguro do Policy Director. O IVBase não é necessário para o Console de Gerenciamento no Windows.

Todos os componentes
Um servidor que fornece os serviços combinados de todas as configurações acima.

Componentes requeridos para configurações comuns

As configurações do Policy Director descritas em “Configurações comuns” na página 15 estão listadas na tabela a seguir. A tabela mostra quais componentes devem ser instalados para cada configuração. Quando lidos da esquerda para a direita, os componentes indicados estão na ordem correta de instalação.

Observe que dois componentes formam o WebSEAL e o NetSEAL:

WebSEAL Gerenciado de Segurança (IVNet) e WebSEAL (IVWeb)

NetSEAL Gerenciador de Segurança (IVNet) e NetSEAL (IVTrap)

Notas para IVBase:

O IVBase não é necessário para o Console de Gerenciamento no Windows.

O IV.Smit é instalado automaticamente com o IV.Base no AIX.

Cenários	Pacotes de Instalação							
	IVBase	IVMgr	IVNet	IVWeb	IVTrap	IVAcld	IVAuthADK	IVConsole
Instância única do servidor de Gerenciamento apenas	X	X						
Gerenciador de Segurança com WebSEAL	X	X***	X	X				
Gerenciador de Segurança com NetSEAL	X	X***	X		X			
Gerenciador de Segurança com WebSEAL e NetSEAL	X	X***	X	X	X			
Servidor de Autorização	X	X***				X		
Servidor de Autorização e ADK	X	X***				X	X	
Console de Gerenciamento	X							X
Todos os componentes	X	X***	X	X	X	X	X	X

*** Se este for o primeiro ou o único computador no domínio seguro, você deve instalar o servidor de Gerenciamento (IVMgr). Se este for um computador adicional em um domínio seguro existente com um servidor de Gerenciamento existente, você não deve instalar outro servidor de

Gerenciamento. Deve haver apenas um servidor de Gerenciamento em um determinado domínio seguro.

Informações requeridas antes da instalação

Antes de iniciar a instalação do Policy Director, tome nota das informações sobre o sistema necessárias para instalar o software Policy Director:

Servidores Policy Director

Nome do usuário para administrador da célula (cell_admin)
Senha para o administrador da célula (cell_admin)
WebSEAL: porta HTTP (padrão)
WebSEAL: diretório raiz do documento Web

Cliente NetSEAT (Windows apenas)

Nome da célula
Nome do host do servidor de segurança
Nome do host do servidor de horário
Nome do Host do Directory Services Broker

Mecanismos de túnel

O Policy Director oferece suporte aos seguintes protocolos para transmissão de dados criptografados:

Túnel do SSL (Secure Sockets Layer)
Túnel do GSS (Generic Security Services)

O WebSEAL oferece suporte à integridade de dados e à privacidade de dados fornecidos pelo túnel criptografado por SSL. O WebSEAL e o NetSEAL oferecem suporte a RPCs. A utilização de integridade e marcas de hora com RPC fornece proteção contra *playback attacks*. Um playback attack ocorre quando os dados de um usuário são capturados conforme fluem entre o cliente do usuário e o servidor. Estes dados são então reproduzidos e re-apresentados ao servidor como um meio de representar o primeiro usuário.

Túnel de SSL: O protocolo SSL permite a troca de sinais para configurar comunicações entre duas estações de trabalho. Este protocolo fornece segurança e privacidade na Internet. O SSL trabalha utilizando chave pública para autenticação e chave secreta para criptografia de dados transferidos através da conexão SSL.

Ative o SSL ao utilizar túnel SSL para servidores NetSEAL do Policy. Esta configuração é utilizada quando um cliente NetSEAT funciona como um cliente SSL para um servidor NetSEAL do Policy Director que está protegendo portas específicas (por exemplo, a porta utilizada pelo Telnet).

O WebSEAL do Policy Director oferece suporte ao SSL Versão 2 e 3.

Túnel GSS: A interface GSS (API GSS) é uma forma padrão de permitir que aplicativos acessem serviços de segurança. O túnel GSS é utilizado através de RPCs seguros. Ative esta opção quando instalar o cliente NetSEAT como um módulo de suporte para o Policy Director para Microsoft Windows NT ou Console de Gerenciamento do Policy Director.

O túnel de GSS fornece serviços de segurança para os responsáveis por chamadas de modo genérico. Ele é suportado com uma faixa de mecanismos e tecnologias de base. Ele permite portabilidade em nível de fonte de aplicativos para ambientes diferentes. O túnel GSS permite controlar o nível de proteção em tráfego viajando nas duas direções independentemente um do outro. Por exemplo, os dados que viajam do cliente para o servidor podem estar completamente protegidos com criptografia de dados em massa enquanto os dados que viajam do servidor para o cliente podem estar desprotegidos.

Requisitos de instalação para o domínio seguro

O Policy Director é um sistema de segurança largamente distribuído cujos componentes podem ser instalados em uma variedade de configurações em um ou mais computadores. A lista a seguir mostra quais componentes devem ser instalados no domínio seguro.

Serviços DCE

Um registro de usuário. (O IBM SecureWay Directory é requerido apenas se você estiver utilizando o LDAP para seu registro de usuário)

Servidores Policy Director

Console de Gerenciamento do Policy Director

ADK de Autorização do Policy Director

Se você estiver utilizando uma instalação existente do DCE ou do LDAP, certifique-se de que a instalação existente esteja no nível correto. Consulte “Outros requisitos de software” na página 12 para obter os níveis corretos. Observe as seguintes dependências antes de instalar o produto Policy Director.

Serviços de ambiente de computação distribuída (DCE)

Cada ambiente seguro Policy Director (célula DCE) requer uma instalação de serviços DCE completa em pelo menos um computador para proteger as comunicações entre os servidores Policy Director. Os serviços DCE podem residir no mesmo host que os servidores Policy Director ou podem ficar localizados em um host remoto na rede.

Para obter informações sobre a instalação DCE, consulte os manuais de instalação e administração e recursos de suporte técnico para suas plataformas necessárias. Consulte “Documentação do IBM Distributed Computing Environment” na página 74 para obter uma lista das documentações do DCE.

Utilize as seguintes instruções ao instalar o DCE:

Se você estiver criando um novo domínio seguro Policy Director em um sistema host único, execute uma instalação completa do servidor DCE

Se os servidores DCE estiverem localizados em um host remoto, crie um novo domínio seguro instalando o Policy Director em um host local.

Se você estiver instalando o Policy Director para Windows NT em um domínio seguro de Policy Director existente, utilize um cliente NetSEAT para fornecer acesso aos serviços DCE requeridos. Instale o cliente NetSEAT no mesmo host que o Policy Director para servidores Windows NT.

Registro de usuário

O Policy Director pode utilizar o registro de usuário IBM SecureWay Directory (LDAP) ou o registro de usuário DCE como seu registro de usuário.

Se você utilizar LDAP como o registro de usuário, você deve ter um servidor LDAP instalado e configurado antes de instalar o Policy Director e deve também instalar um cliente LDAP em cada computador Policy Director.

Consulte o *IBM SecureWay Directory Installation and Configuration, Versão 3.1.1* para obter informações sobre a instalação do LDAP. Consulte "Documentação do IBM SecureWay Directory" na página 75 para obter a localização desta documentação do LDAP.

Ou, consulte as informações sobre o produto DCE, listadas na "Documentação do IBM Distributed Computing Environment" na página 74, para obter informações sobre a instalação do DCE.

Servidores Policy Director

Os requisitos a seguir referem-se à instalação dos servidores Policy Director.

Para uma comunicação apropriada, todos os servidores Windows NT Policy Director requerem o cliente NetSEAT do Policy Director.

Todas as instalações de servidores Policy Director requerem o componente base, que é instalado automaticamente.

Se você estiver instalando o *primeiro* ou o *único* computador no domínio seguro, você deve instalar o servidor de Gerenciamento no computador.

Se você estiver instalando um computador *adicional* em um domínio seguro existente que possui um servidor de Gerenciamento existente, não instale outro servidor de Gerenciamento. Deve haver apenas uma instância do servidor de Gerenciamento em um determinado domínio seguro.

O WebSEAL, o NetSEAL e os componentes do servidor de Autorização são opcionais.

O Gerenciador de Segurança combina com o WebSEAL, para fornecer o componente de servidor HTTP WebSEAL e controle de acesso refinado HTTP e com o NetSEAL, para fornecer o componente de controle de acesso TCP/IP grosseiro.

Todos os servidores Policy Director no AIX e no Solaris requerem um cliente DCE completo e, se você estiver utilizando LDAP como seu registro de usuário, um cliente LDAP.

Console de Gerenciamento

O Console de Gerenciamento requer que o domínio seguro e o servidor de Gerenciamento estejam instalados e configurados. O Console de Gerenciamento requer um cliente DCE e, se ele estiver em um computador Windows, o cliente NetSEAT.

ADK de Autorização

Instale o ADK de Autorização do Policy Director no computador de desenvolvimento de aplicativos. O ADK de Autorização pode ser utilizado para desenvolver aplicativos que permitem que os usuários acessem servidores

protegidos de terceiros. O ADK de Autorização requer o componente base, que é instalado automaticamente quando o ADK de Autorização é instalado.

O domínio seguro no qual o aplicativo é executado deve ter um servidor de Autorização instalado em pelo menos um computador. Um ambiente típico de desenvolvimento inclui o servidor de Autorização no mesmo sistema que o ADK de Autorização.

Visão geral da instalação do Policy Director etapa por etapa

A instalação do Policy Director requer as seguintes etapas:

1. Se você tiver uma versão anterior do IBM SecureWay Policy Director instalada e desejar migrar sua instalação, consulte as informações sobre migração na página da Web do Policy Director (consulte “Informações na Web” na página vii).
2. Verifique se o seu sistema operacional oferece suporte ao Policy Director. Consulte “Servidores do Policy Director” na página 12 para obter informações sobre sistemas operacionais suportados.
3. Determine quais componentes de servidor se ajustam melhor às suas necessidades e em quais computadores instalar estes componentes. Consulte “Configurações comuns” na página 15 para obter assistência.
4. Decida se o domínio seguro utilizará túnel SSL ou túnel GSS. Consulte o “Mecanismos de túnel” na página 17 para obter mais informações.
5. Instale e configure uma infra-estrutura DCE, se ainda não existir uma. Consulte “Serviços de ambiente de computação distribuída (DCE)” na página 18 para obter uma visão geral dos serviços DCE requeridos.
6. Decida se o domínio seguro utilizará um registro de usuário LDAP ou registro de usuário DCE. Se você estiver instalando o IBM SecureWay Directory (LDAP) para seu registro de usuário e não estiver utilizando um LDAP existente, instale e configure o LDAP. Consulte Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23 para obter instruções sobre a instalação do LDAP.
7. Instale os clientes DCE e LDAP nos computadores a serem utilizados para os servidores Policy Director. Consulte as informações sobre o produto DCE, listadas na “Documentação do IBM Distributed Computing Environment” na página 74, para obter informações sobre a instalação do DCE.
8. Instale os componentes do servidor Policy Director. Consulte o capítulo de instalação da plataforma do sistema operacional que estará sendo utilizado. Utilize um dos seguintes:

   Capítulo 5, “Instalação do Policy Director para Windows” na página 35

   Capítulo 6, “Instalação do Policy Director para AIX” na página 47

   Capítulo 7, “Instalação do Policy Director para Solaris” na página 61
9. Configure o CAS (Credentials Acquisition Service) do Policy Director se estiver utilizando o Policy Director CAS para autenticação de certificado de cliente. Consulte “Configuração do Credentials Acquisition Service” na página 21 para obter informações sobre o Policy Director CAS.
10. Instale o Console de Gerenciamento. Consulte o capítulo de instalação referente à plataforma do sistema operacional que estará sendo utilizado. Utilize um dos seguintes:

    Para Windows NT, consulte a “Instalação do Console de Gerenciamento no Windows” na página 42.

Para AIX, consulte a “Instalação do Console de Gerenciamento” na página 57 se você estiver utilizando o registro de usuário DCE ou a “Configuração e início do Console de Gerenciamento” na página 51 se estiver utilizando o registro de usuário LDAP.

Para Solaris, consulte a “Instalação do Console de Gerenciamento” na página 70.

Reinstalação do Policy Director

Se for necessário reinstalar qualquer pacote, você deve remover o pacote existente e, em seguida, reinstalar o pacote desejado. Consulte “Remoção do Policy Director” na página 58 para obter instruções.

Configuração do Credentials Acquisition Service

O Credentials Acquisition Service (CAS) do Policy Director é um componente personalizável do Policy Director que você pode utilizar para estender os mecanismos de autenticação padrão que são suportados pelo WebSEAL.

O CAS do Policy Director é instalado automaticamente. Se desejar utilizar o CAS do Policy Director como seu serviço de aquisição de credenciais, você deve configurá-lo. Consulte os capítulos 2 e 13 no *Policy Director Administration Guide* para obter informações para entendimento e configuração do CAS do Policy Director.

Capítulo 4. Instalação e configuração do IBM SecureWay Directory

Se você planeja utilizar um registro de usuário DCE, você pode ignorar esta seção sobre instalação e configuração do IBM SecureWay Directory (LDAP).

Durante a instalação do Policy Director, será solicitado que você escolha um registro de usuário LDAP ou um DCE.

Se você escolher LDAP, é necessário instalar um Cliente SDK e servidor IBM SecureWay Directory Versão 3.1.1 (LDAP) e, em seguida, configurar o servidor LDAP antes de instalar o Policy Director.

Se você utilizar SSL para acessar o servidor LDAP, o cliente LDAP também deve ser configurado.

Instalação do cliente e do servidor LDAP

O Policy Director requer um servidor e um cliente LDAP se você estiver utilizando LDAP como seu registro de usuário.

Um servidor LDAP deve estar instalado em pelo menos um computador no domínio seguro. O cliente e o servidor LDAP são fornecidos como parte do produto Policy Director. Você deve instalá-los antes de instalar o Policy Director ou utilizar uma instalação de LDAP existente que esteja no nível correto.

Durante a instalação do LDAP, escolha instalar o **SecureWay Directory e Client SDK**.

Para obter mais informações sobre a instalação e configuração do LDAP, consulte a documentação *IBM SecureWay Directory Installation and Configuration, Versão 3.1.1*. Há uma versão separada deste manual no formato HTML para cada um dos sistemas operacionais suportados no CD apropriado. Consulte “Documentação do IBM SecureWay Directory” na página 75 para obter informações sobre como acessar a documentação.

Instalação apenas do cliente LDAP

Se você estiver utilizando LDAP como seu registro de usuário, é necessário instalar o cliente LDAP em cada sistema que irá executar o Policy Director. O cliente LDAP é fornecido como parte do produto Policy Director. Instale o cliente LDAP antes de instalar o Policy Director.

Durante a instalação do LDAP, escolha instalar o **SecureWay Client SDK** apenas se você já tiver uma instalação do servidor LDAP server que esteja no nível correto já instalado e configurado para o Policy Director.

Configuração do servidor LDAP

Se você estiver utilizando LDAP como seu registro de usuário, é necessário configurar o servidor LDAP antes de instalar o primeiro servidor Policy Director. Depois de configurar o servidor LDAP para o primeiro sistema Policy Director, não é necessário reconfigurar o servidor LDAP ao adicionar servidores Policy Director adicionais.

Se você tiver ativado o acesso SSL ao servidor LDAP durante a configuração do servidor LDAP, será necessário copiar um par de conjuntos de chaves cliente e servidor para cada computador adicional que utiliza acesso SSL. Consulte o “Ativação de acesso SSL (opcional)” na página 26 para obter mais informações.

Para configurar o servidor LDAP, é necessário concluir as etapas de configuração na lista a seguir uma única vez para cada domínio seguro:

1. Adicionar sufixos necessários. Consulte “Adição de sufixos” para obter instruções.
2. Instalar objetos e atributos de esquema de segurança. Consulte “Instalação de objetos e atributos de esquema de segurança” na página 25.
3. Ativar controle de acesso LDAP. Consulte “Ativação do controle de acesso LDAP” na página 33 para obter instruções.
4. Ativar acesso SSL. Consulte “Ativação de acesso SSL (opcional)” na página 26 para obter instruções.

Se você ativou o acesso SSL, conclua as etapas em “Configuração do cliente LDAP para acesso SSL” na página 31 toda vez que adicionar um cliente LDAP (servidor Policy Director) que utilize SSL para acessar o servidor LDAP.

Nota: Os administradores LDAP podem especificar definições de criptografia de senha no banco de dados LDAP. O LDAP permite que senhas sejam armazenadas como texto sem proteção, o que representa um risco de segurança. Consulte a documentação do LDAP para obter instruções sobre a definição de atributos de senhas de usuários no nível de criptografia apropriado.

Adição de sufixos

No IBM SecureWay Directory, crie um novo sufixo, concluindo as seguintes etapas:

1. Utilizando um Navegador da web, acesse a ferramenta de Administração da Web do IBM SecureWay Directory Server no endereço

   `http://servername/ldap`

   Inicie sessão através da interface da Web como o administrador LDAP (por exemplo, `cn=root`).
2. Clique em: **Sufixos** → **Adicionar um sufixo**.
3. No campo **DN do Sufixo**, você deve adicionar o sufixo:

   `secAuthority=Default`

   O objeto para `secAuthority=Default` é criado durante a configuração do servidor de Gerenciamento.
4. Clique no botão **Adicionar um novo sufixo**.
5. Para adicionar outro sufixo, clique no link **Adicionar um sufixo** para retornar à janela anterior.
6. Se necessário, adicione um sufixo para seus usuários do Policy Director e dados GSO (Global Sign-On). Por exemplo:

   `o=IBM,c=BR`

   Você pode denominar os sufixos como desejar de uma maneira apropriada para sua instalação, em que `o=` é o nome abreviado de sua organização e `c=` é o país.

Esta etapa cria sufixos para seus dados GSO e para seus usuários e grupos. Estes sufixos são criados com a ferramenta de Administração da Web LDAP.

7. Clique no botão **Adicionar um novo sufixo**.
8. Repita o procedimento para cada novo sufixo que desejar adicionar e que for necessário para sua organização.
9. Clique no link **reiniciar o servidor** na página da Web da ferramenta de Administração LDAP para reiniciar o servidor LDAP quando tiver terminado de adicionar sufixos.

Instalação de objetos e atributos de esquema de segurança

O Policy Director utiliza um conjunto de objetos e atributos LDAP para manter credenciais de usuários dentro do servidor LDAP.

Utilize o IBM SecureWay Directory Management Tool (DMT) para determinar se os objetos e os atributos de segurança estão instalados. Instale-os se eles ainda não estiverem instalados. O DMT é instalado como parte do pacote IBM SecureWay Directory.

Para determinar se os objetos e os atributos do Policy Director estão instalados, conclua as seguintes etapas:

1. Inicie o Directory Management Tool em um cliente LDAP.

   Nota: Se você receber uma mensagem informando que não há nenhuma entrada para o sufixo secAuthority=Default, você pode prosseguir com segurança. O objeto para o sufixo secAuthority=Default é criado durante a configuração do servidor de Gerenciamento.

2. Clique em **Esquema → Classes de objetos → Exibir classes de objetos**.
3. Verifique se todos os seguintes objetos e atributos do Policy Director estão presentes:

   Classes de objetos
   secAuthorityInfo
   secGroup
   secMap
   secPolicy
   secPolicyData
   secUser

4. Clique em **Esquema → Atributos → Exibir atributos**
5. Verifique se todos os seguintes objetos e atributos do Policy Director estão presentes:

   Atributos
   secUUID
   secLoginType
   secAuthority
   secAcctValid
   secPwdValid
   secDN
   secPwdMgmtBind
   secAcctExpires
   secAcctInactivity
   secAcctLife
   secPwdAlpha
   secPwdSpaces
   secPwdFailures

secPwdLastChanged
secPwdLastUsed

6. Execute uma das seguintes etapas baseado nos resultados encontrados na etapa 3 na página 25 e na etapa 5 na página 25.

   Se todos os objetos estiverem presentes, nenhuma ação adicional é necessária. Continue com "Ativação de acesso SSL (opcional)".

   Se *alguns*, mas não todos, dos objetos estiverem presentes, vá para a etapa 7.

   Se *nenhum* dos objetos estiverem presentes, vá para a etapa 8.

7. Se alguns, mas não todos, os objetos e atributos do Policy Director forem encontrados, remova os objetos e atributos do Policy Director existente.

   No DMT, clique em:

   Esquema → Classes de objetos → Excluir classes de objetos e remova as classes de objetos.

   Em seguida, clique em **Esquema → Atributos → Excluir atributos** e remova os atributos.

8. Se nenhum dos objetos e atributos do Policy Director forem encontrados, insira o CD do *IBM SecureWay Policy Director Versão 3.0*.

9. Em um prompt de comandos, utilize **ldapmodify** para carregar o arquivo de esquema. Por exemplo, digite:

   UNIX:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/secschema.def
   ```

   Windows:

   ```
   ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\secschema.def
   ```

   em que *x:* é a letra de sua unidade de CD-ROM do Windows.

10. Se você planejar utilizar o Policy Director para gerenciar usuários do SecureWay Boundary Server, também é necessário adicionar os objetos e atributos do arquivo de esquema do Policy Director:

    Utilize o comando **ldapmodify** em um prompt de comandos para carregar o arquivo de esquema. Por exemplo, digite:

    Windows:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f x:\schema\puschema.def
    ```

    UNIX:

    ```
    ldapmodify -h hostname -p 389 -D cn=root -w password -f /schema/puschema.def
    ```

    em que *x:* é a letra de sua unidade de CD-ROM.

Ativação de acesso SSL (opcional)

Se o acesso SSL ao seu servidor LDAP não for necessário, ignore esta seção. Vá para "Ativação do controle de acesso LDAP" na página 33.

Se o acesso SSL for requerido por seu servidor LDAP, continue com esta seção. Este procedimento precisa ser executado apenas na primeira vez em que a comunicação SSL é configurada entre o servidor e o cliente LDAP.

Opcionalmente, você pode ativar a utilização do SSL para proteger comunicações entre os servidores Policy Director e o servidor LDAP.

O IBM Global Security Kit (GSKit) SSL Runtime Toolkit Versão 3.0.1 é instalado durante a instalação do LDAP. O GSKit fornece duas versões de um Key Management Tool — uma é uma versão em janelas**ikmguiw** e a outra é uma versão sem janelas **ikmgui**. Você pode utilizar qualquer uma das versões sempre que **ikmguiw** for chamado nos seguintes procedimentos.

Instruções completas sobre como utilizar esta ferramenta podem ser encontradas na documentação do LDAP. Consulte “Documentação do IBM SecureWay Directory” na página 75.

Ou, você pode seguir estes procedimentos abreviados especificamente para ativar o Policy Director para acesso SSL.

Criação do arquivo de banco de dados de chaves e do certificado

Para ativar o suporte SSL no servidor LDAP, o servidor deve possuir um certificado que o identifica e que ele pode utilizar como um *certificado pessoal*. Este certificado pessoal é o certificado que o servidor envia para o cliente para permitir que o cliente autentique o servidor. Os certificados e o par de chaves pública e privada são armazenados em um arquivos de banco de dados de chaves. Normalmente, um cliente adquire um *certificado assinado* de um CA (Autoridade de Certificado), como VeriSign.

No entanto, você também pode utilizar um certificado *auto-assinado*. Se utilizar um certificado auto-assinado a máquina em que o certificado é gerada se torna o CA.

Utilize o GSKit's Key Management Tool (**ikmguiw**) para criar o arquivo de banco de dados de chaves e o certificado. Para criar o arquivo de banco de dados de chaves e o certificado (auto-assinado ou assinado):

1. Certifique-se de que o IBM Global Security Kit (GSKit) SSL Runtime Toolkit Versão 3.0.1 e o Key Management Tool baseado em Java estejam instalados no servidor LDAP e em quaisquer clientes LDAP que estarão utilizando o SSL.

   Windows: `C:\Arquivos de Programas\IBM\GSK\bin\ikmguiw.exe`

   Solaris: `/opt/IBM/GSK/bin/ikmguiw`

   AIX: `/usr/lpp/ibm/gsk/bin/ikmguiw`

2. Inicie a ferramenta IBM Key Management (**ikmguiw**).
3. Clique em **Arquivo de Banco de Dados de Chaves → Novo**.
4. Certifique-se de que o **arquivo de banco de dados de chaves CMS** seja o tipo de banco de dados de chaves selecionado.
5. Digite as informações nos campos **Nome do Arquivo** e **Localização** em que você deseja que o arquivo de banco de dados de chaves seja localizado. A extensão do arquivo de banco de dados de chaves é *.kdb*.
6. Clique em **OK**.
7. Digite a senha do arquivo de banco de dados de chaves e confirme-a.

   Memorize esta senha pois ela é necessária para editar o arquivo de banco de dados de chaves.
8. Aceite a data de expiração padrão ou altere-a de acordo com os requisitos de sua organização.

9. Se desejar que a senha seja mascarada e armazenada em um arquivo oculto, clique em **Oculte a senha em um arquivo**.

   Um arquivo oculto pode ser utilizado por alguns aplicativos de maneira que o aplicativo não precise conhecer a senha para utilizar o arquivo de banco de dados de chaves. O arquivo oculto possui a mesma localização e nome que o arquivo de banco de dados de chaves e possui uma extensão *.sth*.
10. Clique em **OK**.

Isto conclui a criação do arquivo de banco de dados de chaves. Há um conjunto de certificados assinados padrão. Estes certificados assinados são as Autoridades de Certificado padrão reconhecidos.

Criação de um Certificado Pessoal

Se você planeja utilizar um certificado de uma Autoridade de Certificado (como VeriSign), você deve pedir o certificado para o CA e recebê-lo depois que ele tiver sido concluído. Conclua as etapas em "Recebimento do certificado".

Recebimento do certificado: Se você estiver utilizando um certificado de uma Autoridade de Certificado (como VeriSign) ao invés de um certificado auto-assinado, conclua estas etapas:

1. Utilize **ikmguiw** para pedir um certificado de um CA (Autoridade de Certificado) e receba o novo certificado em seu arquivo de banco de dados de chaves.
2. Clique na seção **Pedidos de Certificado Pessoal** no arquivo de banco de dados de chaves.
3. Clique em **Novo**.
4. Preencha todas as informações para produzir um pedido que possa ser enviado à Autoridade de Certificado.
5. Clique em **OK**.
6. Quando o CA retornar o certificado, você pode instalá-lo em seu arquivo de banco de dados de chaves, clicando na seção **Certificados Pessoais** e clicando em **Receber**.
7. Quando o certificado do servidor LDAP estiver em seu arquivo de banco de dados de chaves, você pode configurar o servidor LDAP para ativar SSL.

Se seu certificado ainda não for reconhecido, copie o certificado do CA para a máquina do cliente.

Se seu certificado for gerado por um CA que já é reconhecido (como VeriSign), nenhuma ação adicional é necessária. Vá para "Configuração do servidor LDAP para ativar SSL" na página 30.

Criação de um certificado auto-assinado: Se você planejar utilizar um certificado de uma Autoridade de Certificado (como VeriSign) ao invés de um certificado auto-assinado, conclua estas etapas."Recebimento do certificado".

Para criar um novo certificado auto-assinado e armazená-lo no arquivo de banco de dados de chaves:

1. Clique em **Criar → Novo Certificado Auto-Assinado**.
2. Digite um nome no campo **Rótulo de Chave** que o GSKit possa utilizar para identificar este novo certificado no Banco de Dados de Chaves.

   Por exemplo, o rótulo pode ser o nome da máquina do servidor LDAP.

3. Aceite os padrões para o campo **Versão**, que é X509 V3 e para o campo **Tamanho da Chave**.
4. Aceite o nome da máquina padrão ou digite um nome distinto diferente no campo **Nome Comum** para este certificado.
5. Digite um nome de empresa no campo **Organização**.
6. Preencha os campos opcionais ou deixe-os em branco.
7. Aceite os padrões para o campo **País** e 365 para o campo **Período de Validade** ou altere-os de acordo com os requisitos de sua organização.
8. Clique em **OK**.

   O GSKit gera um novo par de chaves pública e privada e cria o certificado.

   Se você tiver mais de um certificado pessoal no arquivo de banco de dados de chaves, o GSKit pergunta se você deseja que esta chave seja a chave padrão no banco de dados. Você pode aceitar uma delas como a padrão. O certificado padrão é utilizado em tempo de execução quando um rótulo não é fornecido para selecionar qual certificado utilizar.

Isto conclui a criação do certificado pessoal do servidor LDAP. Ele deve aparecer na seção Certificados Pessoais do arquivo de banco de dados de chaves. Utilize a barra do meio do Key Management Tool para selecionar entre os tipos de certificados mantidos no arquivo de banco de dados de chaves.

Em seguida, você deve extrair seu certificado de servidor LDAP para um arquivo de dados ASCII codificado em Base64.

Extração do certificado auto-assinado

Se seu certificado for auto-assinado, você deve extrair o certificado do assinante do arquivo de banco de dados de chaves. Continue com este procedimento de extração.

Esta extração é utilizada para configurar a máquina cliente. Se você criou um certificado auto-assinado em “Criação de um certificado auto-assinado” na página 28, ele também aparece na seção `Certificados do Assinante` do arquivo de banco de dados de chaves pois ele é um certificado auto-assinado. Quando você estiver na seção Certificados do Assinante do Banco de Dados de Chaves, certifique-se de que o certificado esteja lá.

Para extrair o certificado do assinante:

1. Utilize **ikmguiw** para extrair seu certificado de servidor LDAP para um arquivo de dados ASCII codificado em Base64. Este arquivo será utilizado no procedimento “Configuração do cliente LDAP para acesso SSL” na página 31.
2. Destaque o certificado auto-assinado que você acabou de adicionar em “Criação de um certificado auto-assinado” na página 28.
3. Clique em **Extrair Certificado**.
4. Clique em **Dados ASCII codificados em Base64** como o tipo de dados.
5. Digite um nome de arquivo de certificado para o certificado recém extraído. A extensão do arquivo de certificado é *.arm*.
6. Digite a localização em que deseja armazenar o certificado extraído.
7. Clique em **OK**.
8. Copie este certificado extraído para a máquina cliente LDAP.
9. Você pode configurar o servidor LDAP para ativar SSL.

Configuração do servidor LDAP para ativar SSL

Para configurar o servidor LDAP para ativar SSL:

1. Certifique-se de que o servidor LDAP esteja instalado e em execução se você for utilizar LDAP como o registro de usuário. Consulte Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23 para obter instruções completas.
2. Utilize a ferramenta de administração LDAP baseada na Web com a seguinte URL:

   ```
   http://servername/ldap
   ```

   Em que *servername* é o nome da máquina do servidor LDAP.
3. Inicie sessão como o administrador LDAP (por exemplo, cn=root) se você já não tiver iniciado sessão.
4. Clique em **Servidor → SSL**.
5. Clique em **SSL Ativado**, que é para ativação de SSL ou não-SSL ou clique em **SSL Apenas** para o status SSL que você deseja definir.
6. Clique em **Autenticação do Servidor** para o tipo de método de autenticação.
7. Digite um número de porta ou aceite o número de porta padrão 636.
8. Digite o caminho do banco de dados de chaves e o nome do arquivo que você especificou na etapa 5 em Criação do arquivo de banco de dados de chaves e do certificado.

   A extensão do arquivo de banco de dados de chaves é.*kdb*
9. Digite o nome no campo **Rótulo de Chave** que você utilizou para identificá-lo quando armazenou o certificado do servidor LDAP no Banco de Dados de Chaves. Por exemplo, o rótulo pode ser o nome da máquina do servidor LDAP.
10. Digite a senha do arquivo de banco de dados de chaves e confirme-a. Ou, deixe o campo da senha em branco se desejar que o servidor LDAP utilize o arquivo oculto.
11. Clique em **Aplicar**.
12. Clique no link **reiniciar o servidor** para reiniciar o servidor LDAP e permitir que esta alteração seja efetivada.

Teste do acesso SSL: Para testar se o SSL foi ativado, digite o seguinte comando em uma linha de comandos do servidor LDAP:

```
ldapsearch -h servername -Z -K keyfile -P key_pw -b "" -s base \
objectclass=
```

A barra invertida (\) neste comando é necessária apenas quando o comando não puder ser digitado em uma linha.

Em que:

Opção	Descrição
servername	O nome do host DNS do servidor LDAP.
keyfile	O nome completo do caminho do conjunto de chaves gerado.
key_pw	A senha do conjunto de chaves gerado.

Este comando retorna informações básicas do LDAP, incluindo os sufixos no servidor LDAP.

A configuração do SSL do servidor está concluída. Em seguida, configure o cliente LDAP para acesso SSL.

Configuração do cliente LDAP para acesso SSL

Depois de configurar o servidor LDAP para acesso SSL, você deve configurar os clientes LDAP para acesso SSL.

Criação de um arquivo de banco de dados de chaves: Certifique-se de que o GSKit esteja instalado no cliente e crie um novo arquivo de banco de dados de chaves utilizando o IBM Key Management Tool conforme descrito em "Criação do arquivo de banco de dados de chaves e do certificado" na página 27.

Para que o cliente seja capaz de autenticar o servidor LDAP, o cliente deve reconhecer a Autoridade de Certificado (assinante) que criou o certificado do servidor LDAP. Se o servidor LDAP estiver utilizando um certificado auto-assinado, o cliente deve ser ativado para reconhecer a máquina que gerou o certificado do servidor LDAP como uma raiz confiável (Autoridade de Certificado).

Adição de um certificado de assinante: Para adicionar um certificado de assinante depois que o arquivo de banco de dados de chaves tiver sido criado:

1. Certifique-se de que o certificado que foi extraído do arquivo de banco de dados de chaves em "Extração do certificado auto-assinado" na página 29 foi copiado para a máquina cliente. Se ele não foi copiado, copie-o agora.
2. Clique na seção **Certificados de Assinantes** do arquivo de banco de dados de chaves CMS.
3. Clique em **Adicionar**.
4. Clique em **Dados ASCII codificados em Base64** para definir o tipo de dados.
5. Indique o nome do arquivo do certificado e sua localização. A extensão do arquivo de certificado é *.arm*.
6. Clique em **OK**.
7. Digite um rótulo para o certificado do assinante que você está adicionando. Por exemplo, talvez você deseje utilizar o nome da máquina do servidor LDAP para o rótulo.
8. Clique em **OK**.

   O certificado auto-assinado aparece no Banco de Dados de Chaves do cliente como um certificado de assinante.
9. Destaque o certificado de assinante recém adicionado e clique em **Exibir/Editar**.
10. Certifique-se de que ele esteja marcado como uma raiz confiável garantindo que **Definir o certificado como uma raiz confiável** está selecionada.

    Se o certificado do servidor LDAP foi gerado por uma Autoridade de Certificado normal, certifique-se de que a Autoridade de Certificado esteja listada como um certificado de assinante e marcada como uma raiz confiável. Caso contrário, adicione o certificado da Autoridade de Certificado como um certificado de assinante e indique que ele é uma raiz confiável.

Neste ponto, o cliente deve estar apto a estabelecer uma sessão SSL com o servidor LDAP.

Teste de ativação SSL: Para testar se o SSL foi ativado, digite o seguinte comando em uma linha de comandos no cliente LDAP:

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -b "" \
-s base objectclass=
```

A barra invertida (\) neste comando é necessária apenas quando o comando não puder ser digitado em uma linha.

Em que:

Opção	Descrição
servername	O nome do host DNS do servidor LDAP.
client_keyfile	O nome completo do caminho do conjunto de chaves gerado.
key_pw	A senha do conjunto de chaves gerado.

Este comando retorna informações básicas do LDAP, incluindo os sufixos no servidor LDAP.

A configuração do SSL está concluída.

Utilização de tipo de autenticação de servidor e cliente LDAP (opcional)

Esta seção da configuração é opcional:

1. Conclua o procedimento conforme descrito em “Configuração do servidor LDAP para ativar SSL” na página 30. No entanto, ao invés de configurar o servidor LDAP para **Autenticação de Servidor**, selecione executar a **Autenticação de Servidor e de Cliente**.

   Neste caso, depois que o servidor tiver enviado seu certificado para o cliente e tiver sido autenticado pelo cliente, o servidor solicita o certificado do cliente. Se o servidor LDAP estiver configurado para ambos, é necessário estabelecer um certificado para a máquina cliente também.
2. Na máquina cliente, o estabelecimento de um certificado para a máquina cliente é feito conforme descrito nestes procedimentos:

   “Criação do arquivo de banco de dados de chaves e do certificado” na página 27

   “Criação de um certificado auto-assinado” na página 28, se seu certificado for um certificado auto-assinado ou “Recebimento do certificado” na página 28, se seu certificado for um certificado de assinante.

   “Extração do certificado auto-assinado” na página 29

   “Configuração do servidor LDAP para ativar SSL” na página 30
3. No servidor LDAP, depois que o certificado pessoal do cliente foi criado e adicionado ao arquivo de banco de dados de chaves do cliente, a Autoridade de Certificado que criou esse certificado de cliente deve ser reconhecida como um certificado de assinante (raiz confiável). O certificado da Autoridade de Certificado é adicionado ao Banco de Dados de Chaves do servidor LDAP conforme descrito em “Adição de um certificado de assinante” na página 31.

Teste do acesso SSL: Depois que o servidor LDAP reconhece a Autoridade de Certificado que criou o certificado pessoal do cliente, a configuração pode ser testada através do seguinte comando:

```
ldapsearch -h servername -Z -K client_keyfile -P key_pw -N client_label \
-b "" \ -s base objectclass=
```

A barra invertida (\) neste comando é necessária apenas quando o comando não puder ser digitado em uma linha.

Em que:

Opção	Descrição
servername	O nome do host DNS do servidor LDAP.
client_keyfile	O nome completo do caminho do conjunto de chaves cliente gerado.
key_pw	A senha do conjunto de chaves gerado.
client_label	O rótulo associado à chave, se existente. Este campo é opcional e é necessário apenas se o servidor LDAP for configurado para executar autenticação de cliente e de servidor.

Este comando retorna informações básicas do LDAP, incluindo os sufixos no servidor LDAP. Observe que o parâmetro **-N** indica o rótulo que foi especificado quando o certificado pessoal do cliente foi adicionado ao arquivo de banco de dados de chaves do cliente.

Não especifique o rótulo do certificado de assinante do servidor LDAP. O parâmetro **-N** indica para o GSKit qual certificado de cliente é enviado para o servidor quando solicitado. Se nenhum rótulo for especificado, o certificado pessoal padrão é enviado quando o servidor solicita o certificado do cliente.

A configuração do SSL está concluída.

Ativação do controle de acesso LDAP

Para concluir a integração de segurança do Policy Director com o registro de usuário LDAP, atualize as ACLs do LDAP que controlam o registro de usuário concluindo as seguintes etapas:

1. Inicie o Directory Management Tool no servidor ou no cliente LDAP, clicando em **Iniciar → Programas → IBM SecureWay Directory → Directory Management Tool**.
2. Faça bind do servidor:
   a. Clique em **Servidor → Refazer bind**.
   b. Clique em **Autenticado**.
   c. Digite o DN do usuário (por exemplo, cn=root).
   d. Digite sua senha.
   e. Clique em **OK**.
3. Clique em **OK** ou feche a janela de mensagem de aviso para cada mensagem de aviso que aparecer.
4. Forneça ao grupo daemon de segurança Policy Director o controle total sobre os sufixos criados em “Adição de sufixos” na página 24.
   a. Clique em **Entradas → Adicionar Entrada**.
   b. Digite o sufixo de seu banco de dados de usuários do Policy Director e usuários GSO em **RDN de entrada**. Por exemplo:

      ```
      o=IBM,c=BR
      ```

   c. Clique em **Organização**.
   d. Clique em **Avançar**.

A janela Criar uma Entrada LDAP aparece.

e. Adicione as informações apropriadas de sua organização e, em seguida, clique no botão **Criar**.

f. Clique em **Árvore → Atualizar árvore** e a nova entrada deve aparecer no Navegador da árvore de diretórios.

5. Forneça ao grupo daemon de segurança do Policy Directoro controle total adicionando o seguinte à lista de proprietários de cada ACL LDAP de controle:

   `cn=SecurityGroup,secAuthority=Default`

   clicando na guia **ACL**.

   A janela **Editar um ACL LDAP** aparece.

   a. Digite `cn=SecurityGroup,secAuthority=Default` no campo DN e, em seguida, clique em **grupo** na lista drop down.

   b. Clique no botão **Adicionar**.

   c. Selecione todas as caixas de opções em Direitos Concedidos para Adicionar, Excluir e Classe.

   d. Ao concluir, clique em **Alterar** e `cn=SecurityGroup,secAuthority=Default` deve aparecer na lista de ACLs de seu DN de sufixo.

   e. Repita o procedimento para cada sufixo, se você possuir mais de um, para adicionar à lista de proprietários.

A configuração do LDAP agora está concluída.

Capítulo 5. Instalação do Policy Director para Windows

As seções deste capítulo descrevem como instalar e configurar o Policy Director em plataformas Windows e Windows NT suportadas.

Antes de começar a instalação do Policy Director, certifique-se de ter revisto as informações em "Antes de instalar o Policy Director para Windows".

Antes de instalar o Policy Director para Windows

Antes de começar a instalação do NetSEAT e Policy Director, leias as seguintes informações:

Antes de instalar o NetSEAT e o Policy Director, você deve inicialmente instalar e configurar o servidor Windows NT.

Você deve conhecer as senhas do administrador de domínio do Windows NT e do administrador de domínio seguro (por exemplo, a conta cell_admin). Certifique-se de obter privilégios de administrador.

Se você estiver criando uma nova célula DCE ao instalar os servidores Policy Director no sistema operacional Windows NT:

— Você deve também instalar e configurar um servidor DCE.

— Se você estiver utilizando LDAP para seu registro de usuário, é necessário também instalar e configurar um servidor LDAP.

Familiarize-se com todas as informações relativas à implementação do Policy Director, conforme descrito em "Requisitos de instalação para o domínio seguro" na página 18.

Instalação do NetSEAT e do Policy Director

Antes de começar a instalação do Policy Director, certifique-se de que todos os aplicativos estejam fechados. Depois de terminar a instalação do Policy Director, você deve encerrar e reiniciar o computador.

Conclusão do Inventário do Domínio Seguro

Durante a instalação, você deve fornecer as informações a seguir para a configuração de seu domínio seguro:

O nome de seu domínio seguro (célula DCE), por exemplo cell_admin.

Os nomes dos computadores que estiverem fornecendo os seguintes serviços:

— Segurança

— Hora

— CSD (Cell Directory Services)

— DSB (Directory Services Broker)

Instalação do NetSEAT

O arquivo de configuração do NetSEAT do Policy Director copia os arquivos do NetSEAT em seu disco rígido e, em seguida, inicia o utilitário de configuração do NetSEAT automaticamente.

Para instalar o NetSEAT:

1. Inicie sessão como um usuário com privilégios de administrador.
2. Insira o *IBM SecureWay Policy Director Versão 3.0* CD na unidade de CD-ROM.
3. Altere para o diretório \win32\client no CD.
4. Dê um clique duplo no arquivo Setup.exe e o programa InstallShield é iniciado.
5. Quando a janela Escolher Idioma de Instalação aparecer, selecione o idioma apropriado.
6. Clique em **Avançar** e a janela Bem-Vindo do Policy Director é exibida.
7. Clique em **Avançar**.
8. Quando a janela Escolher Componentes a Instalar for exibida, clique em **Cliente para produtos do servidor Policy Director**.
9. Clique em **Avançar**.
10. Quando a janela Escolher Tipo de Configuração for exibida, clique em **Típica**.

    A localização padrão de uma instalação típica é:

    `c:\Arquivos de Programas\ibm\netseat\`

    Ou, se você clicar em **Personalizar**, especifique a unidade e o diretório em que deseja que o NetSEAT seja instalado.

    A janela Escolher Localização de Destino é exibida.
11. Clique em **Avançar**.

    Os arquivos do NetSEAT são copiados para a localização padrão do NetSEAT em seu disco rígido. A janela Configuração do NetSEAT é exibida.

Configuração do NetSEAT

As tarefas de configuração do NetSEAT fornecem ao NetSEAT as informações sobre o domínio seguro, como os nomes de servidores DCE, localizações e serviços.

Depois que todos os arquivos do NetSEAT tiverem sido copiados para o disco rígido, a janela Configuração do NetSEAT (guia **Domínios Seguros**) é exibida.

Para configurar o NetSEAT:

1. Para adicionar uma entrada de um novo domínio seguro, clique em **Adicionar**.

   A janela Novo Domínio Seguro é exibida.
2. Digite o nome do domínio seguro (célula DCE) ao qual o NetSEAT irá pertencer, como cell_admin.
3. Selecione a caixa de opções **Ativar GSS** ou **Ativar SSL**.
4. Clique em **OK**.

   A janela Propriedades do Domínio Seguro é exibida.
5. Para adicionar um servidor DCE e os serviços fornecidos por ele, clique em **Adicionar**.

   A janela Adicionar um Servidor DCE é exibida.

   Utilize esta janela para informar o NetSEAT sobre os servidores DCE existentes no domínio seguro e os serviços fornecidos por cada um. Pode ser necessário adicionar mais de um servidor DCE. Todos os serviços podem estar em um computador ou divididos entre vários computadores.

Os cenários possíveis incluem:

Novo Domínio Seguro (um sistema host)

Se você estiver criando um novo domínio seguro que consiste em apenas um sistema host, seu sistema host fornece todos os serviços DCE. Digite o nome de seu sistema host no campo **Nome da Máquina**. Selecione um serviço ou mais. Selecione o DSB mesmo que ele ainda não esteja instalado.

Novo Domínio Seguro (mais de um host)

Se você estiver criando um novo domínio seguro e os serviços DCE estiverem localizados em outro host, seu host local fornecerá apenas o serviço DSB. Neste caso, primeiro adicione o servidor DCE que está fornecendo os serviços DCE (Segurança, Hora, CDS). Em seguida, adicione outro servidor DCE denominado `localhost` para representar seu sistema local e selecione a caixa de opções DSB. Você pode selecionar o DSB mesmo que ele ainda não esteja instalado.

Domínio Seguro Existente

Se você estiver adicionando o Policy Director em um domínio seguro existente, adicione o nome do servidor DCE que fornece Segurança, Hora e CDS. Em seguida, adicione o nome do servidor DCE que inclui o servidor de Gerenciamento do Policy Director que possui o DSB instalado automaticamente. Selecione a caixa de opções DSB deste sistema. Neste cenário todos os serviços, inclusive o DSB, podem estar localizados no mesmo sistema host.

6. Para cada servidor, digite o nome da máquina DN completo de um servidor existente no domínio seguro (por exemplo, SFF98732.austin.ibm.com).
7. Para cada servidor, selecione um ou mais serviços do servidor:

   Segurança

   DSB

   Hora

   CDS
8. Clique em **OK**.

   A janela Propriedades do Domínio Seguro exibe a nova entrada.
9. Conforme necessário, repita a etapa 5 na página 36 até a etapa 8 para adicionar servidores e serviços adicionais.
10. Na janela Propriedades do Domínio Seguro, aceite a configuração de início de sessão avançada de **Início de sessão DCE apenas**.

    A área de início de sessão integrado da janela Propriedades de Domínios Seguros não é utilizada nesta instalação do NetSEAT.
11. Clique em **OK**.

    A janela Configuração do NetSEAT é exibida.
12. Clique em **OK**.

    A janela Reinício do Sistema Requerido é exibida.
13. Clique em **Sim** para reiniciar o computador.
14. Clique em **OK**.

    Quando o computador é reiniciado, o NetSEAT iniciar automaticamente. Um ícone do NetSEAT aparece na barra de tarefas do Windows.

    A instalação e a configuração do NetSEAT estão concluídas.

Verificação da configuração do cliente NetSEAT

Antes de instalar o servidor Policy Director, verifique se o cliente NetSEAT está configurado com êxito no domínio seguro especificado. Utilize **netseat_ping** para determinar se os serviços a seguir estão disponíveis:

Serviço de Segurança

Serviço de Hora

Serviço do Diretório de Células

DSB (Directory Services Broker)

Para verificar se o cliente NetSEAT pode se comunicar com os serviços necessários, conclua as etapas a seguir:

1. Clique em **Iniciar → Programas → NetSEAT → Início de Sessão do NetSEAT** para iniciar sessão como cell_admin.

   Ou, você pode utilizar o comando **netseat_login** na linha de comandos para iniciar sessão.
2. Não selecione Início de sessão PKI a menos que ele seja especificamente necessário para sua configuração.
3. Digite o nome e a senha do usuário do Administrador do Policy Director.
4. Clique em **OK**.
5. Na linha de comandos, utilize o comando **netseat_ping** para obter o status da configuração.

   Por exemplo, se um cliente NetSEAT for configurado em um domínio seguro denominado "redback," obtenha o status digitando este comando no prompt do DOS:

   ```
   netseat_ping -C redback
   ```

   Informações semelhantes a saída a seguir devem ser exibidas:

   ```
   /.../redback:
         SecurityServers:
                   ncacn_ip_tcp:redback[ ] está disponível
                   ncadg_ip_udp:redback[ ] está disponível
         CdsServers:
                   ncacn_ip_tcp:redback[ ] está disponível
                   ncadg_ip_udp:redback[ ] está disponível
         TimeServers:
                   ncacn_ip_tcp:redback[ ] está disponível
                   ncadg_ip_udp:redback[ ] está disponível
         DsbServers:
                   ncacn_ip_tcp:redback[ ] não disponível
                   ncacn_ip_udp:redback[ ] não disponível
   ```

   No entanto, observe que o DSB ainda não estará sendo executado se você planeja criar um novo domínio seguro. Neste caso, a saída do **netseat_ping** para o DSB será `não disponível`. Este status é a saída esperada para este cenário. Você pode prosseguir com segurança com a instalação do Policy Director pois a instalação do componente do servidor de Gerenciamento do Policy Director instalará, configurará e iniciará o DSB automaticamente. Se o DSB já estiver sendo executado, a saída do DSB será `está disponível (v3.1)`.
6. Se quaisquer serviços além do DSB não estiverem disponíveis, resolva o problema antes de instalar os servidores Policy Director.

Instalação dos servidores Policy Director

Antes de iniciar a instalação dos servidores Policy Director, certifique-se de que você sabe o nome e a senha do usuário de um administrador.

Para instalar os componentes do servidor Policy Director:

1. Certifique-se de que o servidor LDAP esteja instalado e em execução se você for utilizar LDAP como o registro de usuário. Consulte Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23 para obter instruções completas
2. Insira o CD do *IBM SecureWay Policy Director Versão 3.0* na unidade de CD-ROM.
3. Altere para o diretório \win32\server no CD.
4. Clique no arquivo Setup.exe e o programa InstallShield é iniciado.
5. Quando a janela Escolher Idioma de Instalação for exibida, selecione o idioma apropriado.
6. Clique em **Avançar** e a janela Bem-Vindo do Policy Director é exibida.
7. Clique em **Avançar**.

   A janela Escolher Localização de Destino é exibida.
8. Aceite a localização de diretório padrão para os arquivos do programa ou clique no botão **Procurar** para criar ou selecionar outro diretório.

   A localização padrão é: `C:\Arquivos de Programas\IBM\`

   Se você instalou o NetSEAT em uma localização não-padrão, instale os servidores do Policy Director na mesma localização.
9. Clique em **Avançar**.

   A janela Selecionar Componentes é exibida.
10. Selecione os componentes de servidor Policy Director apropriados. Para obter assistência para a seleção, consulte “Configurações comuns” na página 15.

    Deve haver pelo menos uma instância do servidor de Gerenciamento do Policy Director (IVMgr) no domínio seguro.
11. Clique em **Avançar**.
12. Se você não selecionou o WebSEAL, vá para 14.

    Se você selecionou o componente WebSEAL (IVWeb), a janela Escolher Localização da Raiz de Documento da Web é exibida. Esta janela solicita que você informe a localização do diretório raiz de seu espaço da Web. Todos os recursos pertencentes ao seu site da Web residem neste diretório.
13. Aceite a localização do diretório raiz padrão ou clique no botão **Procurar** para criar ou selecionar outro diretório. A localização padrão é:

    `C:\...\IBM\Policy Director\www\docs`

    Os arquivos do Policy Director são copiados do CD para sua unidade de disco rígido. A janela Início de Sessão do Administrador do domínio seguro é exibida. Esta etapa é necessária para estabelecer credenciais de segurança e concluir o processo de configuração.
14. Preencha o nome e a senha do Administrador de Células do DCE.
15. Se você selecionou o componente do servidor de Gerenciamento (IVMgr), é solicitado que você selecione **Registro LDAP** ou **Registro DCE**.

Se você não selecionou o servidor de Gerenciamento, o tipo de Registro do Usuário para o domínio seguro existente é detectado automaticamente:

Se um registro de usuário LDAP for detectado, a instalação continua conforme descrição em “Utilização de um registro de usuário LDAP”.

Se um registro de usuário DCE for detectado, a instalação continua conforme descrição em “Utilização de um registro de usuário DCE” na página 41.

16. Clique em um dos seguintes para seu registro de usuário:

    Se você selecionou **Registro de Usuário LDAP**, vá para “Utilização de um registro de usuário LDAP”.

    Se você selecionou **Registro de Usuário DCE**, vá para “Utilização de um registro de usuário DCE” na página 41.

Utilização de um registro de usuário LDAP

Se seu domínio seguro do Policy Director utiliza um registro de usuário LDAP ou se você estiver instalando o IVMgr e tiver selecionado **Registro LDAP**, a janela Informações sobre o servidor LDAP é exibida.

1. Digite as informações necessárias para a configuração do servidor LDAP:

   Nome do Host LDAP

   Número da Porta

   Número da Porta SSL (requerido apenas se o SSL for utilizado para acessar o servidor LDAP)

   DN do LDAP para banco de dados GSO (por exemplo, o=ibm,c=br)

2. Clique em **Avançar**.

   A janela Comunicação com o Servidor LDAP é exibida.

3. Escolha ativar ou inativar a comunicação SSL entre o Policy Director e o servidor LDAP. Clique em **Sim** para ativar a comunicação SSL ou clique em **Não** para inativar a comunicação SSL.

   No Windows NT, a comunicação SSL é ativada uma vez entre todos os servidores Policy Director no sistema host e o servidor LDAP.

   Se você tiver ativado a comunicação SSL, vá para a etapa 4.

   Se você tiver inativado a comunicação, vá para a etapa 5.

4. Forneça os valores para os seguintes prompts:

   Localização do Arquivo de Chaves SSL

   DN do Arquivo SSL (rótulo de chave)

   Senha do Arquivo de Chaves SSL

   Consulte “Criação do arquivo de banco de dados de chaves e do certificado” na página 27 para obter informações.

5. Clique em **Avançar**.

   A janela Início de Sessão do Administrador LDAP é exibida.

6. Preencha as informações de nome do Administrador (por exemplo, cn=root) e senha e clique em **OK**.

   Os servidores são configurados e inicializados. Isto pode levar vários minutos. A janela Informações sobre o Sistema aparece e exibe o status dos servidores, inclusive informações de registro.

7. Clique em **Avançar**.

   A janela Configuração do Policy Director Concluída é exibida.
8. Clique em **Sim** para reiniciar.

   Se você marcou **Não** na opção de reinício, você deve reiniciar o Windows NT mais tarde para concluir o processo de configuração. Isto conclui a instalação do Policy Director.
9. Clique em **Concluir**.

   É solicitado que você reinicie seu sistema.

Utilização de um registro de usuário DCE

Se seu domínio seguro do Policy Director utiliza um registro de usuário DCE ou se você estiver instalando o IVMgr e tiver selecionado **Registro de Usuário DCE**, a instalação continua da seguinte maneira:

1. Se você selecionou o componente WebSEAL (IVWeb), a janela Escolher Localização da Raiz de Documento da Web é exibida. Esta janela solicita que você informe a localização do diretório raiz de seu espaço na Web. Todos os recursos pertencentes ao seu site da Web residem neste diretório.

   Se você não selecionou o WebSEAL, vá para 3.
2. Aceite a localização do diretório raiz padrão ou clique no botão **Procurar** para criar ou selecionar outro diretório. A localização padrão é:

   ```
   C:\Arquivos de Programas\IBM\Policy Director\www\docs
   ```
3. Clique em **Avançar**.

   Os arquivos do Policy Director são copiados do CD para sua unidade de disco rígido. A janela Início de Sessão do Administrador do domínio seguro é exibida.
4. Preencha as informações de nome e senha do Administrador LDAP e, em seguida, clique em **OK**.

   Os servidores são configurados e inicializados. Isto pode levar vários minutos. A janela Informações sobre o Sistema aparece e exibe o status dos servidores, inclusive informações de registro.
5. Clique em **Avançar**.

   A janela Configuração do Policy Director Concluída é exibida.
6. Clique em **Concluir**.

   É solicitado que você reinicie seu sistema.
7. Clique em **Sim** para reiniciar.

   Se você marcou **Não** na opção de reinício, você deve reiniciar o Windows NT mais tarde para concluir o processo de configuração. Isto conclui a instalação do Policy Director.

Configuração do Credentials Acquisition Service

O CAS do Policy Director é instalado automaticamente. Se desejar utilizar o CAS para seu serviço de aquisição de credenciais, você deve configurá-lo. Consulte as informações sobre configuração de um serviço de aquisição de credenciais no *Policy Director Administration Guide* para obter instruções.

Utilização do NetSEAL Trap no Windows NT

O NetSEAL do Policy Director (IVTrap) faz trap em pedidos feitos a portas específicas. Para utilizar o trap do NetSEAL, é necessário parar e reiniciar todos os aplicativos que utilizam portas específicas.

Para obter mais informações sobre a configuração do NetSEAL do Policy Director para fazer trap em portas específicas, consulte as informações da visão geral sobre o NetSEAL no *Policy Director Administration Guide*.

Instalação do Console de Gerenciamento no Windows

O Policy Director fornece um Console de Gerenciamento que gerencia muitos componentes do sistema de segurança do Policy Director a partir de um desktop do Windows. O Console de Gerenciamento pode ser instalado em qualquer um dos seguintes sistemas operacionais:

Windows 95

Windows 98

Windows NT Versão 4.0, com Service Pack 4 ou superior

Cada sistema operacional Windows que executa o Policy Director requer o cliente NetSEAT do Policy Director.

O cliente NetSEAT pode ser configurado como um cliente de tempo de execução DCE ou como um cliente para um servidor Policy Director. Embora as duas configurações sejam aceitas para o Console de Gerenciamento, os servidores Policy Director requerem o cliente completo para o servidor Policy Director.

Se for necessário reinstalar qualquer um dos componentes, você deve remover o componente existente antes de reinstalá-lo.

Instalação do Console de Gerenciamento com componentes do servidor

Depois que os componentes de servidor do Policy Director tiverem sido instalados e configurados, “Instalação dos servidores Policy Director” na página 39, conclua as etapas a seguir:

1. Insira o CD do *IBM SecureWay Policy Director Versão 3.0* na unidade de CD-ROM.
2. Altere para o diretório \win32\Console.
3. Dê um clique duplo no arquivo Setup.exe e o programa InstallShield é iniciado.
4. Quando a janela Escolher Idioma de Instalação for exibida, selecione o idioma apropriado.
5. Clique em **Avançar** e a janela Bem-Vindo do Policy Director é exibida.
6. Clique em **Avançar** e a janela Escolher Localização de Destino é exibida.
7. Indique a localização em que deseja que os arquivos sejam instalados.

   Os arquivos são copiados em suas localizações apropriadas no computador do Windows. Uma janela de informações é exibida, indicando que a instalação foi bem-sucedida.
8. Se for questionado se você deseja reiniciar o Windows, clique em **sim**.
9. Clique em **OK**.

10. Vá para “Início do Console de Gerenciamento” na página 43.

Instalação do Console de Gerenciamento sem componentes do servidor

Para ativar a administração de segurança do Policy Director a partir de sistemas Windows adicionais, você pode instalar o Console de Gerenciamento em sistemas Windows que não tenham os componentes do servidor Policy Director instalados. Quando você instala o Console de Gerenciamento desta forma, o cliente NetSEAT pode ser configurado como um cliente de tempo de execução DCE ou como um cliente para um servidor Policy Director.

Para instalar o Console de Gerenciamento sem os componentes do servidor, vá para o sistema desktop do Windows e conclua as seguintes etapas:

1. Verifique se o sistema operacional Windows é uma plataforma suportada. Consulte “Servidores do Policy Director” na página 12.
2. Instale o cliente NetSEAT do Policy Director. Siga as instruções em “Instalação do NetSEAT” na página 35.
3. Verifique se o cliente NetSEAT está configurado apropriadamente no domínio seguro em que você irá executar o Console de Gerenciamento. Consulte “Verificação da configuração do cliente NetSEAT” na página 38.
4. Insira o *IBM SecureWay Policy Director Versão 3.0* CD na unidade de CD-ROM.
5. Altere para o diretório \win32\Console.
6. Dê um clique duplo no arquivo Setup.exe e o programa InstallShield é iniciado.
7. Quando a janela Escolher Idioma de Instalação for exibida, selecione o idioma apropriado.
8. Clique em **Avançar** e a janela Bem-Vindo do Policy Director é exibida.
9. Clique em **Avançar** e a janela Escolher Localização de Destino é exibida.
10. Indique a localização em que deseja que os arquivos sejam instalados.

    Os arquivos são copiados em suas localizações apropriadas no computador do Windows. Uma janela de informações é exibida, indicando que a instalação foi bem-sucedida.
11. Clique em **OK** para concluir a instalação
12. Para iniciar o Console de Gerenciamento, vá para “Início do Console de Gerenciamento”.

Início do Console de Gerenciamento

Para iniciar o Console de Gerenciamento:

1. Certifique-se de que os servidores Policy Director estejam instalados e em execução.
2. Clique em **Iniciar → Programas → Policy Director → Console de Gerenciamento.**

   A janela Console de Gerenciamento do Policy Director é exibida.
3. Inicie sessão no Console de Gerenciamento como um usuário com privilégios de administrador, como cell_admin.

Remoção do Policy Director

Para remover os componentes do Policy Director certifique-se de iniciar sessão como administrador. Inicie sessão no domínio do Windows como um usuário com credenciais de administrador. Por exemplo:

```
dce_login cell_admin password
```

Se você tentar remover um componente sem as credenciais de domínio seguro apropriadas, uma janela de Falha na Autorização é exibida.

Você deve remover os componentes do Policy Director na ordem exatamente inversa da instalação. Utilize o ícone **Adicionar/Remover Programas** no Painel de Controle para remover o Policy Director.

Para remover uma instalação completa do Policy Director, execute os seguintes procedimentos na ordem mostrada:

1. Remova o Console de Gerenciamento.
2. Remova os componentes do servidor.
3. Remova o cliente NetSEAT.

Remoção do Console de Gerenciamento

Para remover o Console de Gerenciamento:

1. Se o Console de Gerenciamento estiver em execução, feche-o.
2. Vá para **Adicionar/Remover Programas** no Painel de Controle e clique em **Console de Gerenciamento do Policy Director.**
3. Clique no botão **Adicionar/Remover**.
4. Quando questionado, clique **sim** para confirmar se você deseja remover o programa.
5. Clique em **OK**.

Remoção dos componentes do servidor

Para remover os componentes do servidor do Policy Director, você deve primeiro obter privilégios e credenciais e, em seguida, remover os componentes.

Para remover componentes do servidor:

1. Certifique-se de que os servidores Policy Director estejam instalados e em execução.
2. Vá para **Adicionar/Remover Programas** no Painel de Controle e, em seguida, selecione o primeiro componente do servidor Policy Director que deseja remover.
3. Remova os componentes do servidor Policy Director na ordem exatamente inversa em que foram instalados.

   Por exemplo, se você desejar instalar todos os componentes, remova-os na seguinte ordem:

   ADK de Autorização (IVAuthADK)

   Servidor de Autorização (IVAcld)

   NetSEAL (IVTrap).

   WebSEAL (IVWeb).

   Gerenciador de Segurança (IVNet).

Servidor de Gerenciamento (IVMgr).

Base (IVBase). Este componente é sempre instalado automaticamente.

O Console de Gerenciamento do Policy Director pode ser removido a qualquer momento. Para obter mais informações sobre a ordem na qual os componentes são instalados, consulte “Visão geral da instalação do Policy Director etapa por etapa” na página 20.

4. Clique no botão **Adicionar/Remover**.
5. Digite o nome e a senha do usuário do Administrador do LDAP quando solicitados.
6. Repita a etapa 2 na página 44 até a etapa 5 para cada componente do servidor Policy Director.
7. Clique em **OK** quando concluir.

Remoção do cliente NetSEAT

Você deve possuir privilégios de administrador do Windows NT para remover os componentes NetSEAT do Policy Director.

1. Vá para **Adicionar/Remover Programas** no Painel de Controle e, em seguida, clique na guia **Instalar/Desinstalar**.
2. Na janela de listagem da guia, clique em **Cliente NetSEAT do Policy Director**.
3. Clique em **Adicionar/Remover**.
4. Clique em **OK**.

Capítulo 6. Instalação do Policy Director para AIX

As seções deste capítulo descrevem como instalar e configurar o Policy Director no ambiente operacional AIX.

Antes de começar a instalação do Policy Director, certifique-se de ter revisto as informações em "Antes de instalar o Policy Director para AIX".

Antes de instalar o Policy Director para AIX

Antes de iniciar a instalação do NetSEAT e do Policy Director, leia as informações a seguir:

Se você estiver criando uma nova célula DCE ao instalar os servidores Policy Director:

— Você deve também instalar e configurar um servidor DCE.

— Se você estiver utilizando LDAP para seu registro de usuário, é necessário também instalar e configurar um servidor LDAP.

Familiarize-se com todas as informações relativas à implementação do Policy Director, conforme descrito em "Requisitos de instalação para o domínio seguro" na página 18.

Instalação do Console de Gerenciamento

O Policy Director fornece um Console de Gerenciamento que pode ser utilizado para gerenciar todos os componentes do sistema Policy Director. Os administradores podem escolher instalar o Console de Gerenciamento em um sistema AIX, em um sistema Windows ou em ambos.

O Console de Gerenciamento para AIX é distribuído como um pacote denominado IV.Console. Utilize o SMIT para instalar e configurar o pacote.

Instalação do Policy Director

Para instalar o Policy Director no AIX, utilize as seguintes instruções:

1. Certifique-se de que o servidor LDAP esteja instalado e em execução se você for utilizar LDAP como o registro de usuário. Consulte Capítulo 4, "Instalação e configuração do IBM SecureWay Directory" na página 23 para obter instruções completas
2. Inicie sessão como root.
3. Insira o CD do *IBM SecureWay Policy Director Versão 3.0* na unidade de CD-ROM.
4. Inicie o SMIT.
5. Clique em **Instalação e Manutenção de Software**.

   O menu Instalação e Manutenção de Software é exibido.
6. Clique em **Instalar e Atualizar Software**.

   O menu Instalar e Atualizar Software é exibido.
7. Clique em **Instalar e Atualizar Software por Nome de Pacote**.

A janela Instalar e Atualizar Software por Nome de Pacote é exibida.

8. Digite o nome do dispositivo a partir do qual você está instalando o software.

   Por exemplo:

   Se estiver instalando a partir de uma unidade de CD, você deve digitar: `/dev/cd`

   Se estiver instalando de um diretório em um servidor montado, você deve digitar: `/mnt/user/lpp/IV`

   Depois de digitar o nome do dispositivo, uma janela de Listagem de multi-seleção é exibida.

9. Clique em **IV**.

   Uma janela de Listagem de multi-seleção exibe a lista de pacotes do software Policy Director.

10. Selecione os pacotes que deseja instalar.

    Para instalar todos os pacotes do Policy Director, clique na entrada **IV**.

    Ao instalar apenas alguns dos pacotes do Policy Director, certifique-se de observar as dependências de instalação descritas em “Requisitos de instalação para o domínio seguro” na página 18.

11. Clique em **OK**.

    O menu do SMIT Instalar e Atualizar Software por Nome de Pacote é exibido.

12. Clique em **sim** no campo rotulado:

    `Instalar AUTOMATICAMENTE software de requisito?`

    Esta etapa assegura que os pacotes do Policy Director base (IV.Base) e da configuração do SMIT (IV.smit) são instalados. Estes pacotes são software de pré-requisito para os outros pacotes do Policy Director. Se você optar por definir este campo como **não**, retorne para o menu de seleção do pacote. Certifique-se de ter selecionado IV.Base e IV.Smit.

13. Defina outros campos com valores apropriados à sua instalação.
14. Clique em **OK**.

    O SMIT exibe mensagens de status, incluindo:

    Verificação da pré-instalação dos pacotes do software Policy Director.

    Nome de cada pacote durante a extração dos arquivos do pacote.

    Criação de menus de configuração para cada pacote.

    Uma mensagem de status que indica o êxito ou a conclusão da extração do arquivo.

15. Quando a extração dos arquivos for concluída, configure os pacotes do Policy Director, utilizando as informações em “Configuração do Policy Director com um registro de usuário LDAP”. Ou, se estiver utilizando o registro DCE, consulte a seção “Configuração do Policy Director com um registro de usuário DCE” na página 54.

Configuração do Policy Director com um registro de usuário LDAP

Você deve instalar os pacotes do software Policy Director antes de poder configurá-los. Se ainda não tiver instalado os pacotes do Policy Director, consulte “Instalação do Policy Director” na página 47.

Se você tiver instalado o Policy Director com um registro de usuário DCE, vá para "Configuração do Policy Director com um registro de usuário DCE" na página 54.

Você deve configurar cada pacote instalado do Policy Director, com exceção da Configuração do SMIT. Configure um pacote por vez. Alguns dos pacotes do Policy Director requerem que o administrador responda a prompts na tela durante a configuração.

Para configurar os pacotes do Policy Director:

1. Inicie o SMIT.

   O menu Gerenciamento do Sistema é exibido.
2. Clique em **Aplicativos de Comunicação e Serviços**.

   Uma lista dos pacotes de software instalados é exibida. Por exemplo:

   TCP/IP

   NFS

   DCE (Distributed Computing Environment)

   Policy Director
3. Clique em **Policy Director**.

   O menu Policy Director é exibido com as seguintes opções:

   Configuração do Policy Director

   Remoção da Configuração do Policy Director
4. Clique em **Configuração do Policy Director**.

   Uma lista dos pacotes instalados do Policy Director é exibida, como:

   Configuração do Policy Director Base

   Configuração do Servidor de Gerenciamento do Policy Director

   Configuração do Console de Gerenciamento do Policy Director

   Configuração do Gerenciador de Segurança do Policy Director

   Configuração do WebSEAL do Policy Director

   Configuração do Servidor de Autorização do Policy Director

   Configuração do NetSEAL do Policy Director

   Configuração do ADK de Autorização do Policy Director
5. Clique em cada pacote para configurar, um de cada vez.

   Você deve configurar os pacotes do Policy Director na ordem em que eles aparecem na lista de configuração do Policy Director. Selecione cada pacote por vez, do primeiro item da lista ao último.

É necessário agora configurar os pacotes do Policy Director selecionados, utilizando as instruções de configuração apropriadas nas seções a seguir.

Configuração do pacote Base

O pacote Base é instalado em um computador sempre que você instala qualquer um dos outros pacotes. Para configurar o pacote Base, clique em **Policy Director Base** na lista de configurações do Policy Director.

A configuração do pacote Base do Policy Director é concluída sem qualquer entrada do usuário.

Configuração do servidor de Gerenciamento

Para configurar o servidor de Gerenciamento:

1. Clique em **Servidor de Gerenciamento do Policy Director** na lista de configurações do Policy Director.

   Aparece um prompt solicitando que você escolha um tipo de registro de usuário.

2. Se você estiver utilizando LDAP como seu registro de usuário, digite `2` para registro de usuário LDAP.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

3. Quando solicitado, digite o nome e a senha da conta do Administrador de Células do DCE.

   Se você estiver utilizando LDAP como seu registro de usuário, uma série de prompts aparece para configurar a comunicação entre o servidor de Gerenciamento e o servidor LDAP.

4. Digite as informações requeridas para a configuração do servidor LDAP:

   Nome do host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP (opcional)

5. Digite o nome do usuário e a senha do usuário administrativo LDAP (por exemplo, `cn=root`). As informações de segurança do Policy Director agora estão registradas com o servidor LDAP.

6. Escolha ativar ou inativar a comunicação SSL entre o servidor de Gerenciamento e o servidor LDAP.

   Nota: Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o servidor de Gerenciamento (IVMgr) e o servidor LDAP.

7. Se você tiver inativado a comunicação SSL, vá para a etapa 8. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

   Localização do Arquivo de Conjuntos de Chaves SSL

   Rótulo de Chave SSL

   Senha da Chave do SSL

8. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

   Por exemplo:

   ```
   o=IBM,c=BR
   ```

   Depois que o acesso ao banco de dados GSO é configurado, o Gerenciador de Configuração do Policy Director configura um Directory Services Broker automaticamente. Uma série de mensagens lista cada etapa automatizada conforme ela é concluída.

   Aparece uma mensagem indicando que a instalação do pacote IVMgr foi bem-sucedida.

   A lista de pacotes disponíveis é exibida novamente.

Configuração e início do Console de Gerenciamento

Para configurar o Console de Gerenciamento, clique em **Policy Director Console de Gerenciamento** na lista de configurações do Policy Director.

A configuração do Console de Gerenciamento do Policy Director é concluída sem qualquer entrada do usuário.

Para iniciar a versão do AIX do Console de Gerenciamento:

1. Certifique-se de que os servidores Policy Director estejam instalados e em execução.
2. Digite o seguinte comando:

```
$ /opt/intraverse/bin/ivconsole
```

Ou, se você estiver utilizando a versão do cliente Windows do Console de Gerenciamento, siga as instruções em “Início do Console de Gerenciamento” na página 43.

Configuração do Gerenciador de Segurança

Para configurar o Gerenciador de Segurança (IVNet):

1. Clique em **Servidor de Segurança do Policy Director** na lista de configurações do Policy Director.

   Uma série de prompts aparecem para integrar o Gerenciador de Segurança com o servidor LDAP.
2. Se solicitado, digite as informações requeridas para a configuração do servidor LDAP:

   Nome de host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP (opcional)

   Estes prompts não aparecem se o servidor de Gerenciamento do Policy Director ou o servidor de Autorização foram configurados anteriormente.
3. Digite o nome do usuário e a senha do usuário administrativo LDAP. As informações de segurança do Policy Director agora estão registradas com o servidor LDAP.
4. Escolha ativar ou inativar a comunicação SSL entre o Gerenciador de Segurança e o servidor LDAP.

   Nota: Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor Policy Director e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o Gerenciador de Segurança (IVNet, para utilização pelo WebSEAL e o NetSEAL) e o servidor LDAP.

5. Se você tiver inativado a comunicação SSL, vá para a etapa 6. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

   Localização do Arquivo de Conjuntos de chaves SSL

   Rótulo de Chave SSL

   Senha da Chave do SSL
6. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

Por exemplo:

```
o=IBM,c=BR
```

Este prompt não aparece se o servidor de Gerenciamento do Policy Director ou o servidor de Autorização foram configurados anteriormente.

Aparece um prompt solicitando o nome e a senha da Administração de Células do DCE.

7. Quando solicitado, digite o nome e a senha da conta do Administrador de Células do DCE.

   O Gerenciador de Segurança é configurado e iniciado. O servidor CAS também é iniciado.

   Aparece uma mensagem indicando que a instalação do pacote do Gerenciador de Segurança foi bem-sucedida.

Configuração do WebSEAL do Policy Director

Para configurar o WebSEAL do Policy Director (IVWeb):

1. Clique em **WebSEAL do Policy Director** na lista de configurações do Policy Director.

   O menu de configuração do WebSEAL do Policy Director é exibido com valores que confirmam o seguinte:

   Acesso de cliente HTTP e HTTPS

   Portas requeridas do TCP (Transmission Control Protocol)

   O diretório raiz do documento da Web padrão

2. Confirme os valores de configuração atuais:

```
Verifique a configuração do Servidor da Web:
1. Ativar TCP HTTP?               Sim
2. Porta HTTP                    8
3. Ativar HTTPS?                  Sim
4. Porta HTTPS                   443
5. Diretório raiz do doc. da Web     /opt/Policy Director/www/docs
a. Aceitar a configuração e continuar com a instalação
x. Sair da instalação

Selecione o item a ser alterado: a
```

3. Digite a para aceitar a configuração e continuar a instalação ou digite o número de um valor a ser alterado.

   A configuração do Gerenciador de Segurança do Policy Director solicita o nome e a senha do Administrador de Células do DCE.

4. Digite o nome e a senha da conta do Administrador de células do DCE.

   O Gerenciador de Segurança do Policy Director é reiniciado.

   A instalação configura e ativa o WebSEAL do Policy Director no computador.

Configuração do servidor de Autorização do Policy Director

Para configurar o servidor de Autorização do Policy Director (IVAcld):

1. Clique em **Servidor de Autorização do Policy Director** na lista de configurações do Policy Director.

Aparecem um ou mais prompts para integrar o servidor de Autorização do Policy Director com o servidor LDAP.

2. Se solicitado, digite as informações requeridas para a configuração do servidor LDAP:

   Nome de host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP (opcional)

   Estes prompts não aparecem se o servidor de Gerenciamento do Policy Director ou o servidor de Autorização foram configurados anteriormente.
3. Digite o nome do usuário e a senha do usuário administrativo LDAP. As informações de segurança do Policy Director agora estão registradas com o servidor LDAP.
4. Escolha ativar ou inativar a comunicação SSL entre o Gerenciador de Segurança e o servidor LDAP.

   Nota: Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor Policy Director e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o servidor de Autorização (IVAcld) e o servidor LDAP.

5. Se você tiver inativado a comunicação SSL, vá para a etapa 6. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

   Localização do Arquivo de Conjuntos de chaves SSL

   Rótulo de Chave SSL

   Senha da Chave do SSL
6. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

   Por exemplo:

   ```
   o=IBM,c=BR
   ```

   Este prompt não aparece se o servidor de Gerenciamento do Policy Director ou o servidor de Autorização foram configurados anteriormente.

   Aparece um prompt solicitando o nome e a senha da Administração de Células do DCE.
7. Quando solicitado, digite o nome e a senha da conta do Administrador de Células do DCE.

   O servidor de Autorização é configurado e iniciado.

   Aparece uma mensagem indicando que a instalação do pacote do servidor de Autorização foi bem-sucedida.

Configuração do NetSEAL do Policy Director

Para configurar o NetSEAL do Policy Director:

1. Clique em **NetSEAL do Policy Director** na lista de configurações do Policy Director.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

2. Digite o nome do usuário e a senha do usuário administrativo LDAP. As informações de segurança do Policy Director agora estão registradas com o servidor LDAP.

   A configuração do pacote NetSEAL do Policy Director é concluída.

O NetSEAL do Policy Director faz trap em pedidos feitos a portas específicas. Para utilizar o trap do NetSEAL, é necessário parar e reiniciar todos os aplicativos que utilizam portas específicas. Para obter mais informações sobre a utilização do NetSEAL do Policy Director, consulte “Utilização do NetSEAL Trap no AIX” na página 58.

Configuração do ADK de Autorização do Policy Director

Para configurar o ADK de Autorização do Policy Director, clique em **ADK de Autorização do Policy Director** na lista de configurações do Policy Director.

A configuração do pacote de Autorização do Policy Director é concluída sem qualquer entrada do usuário.

Configuração do Credentials Acquisition Service do Policy Director

O CAS do Policy Director é instalado automaticamente. Se desejar utilizar o CAS do Policy Director para seu serviço de aquisição de credenciais, você deve configurá-lo. Consulte informações sobre o CAS do Policy Director e sobre como configurá-lo no *Policy Director Administration Guide*.

Configuração do Policy Director com um registro de usuário DCE

Você deve instalar os pacotes do software Policy Director antes de poder configurá-los. Se ainda não tiver instalado os pacotes do Policy Director, primeiro consulte “Instalação do Policy Director” na página 47.

Se você tiver instalado o Policy Director com um registro de usuário LDAP, vá para “Configuração do Policy Director com um registro de usuário LDAP” na página 48.

Você deve configurar cada pacote instalado do Policy Director, com exceção da Configuração do SMIT. Configure um pacote por vez. Alguns dos pacotes do Policy Director requerem que o administrador responda a prompts na tela durante a configuração.

Para configurar os pacotes do Policy Director:

1. Inicie o SMIT.

   O menu Gerenciamento do Sistema é exibido.
2. Clique em **Aplicativos de Comunicação e Serviços**.

   Uma lista dos pacotes de software instalados é exibida. Por exemplo:

   TCP/IP

   NFS

   DCE (Distributed Computing Environment)

   Policy Director
3. Clique em **Policy Director**.

O menu Policy Director é exibido com as seguintes opções:

Configuração do Policy Director

Remoção da Configuração do Policy Director

4. Clique em **Configuração do Policy Director**.

   Uma lista dos pacotes instalados do Policy Director é exibida, como:

   Configuração do Policy Director Base

   Configuração do Servidor de Gerenciamento do Policy Director

   Configuração do Console de Gerenciamento do Policy Director

   Configuração do Gerenciador de Segurança do Policy Director

   Configuração do WebSEAL do Policy Director

   Configuração do Servidor de Autorização do Policy Director

   Configuração do NetSEAL do Policy Director

   Configuração do ADK de Autorização do Policy Director

5. Clique em cada pacote para configurar, um de cada vez.

   Você deve configurar os pacotes do Policy Director na ordem em que eles aparecem na lista de configuração do Policy Director. Selecione cada pacote por vez, do primeiro item da lista ao último.

É necessário agora configurar os pacotes do Policy Director selecionados, utilizando as instruções de configuração apropriadas nas seções a seguir.

Configuração do pacote Base

O pacote Base é instalado em um computador sempre que você instala qualquer um dos outros pacotes. Para configurar o pacote Base, clique em **Policy Director Base** na lista de configurações do Policy Director.

A configuração do pacote Base do Policy Director é concluída sem qualquer entrada do usuário.

Configuração do servidor de Gerenciamento

Para configurar o servidor de Gerenciamento:

1. Clique em **Servidor de Gerenciamento do Policy Director** na lista de configurações do Policy Director.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

2. Quando solicitado, digite o nome e a senha da conta do Administrador de Células do DCE.

   A instalação configura e inicia o servidor de Gerenciamento.

Configuração e início do Console de Gerenciamento

Para configurar o Console de Gerenciamento, clique em **Policy Director Console de Gerenciamento** na lista de configurações do Policy Director.

A configuração do Console de Gerenciamento do Policy Director é concluída sem qualquer entrada do usuário.

Para iniciar a versão do AIX do Console de Gerenciamento:

1. Certifique-se de que os servidores Policy Director estejam instalados e em execução.
2. Digite o seguinte comando:

```
$ /opt/intraverse/bin/ivconsole
```

Configuração do Gerenciador de Segurança

Para configurar o Gerenciador de Segurança (IVNet):

1. Clique em **Servidor de Segurança do Policy Director** na lista de configurações do Policy Director.
2. Quando solicitado, digite o nome e a senha da conta do Administrador de Células do DCE.

A instalação configura e inicia o servidor de Gerenciamento.

Configuração do WebSEAL do Policy Director

Para configurar o WebSEAL do Policy Director (IVWeb):

1. Clique em **WebSEAL do Policy Director** na lista de configurações do Policy Director.

   O menu de configuração do WebSEAL do Policy Director é exibido com valores que confirmam o seguinte:

   Acesso de cliente HTTP e HTTPS

   Portas requeridas do TCP (Transmission Control Protocol)

   O diretório raiz do documento da Web padrão
2. Confirme os valores de configuração atuais:

```
Verifique a configuração do Servidor da Web:
1. Ativar TCP HTTP?               Sim
2. Porta HTTP                    8
3. Ativar HTTPS?                  Sim
4. Porta HTTPS                   443
5. Diretório raiz do doc. da Web     /opt/Policy Director/www/docs
a. Aceitar a configuração e continuar com a instalação
x. Sair da instalação

Selecione o item a ser alterado: a
```

3. Digite a para aceitar a configuração e continuar a instalação ou digite o número de um valor a ser alterado.

   A configuração do Gerenciador de Segurança do Policy Director solicita o nome e a senha do Administrador de Células do DCE.
4. Digite o nome e a senha da conta do Administrador de células do DCE.

   O Gerenciador de Segurança do Policy Director é reiniciado.

   A instalação configura e ativa o WebSEAL do Policy Director no computador.

Configuração do servidor de Autorização do Policy Director

Para configurar o servidor de Autorização do Policy Director (IVAcld):

1. Clique em **Servidor de Autorização do Policy Director** na lista de configurações do Policy Director.

Aparece um prompt solicitando o nome e a senha da Administração de Células do DCE.

2. Digite o nome e a senha da conta do Administrador de células do DCE.

   O servidor de Autorização é configurado e iniciado.

Configuração do NetSEAL do Policy Director

Para configurar o NetSEAL do Policy Director:

1. Clique em **NetSEAL do Policy Director** na lista de configurações do Policy Director.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

2. Digite o nome do usuário e a senha do usuário administrativo LDAP. As informações de segurança do Policy Director agora estão registradas com o servidor LDAP.

   A configuração do NetSEAL do Policy Director é concluída.

O NetSEAL do Policy Director faz trap em pedidos feitos a portas específicas. Para utilizar o trap do NetSEAL, é necessário parar e reiniciar todos os aplicativos que utilizam portas específicas. Para obter mais informações sobre a utilização do NetSEAL do Policy Director, consulte “Utilização do NetSEAL Trap no AIX” na página 58.

Configuração do ADK de Autorização do Policy Director

Para configurar o ADK de Autorização do Policy Director, clique em **ADK de Autorização do Policy Director** na lista de configurações do Policy Director.

A configuração do pacote de Autorização do Policy Director é concluída sem qualquer entrada do usuário.

Configuração do Credentials Acquisition Service do Policy Director

O CAS do Policy Director é instalado automaticamente. Se desejar utilizar o CAS do Policy Director para seu serviço de aquisição de credenciais, você deve configurá-lo. Consulte informações sobre o CAS do Policy Director e sobre como configurá-lo no *Policy Director Administration Guide*.

Instalação do Console de Gerenciamento

O Policy Director fornece um Console de Gerenciamento que gerencia muitos componentes do sistema de segurança do Policy Director a partir de um desktop do Windows. O Console de Gerenciamento pode ser instalada em qualquer um dos seguintes sistemas operacionais:

Windows 95

Windows 98

Windows NT Versão 4.0, com Service Pack 4 ou superior

AIX Versão 4.3.1.0 ou superior

Cada sistema operacional Windows que executa o Policy Director requer o cliente NetSEAT do Policy Director.

O cliente NetSEAT pode ser configurado como um cliente de tempo de execução DCE ou como um cliente para um servidor Policy Director. Embora as duas configurações sejam aceitas para o Console de Gerenciamento, os servidores Policy Director requerem o cliente completo para o servidor Policy Director.

Se for necessário reinstalar qualquer um dos componentes, você deve remover o componente existente antes de reinstalá-lo.

Utilização do NetSEAL Trap no AIX

Para utilizar o trap NetSEAL do Policy Director, o daemon do NetSEAL Gerenciador de Segurança (secmgrd) deve ser iniciado antes de qualquer aplicativo que acesse portas protegidas (com trap). Utilize entradas /etc/inittab para assegurar que o secmgrd é iniciado antes dos aplicativos durante o processo de inicialização.

Utilize o trap do NetSEAL com aplicativos de rede, como o Telnet, RLOGIN e POP3. O daemon **inetd** controla estes aplicativos. O script de inicialização do Policy Director, /etc/iv/iv, inicia o secmgrd e, em seguida, para e reinicia o daemon inetd. Este procedimento assegura a execução de trap destes aplicativos depois da inicialização do sistema.

Se você parar e reiniciar o Policy Director, você deve também parar e reiniciar quaisquer aplicativos que fazem pedidos a portas com trap. Para automatizar este processo, você pode adicionar código ao /etc/iv/iv para parar e iniciar os aplicativos depois que o secmgrd é iniciado. Utilize a técnica de script /etc/iv/iv para parar e reiniciar o **inetd** como um gabarito sobre como parar e iniciar outros aplicativos.

Para obter mais informações sobre a configuração do NetSEAL do Policy Director para fazer trap em portas específicas, consulte as informações sobre o NetSEAL no *Policy Director Administration Guide*.

Remoção do Policy Director

Você deve remover a configuração do Policy Director para AIX antes de poder removê-lo.

Para obter informações sobre como remover a configuração do Policy Director, consulte “Remoção da configuração de pacotes do Policy Director”.

Para obter informações sobre a remoção do Policy Director, consulte “Remoção de pacotes do Policy Director” na página 59.

Para remover a versão do Windows do Console de Gerenciamento, consulte

Remoção da configuração de pacotes do Policy Director

Para remover a configuração de servidores do Policy Director, conclua as seguintes etapas:

1. Inicie o SMIT.
2. Clique em **Aplicativos de Comunicação e Serviços**.

   O menu Aplicativos de Comunicação e Serviços é exibido.

3. Clique em **Policy Director**.

   O menu Policy Director é exibido.
4. No menu, clique em **Remoção da configuração do Policy Director**.

   A lista de pacotes configurados do Policy Director é exibida.

   Selecione o pacote cuja configuração deve ser removida. Os pacotes que devem ser mostrados são:

   Remoção do Configuração do Servidor de Autorização do Policy Director

   Remoção da Configuração do ADK de Autorização do Policy Director

   Remoção da Configuração do NetSEAL do Policy Director

   Remoção da Configuração do WebSEAL do Policy Director

   Remoção da Configuração do Gerenciador de Segurança do Policy Director

   Remoção da Configuração do Servidor de Gerenciamento do Policy Director

   Remoção da Configuração do Console de Gerenciamento do Policy Director

   Remoção da Configuração do Policy Director Base

   Remoção da Configuração do menu IV Smit
5. A remoção da configuração dos pacotes deve ser feita uma por vez.

   Nota: Você deve remover a configuração dos pacotes na ordem inversa em que eles foram instalados. Para garantir esta ordem, remova a configuração dos pacotes do primeiro do menu ao último.

6. Se você estiver removendo a configuração dos pacotes do Policy Director por que você deseja remover todo o Policy Director do computador, clique em **Remover Configuração do Policy Director do menu Smit** depois de remover a configuração de todos os pacotes do Policy Director.

   Esta etapa remove as informações do pacote do Policy Director do banco de dados do SMIT.
7. Consulte “Remoção de pacotes do Policy Director” para remover o Policy Director.

Remoção de pacotes do Policy Director

Antes de tentar remover o Policy Director, primeiro verifique se foi removida a configuração do software Policy Director.“Remoção da configuração de pacotes do Policy Director” na página 58 fornece instruções de remoção da configuração.

Para remover o Policy Director:

1. Inicie o SMIT.
2. Clique em **Instalação e Manutenção de Software**.

   O menu Instalação e Manutenção de Software é exibido.
3. Clique em **Manutenção de Utilitários de Software**.

   O menu Manutenção de Utilitários de Software é exibido.
4. Clique em **Remover Software Instalado**.

   A janela Remover Software instalado é exibida.

5. Selecione os pacotes do Policy Director a remover. Você pode selecionar mais de um pacote ao mesmo tempo.

   Para remover todos os pacotes do Policy Director, digite `IV`.

O software do Policy Director é removido.

Remoção do Console de Gerenciamento e do NeatSEAT

O Console de Gerenciamento e o cliente NetSEAT no Windows podem ser removidos através da função de remoção da instalação do InstallShield:

Remover o Console de Gerenciamento. Consulte “Remoção do Console de Gerenciamento” na página 44 para obter instruções.

Remover o cliente NetSEAT. Consulte “Remoção do cliente NetSEAT” na página 45 para obter instruções.

Capítulo 7. Instalação do Policy Director para Solaris

As seções deste capítulo descrevem como instalar e configurar o Policy Director no sistema operacional Solaris.

Antes de começar a instalação do Policy Director, certifique-se de ter revisto as informações em “Antes de instalar o Policy Director para Solaris”.

Antes de instalar o Policy Director para Solaris

Antes de iniciar a instalação do Policy Director, leia as informações a seguir:

O procedimento de instalação para este release do Policy Director requer o comando **pkgadd**. Para executar o comando **pkgadd**, digite o seguinte em um prompt de comandos:

```
# pkgadd -d /cdrom/cdrom /solaris
```

Utilize o comando **pkgadd** para instalar o software Policy Director. O comando **pkgadd** muitas vezes exibe prompts adicionais que não são indicados nas instruções do procedimento padrão. Estes prompts são exibidos em resposta a situações específicas da instalação e configuração do seu sistema. Responda sempre `s` a qualquer dos prompts que ocorrerem fora dos procedimentos padrão.

Antes de instalar o Policy Director:

Você deve instalar um cliente DCE.

Se estiver utilizando LDAP para seu registro de usuário, é necessário também instalar um cliente LDAP.

Você deve ativar os recursos da administração remota Transarc DCE antes de iniciar a instalação do Policy Director. Você não pode concluir a instalação do Policy Director se os recursos da administração remota não estiverem ativados.

A utilização de alguns recursos da administração remota ativa o Administrador de Células para que se torne essencialmente equivalente à conta root local. Normalmente, o Transarc DCE inativa estes recursos de administração remota. No entanto, o software Policy Director requer estes recursos.

Consulte a seção 4.2.1 do *Transarc Release Notes, Release 1.1* (DCE-D1002-01) para obter informações sobre como ativar os recursos da administração remota.

Saída da tela de instalação

Os procedimentos padrão deste documento não indicam todas as saídas de tela possíveis do comando **pkgadd**. Muitas das saídas de telas não documentadas fornecem informações adicionais sobre as operações que você está executando. Em geral, os procedimentos padrão desta documentação mostram apenas as mensagens que requerem uma resposta do usuário.

Instalação dos servidores Policy Director com um registro de usuário LDAP

Se você estiver instalando o Policy Director com um registro de usuário DCE, vá para “Instalação do servidor Policy Director com um registro de usuário DCE” na página 67.

Os pacotes do servidor ficam localizados no diretório /solaris no CD do *IBM SecureWay Policy Director Versão 3.0*.

Você deve ter iniciado sessão como usuário root para instalar os pacotes do Policy Director.

Se for necessário reinstalar qualquer pacote, você deve primeiro remover o pacote existente (**pkgrm**) antes de reinstalar o pacote desejado.

Para instalar o servidor de Gerenciamento:

1. Certifique-se de que o servidor LDAP esteja instalado e em execução se você for utilizar LDAP como o registro de usuário. Consulte Capítulo 4, “Instalação e configuração do IBM SecureWay Directory” na página 23 para obter instruções completas.
2. Digite o comando **pkgadd** para listar os pacotes disponíveis no CD:

   ```
   # pkgadd -d /cdrom/cdrom /solaris
   ```

   A lista de pacotes disponíveis é exibida no vídeo.

   Se você utilizar um ponto de montagem de CD-ROM diferente, substitua-o no comando acima.
3. Digite o número de seleção do IVBase para instalar os arquivos do Policy Director Base e, em seguida, pressione Enter.

   Este comando extrai arquivos do CD e instala-os onde você especificar no disco rígido.

   Um prompt é exibido indicando que a instalação do pacote IVBase foi bem-sucedida. A lista de pacotes disponíveis reaparece.

   Antes de continuar com a próxima etapa, lembre-se que deve haver apenas uma instância do servidor de Gerenciamento (IVMgr) no domínio seguro. Se esta for uma instalação de sistema independente, continue com a próxima etapa. Se você estiver instalando em um servidor secundário, certifique-se de rever “Requisitos de instalação para o domínio seguro” na página 18.
4. Digite o número de seleção do IVMgr para instalar os arquivos do servidor de Gerenciamento do Policy Director. Pressione Enter.

   Este comando extrai arquivos do CD e instala-os onde você especificar no disco rígido.

   Aparece um prompt solicitando que você escolha um tipo de registro de usuário.
5. Se você estiver utilizando LDAP como seu registro de usuário, digite 2 para registro de usuário LDAP.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
6. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

Uma série de prompts é exibida para configurar a comunicação entre o servidor de Gerenciamento e o servidor LDAP.

7. Digite as informações requeridas para a configuração do servidor LDAP:

   Nome de host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP

8. Digite o DN e a senha do usuário administrativo LDAP (por exemplo, `cn=root`). O servidor LDAP agora contém informações de segurança do Policy Director.
9. Escolha ativar ou inativar a comunicação SSL entre o servidor de Gerenciamento e o servidor LDAP.

   Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor Policy Director e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o servidor de Gerenciamento e o servidor LDAP.
10. Se você tiver inativado a comunicação SSL, ignore esta etapa. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

    `Localização do Arquivo de Conjuntos de Chaves SSL`

    `Rótulo de Chave SSL`

    `Senha da Chave SSL`

11. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

    Por exemplo:

    `o=IBM,c=BR`

    Depois que o acesso ao banco de dados GSO é configurado, o Gerenciador de Configuração do Policy Director configura um DSB automaticamente. Uma série de mensagens lista cada etapa automatizada conforme ela é concluída.

    Aparece uma mensagem indicando que a instalação do pacote IVMgr foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Instalação do Gerenciador de Segurança para WebSEAL e NetSEAL

O pacote do Gerenciador de Segurança (IVNet) requer recursos do pacote Base. Certifique-se de que o componente Base esteja instalado antes de instalar o IVNet.

1. Digite o número de seleção do IVNet para instalar os arquivos do Gerenciador de Segurança do Policy Director e, em seguida, pressione Enter.

   Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão.

   Se você estiver utilizando LDAP como seu registro de usuário, uma série de prompts é exibida para integrar o Gerenciador de Segurança com o servidor LDAP.
2. Se solicitado, digite as informações requeridas para a configuração do servidor LDAP:

   Nome de host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP

Os prompts da configuração do servidor LDAP acima aparecem apenas se a comunicação com o servidor LDAP não tiver sido configurada anteriormente para qualquer outro pacote do Policy Director neste sistema. Se o servidor de Gerenciamento (IVMgr) ou o servidor de autorização (IVAcld) tiverem sido configurados neste sistema, os prompts anteriores não aparecem nesta etapa.

3. Digite o DN e a senha do usuário administrativo do LDAP.

   O servidor LDAP agora contém informações de segurança do Policy Director.

4. Escolha ativar ou inativar a comunicação SSL entre o Gerenciador de Segurança e o servidor LDAP.

   Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor Policy Director e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o Gerenciador de Segurança e o servidor LDAP.

5. Se você tiver inativado a comunicação SSL, ignore esta etapa. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

   ```
   Localização do Arquivo de Conjuntos de chaves SSL
   Rótulo de Chave SSL
   Senha da Chave SSL
   ```

6. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

   Por exemplo:

   ```
   o=IBM,c=BR
   ```

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

7. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

   O Gerenciador de Segurança é configurado e iniciado.

   O servidor CAS é configurado e iniciado.

   Aparece uma mensagem indicando que a instalação do pacote IVNet foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Ativação do componente WebSEAL

Instale o pacote do WebSEAL (IVWeb) se desejar ativar o componente WebSEAL.

1. Digite o número de seleção do IVWeb para instalar os arquivos necessários para ativar o componente servidor HTTP do WebSEAL.
2. Pressione Enter para continuar.

   Os arquivos são extraídos do CD e instalados no disco rígido.

   Uma lista de configurações é exibida com valores que confirmam o acesso ao cliente HTTP e HTTPS, as portas TCP requeridas e o diretório raiz do documento da Web padrão.

3. Confirme os valores de configuração atuais:

```
Verifique a configuração do Servidor da Web:
1. Ativar TCP HTTP?               Sim
2. Porta HTTP                    8
3. Ativar HTTPS?                  Sim
4. Porta HTTPS                   443
5. Diretório raiz do doc. da Web     /opt/Policy Director/www/docs

a. Aceitar a configuração e continuar com a instalação
x. Sair da instalação

Selecione o item a ser alterado: a
```

4. Digite a para aceitar a configuração e continuar a instalação e, em seguida, pressione Enter.
5. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

   A instalação configura e ativa o WebSEAL no computador. O Gerenciador de Segurança é reiniciado automaticamente.

Ativação do componente NetSEAL

Instale o pacote do NetSEAL (IVTrap) se desejar ativar o componente NetSEAL.

1. Digite o número de seleção do IVTrap para instalar os arquivos necessários para ativar o componente de controle de acesso TCP/IP grosseiro do NetSEAL.

   O NetSEAL é configurado e ativado.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
2. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   Aparece uma mensagem informando que é necessário especificar portas protegidas utilizando o comando **ivadmin**.

   Aparecem outras mensagens, informando que você precisa reiniciar o sistema para assegurar que todas as portas protegidas sejam colocadas sob o controle do NetSEAL.

   Aparece um prompt indicando que a instalação do pacote IVTrap foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

O NetSEAL do Policy Director faz trap em pedidos feitos a portas específicas. Para utilizar o trap do NetSEAL, é necessário parar e reiniciar todos os aplicativos que utilizam portas específicas. Para obter mais informações sobre a configuração do NetSEAL do Policy Director para fazer trap em portas específicas, consulte as informações da visão geral sobre o NetSEAL no *Policy Director Administration Guide*.

Instalação do servidor de Autorização

Para instalar o servidor de Autorização:

1. Digite o número de seleção do IVAcld para instalar os arquivos do Gerenciador de Autorização do Policy Director e, em seguida, pressione Enter.

Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão.

Se você estiver utilizando LDAP como seu registro de usuário, um série de prompts é exibida para integrar o servidor de Autorização com o servidor LDAP.

2. Se solicitado, digite as informações requeridas para a configuração do servidor LDAP:

   Nome de host do servidor LDAP

   Número da porta do servidor LDAP

   Número da porta SSL do servidor LDAP

   Os prompts da configuração do servidor LDAP acima aparecem apenas se a comunicação com o servidor LDAP não tiver sido configurada anteriormente para qualquer outro pacote do Policy Director neste sistema. Se o servidor de Gerenciamento (IVMgr) ou o Gerenciador de Segurança (IVNet) tiverem sido configurados neste sistema, os prompts anteriores não aparecem nesta etapa.

3. Digite o DN e a senha do usuário administrativo do LDAP.

   O servidor LDAP agora contém informações de segurança do Policy Director.

4. Escolha ativar ou inativar a comunicação SSL entre o servidor de Gerenciamento e o servidor LDAP.

   Você pode ativar ou inativar individualmente a comunicação SSL entre cada servidor Policy Director e o servidor LDAP. Neste caso, você está definindo a comunicação SSL entre o servidor de Gerenciamento e o servidor LDAP.

5. Se você tiver inativado a comunicação SSL, ignore esta etapa. Se você tiver ativado a comunicação SSL, forneça valores para os seguintes prompts:

   ```
   Localização do Arquivo de Conjuntos de Chaves SSL
   Rótulo de Chave SSL
   Senha da Chave SSL
   ```

6. Ative o acesso ao banco de dados GSO fornecendo o DN do sufixo do banco de dados GSO, que você adicionou em “Adição de sufixos” na página 24.

   Por exemplo:

   ```
   o=IBM,c=BR
   ```

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.

7. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

   O servidor de Autorização é configurado e iniciado.

   Aparece um prompt indicando que a instalação do pacote IVAcld foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Instalação do componente API de Autorização

Para instalar a API de Autorização para arquivos C, digite o número de seleção do IVAuthADK e, em seguida, pressione Enter.

Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão.

Aparece um prompt indicando que a instalação do pacote IVAuthADK foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Instalação do servidor Policy Director com um registro de usuário DCE

Se você estiver instalando o Policy Director com um registro de usuário LDAP, vá para “Instalação dos servidores Policy Director com um registro de usuário LDAP” na página 61.

Os pacotes do servidor ficam localizados no diretório /solaris no CD do *IBM SecureWay Policy Director Versão 3.0*.

Você deve ter iniciado sessão como usuário root para instalar os pacotes do Policy Director.

Se for necessário reinstalar qualquer pacote, você deve primeiro remover o pacote existente (**pkgrm**) antes de reinstalar o pacote desejado.

Para instalar o servidor de Gerenciamento:

1. Digite o comando **pkgadd** para listar os pacotes disponíveis no CD:

   ```
   # pkgadd -d /cdrom/cdrom /solaris
   ```

   A lista de pacotes disponíveis é exibida no vídeo.

   Se você utilizar um ponto de montagem de CD-ROM diferente, substitua-o no comando acima.
2. Digite o número de seleção do IVBase para instalar os arquivos do Policy Director Base e, em seguida, pressione Enter.

   Este comando extrai arquivos do CD e instala-os onde você especificar no disco rígido.

   Um prompt é exibido indicando que a instalação do pacote IVBase foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

   Antes de continuar com a próxima etapa, lembre-se que deve haver apenas uma instância do servidor de Gerenciamento (IVMgr) no domínio seguro. Se esta for uma instalação de sistema independente, continue com a próxima etapa. Se você estiver instalando em um servidor secundário, certifique-se de rever “Requisitos de instalação para o domínio seguro” na página 18.
3. Digite o número de seleção do IVMgr para instalar os arquivos do servidor de Gerenciamento do Policy Director. Pressione Enter.

   Este comando extrai arquivos do CD e instala-os onde você especificar no disco rígido.

   Aparece um prompt solicitando que você escolha um tipo de registro de usuário.
4. Se você estiver utilizando DCE como seu registro de usuário, digite `1`.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
5. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

Aparece uma mensagem indicando que a instalação do pacote IVMgr foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Instalação do Gerenciador de Segurança para WebSEAL e NetSEAL

O pacote do Gerenciador de Segurança (IVNet) requer recursos do pacote Base. Certifique-se de que o componente Base esteja instalado antes de instalar o IVNet.

1. Digite o número de seleção do IVNet para instalar os arquivos do Gerenciador de Segurança do Policy Director e, em seguida, pressione Enter.

   Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão. Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
2. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

   O Gerenciador de Segurança é configurado e iniciado.

   Aparece uma mensagem indicando que a instalação do pacote IVNet foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Ativação do componente WebSEAL

Instale o pacote do WebSEAL (IVWeb) se desejar ativar o componente WebSEAL.

1. Digite o número de seleção do IVWeb para instalar os arquivos necessários para ativar o componente servidor HTTP do WebSEAL.
2. Pressione Enter para continuar.

   Os arquivos são extraídos do CD e instalados no disco rígido.

   Uma lista de configurações é exibida com valores que confirmam o acesso ao cliente HTTP e HTTPS, as portas TCP requeridas e o diretório raiz do documento da Web padrão.
3. Confirme os valores de configuração atuais:

   ```
   Verifique a configuração do Servidor da Web:
   1. Ativar TCP HTTP?               Sim
   2. Porta HTTP                    8
   3. Ativar HTTPS?                  Sim
   4. Porta HTTPS                   443
   5. Diretório raiz do doc. da Web     /opt/Policy Director/www/docs

   a. Aceitar a configuração e continuar com a instalação
   x. Sair da instalação

   Selecione o item a ser alterado: a
   ```
4. Digite a para aceitar a configuração e continuar a instalação e, em seguida, pressione Enter.
5. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

A instalação configura e ativa o WebSEAL no computador. O Gerenciador de Segurança é reiniciado automaticamente.

Ativação do componente NetSEAL

Instale o pacote do NetSEAL (IVTrap) se desejar ativar o componente NetSEAL.

1. Digite o número de seleção do IVTrap para instalar os arquivos necessários para ativar o componente de controle de acesso TCP/IP grosseiro do NetSEAL.

   O NetSEAL é configurado e ativado.

   Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
2. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   Aparece uma mensagem informando que é necessário especificar portas protegidas utilizando o comando **ivadmin**.

   Aparecem outras mensagens, informando que você precisa reiniciar o sistema para assegurar que todas as portas protegidas sejam colocadas sob o controle do NetSEAL.

   Aparece um prompt indicando que a instalação do pacote IVTrap foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

O NetSEAL do Policy Director faz trap em pedidos feitos a portas específicas. Para utilizar o trap do NetSEAL, é necessário parar e reiniciar todos os aplicativos que utilizam portas específicas. Para obter mais informações sobre a configuração do NetSEAL do Policy Director para fazer trap em portas específicas, consulte as informações da visão geral sobre o NetSEAL no *Policy Director Administration Guide*.

Instalação do servidor de Autorização

Para instalar o servidor de Autorização:

1. Digite o número de seleção do IVAcld para instalar os arquivos do Gerenciador de Autorização do Policy Director e, em seguida, pressione Enter.

   Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão. Aparece um prompt solicitando o nome e a senha do Administrador de Células do DCE.
2. Digite as informações requeridas para acesso à conta de Administração de Células DCE.

   ```
   Digite o nome do usuário do Administrador de Células [cell_admin]:
   Digite a senha do Administrador de Células:
   ```

   O servidor de Autorização é configurado e iniciado.

   Aparece um prompt indicando que a instalação do pacote IVAcld foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Instalação do componente API de Autorização

Para instalar a API de Autorização para arquivos C, digite o número de seleção do IVAuthADK e, em seguida, pressione Enter.

Os arquivos são extraídos do CD e instalados no disco rígido no diretório padrão.

Aparece um prompt indicando que a instalação do pacote IVAuthADK foi bem-sucedida. A lista de pacotes disponíveis é exibida novamente.

Configuração do Credentials Acquisition Service

O CAS do Policy Director é instalado automaticamente. Se desejar utilizar o CAS do Policy Director para seu serviço de aquisição de credenciais, você deve configurá-lo. Consulte as informações sobre configuração de um serviço de aquisição de credenciais no *Policy Director Administration Guide* para obter instruções.

Instalação do Console de Gerenciamento

O Policy Director fornece um Console de Gerenciamento que gerencia muitos dos componentes do Policy Director.

O Console de Gerenciamento para Solaris é instalada através do pacote de instalação do IVConsole. Utilize **pkgadd** para instalar e configurar o pacote.

1. Inicie sessão como root.
2. Insira e monte o CD do *IBM SecureWay Policy Director Versão 3.0* na unidade de CD-ROM do sistema do servidor Policy Director.
3. Exiba a lista de pacotes disponíveis:

   ```
   # pkgadd -d /cdrom/cdrom /solaris
   ```

4. Digite o número de seleção do IVBase se ele ainda não estiver instalado. Se o IVBase já estiver instalado, vá para a etapa 6.
5. Digite `s` para continuar.

   A lista de pacotes é exibida.
6. Digite o número de seleção do IVConsole.
7. Digite `s` para continuar.

   Aparece um prompt indicando que a instalação foi bem-sucedida. O Console de Gerenciamento está agora pronta para ser iniciada.

Início do Console de Gerenciamento

Para iniciar o Console de Gerenciamento:

1. Certifique-se de que os servidores Policy Director estejam instalados e em execução.
2. Digite o seguinte comando:

```
$ /opt/intraverse/bin/ivconsole
```

Remoção do Policy Director

Remova os servidores Policy Director do computador utilizando o utilitário **pkgrm**. Os pacotes devem ser removidos na ordem oposta seguida durante a instalação. Os comandos **pkgrm** e **pkgadd** são membros da mesma família de utilitários e possuem a mesma interface com o usuário. O usuário root executa o utilitário **pkgrm**.

Há vários métodos para utilizar este comando:

Inicie o comando **pkgrm** sem nenhum argumento.

Uma lista numerada dos pacotes atuais em seu computador é exibida. Digite um número de seleção referente ao pacote que deseja remover.

Inicie o comando **pkgrm** e especifique um único nome de pacote como argumento do comando. Por exemplo:

```
# pkgrm IVBase
```

Inicie o comando **pkgrm** e especifique uma seqüência de nomes de pacotes como argumentos múltiplos para o comando. Por exemplo:

```
# pkgrm IVAuthADK IVAcld IVTrap IVWeb IVNet IVMgr IVBase
```

Consulte a documentação do sistema operacional Solaris para obter mais informações detalhadas sobre o comando **pkgrm**.

Nota: Você deve remover os pacotes do Policy Director na ordem exatamente inversa à ordem requerida para a instalação.

Para remover o Policy Director:

1. Inicie sessão no sistema operacional Solaris como root.

   Utilize um dos métodos anteriores para iniciar o comando **pkgrm**.
2. Os componentes do Policy Director devem ser removidos na seguinte ordem:

   IVTrap
   IVWeb
   IVNet
   IVAuthADK
   IVAcld
   IVMgr
   IVBase

   A configuração do seu sistema pode não incluir todos os pacotes que são mostrados na lista anterior. O Console de Gerenciamento do Policy Director (IVConsole) pode ser removida a qualquer momento antes do IVBase.

Remoção do Console de Gerenciamento

Para remover o Console de Gerenciamento:

1. Inicie sessão como usuário root.
2. Digite o seguinte comando:

   ```
   # pkgrm ivconsole
   ```

Capítulo 8. Documentação Relacionada

Você pode utilizar a documentação relacionada neste capítulo para encontrar mais informações sobre o Policy Director Versão 3.0 e os produtos relacionados.

Documentação do Policy Director

Este manual, *Instalação e Uso do IBM SecureWay Policy Director, Versão 3.0*, além de ser fornecido junto com o produto Policy Director, também está disponível em um pacote de documentação. O pacote de documentação do Policy Director inclui este manual e as informações sobre licença do Policy Director.

Além deste manual, os seguintes documentos contêm informações sobre o Policy Director e estão disponíveis em formato PDF (PostScript Document Format) no subdiretório /doc no CD do *IBM SecureWay Policy Director Versão 3.0*:

IBM SecureWay Policy Director Administration Guide, Versão 3.0

Este manual fornece instruções detalhadas para a administração do Policy Director. Ele fornece informações sobre o IBM SecureWay Policy Director, tais como:

- Os conceitos do Policy Director tais como autenticação, autorização e aquisição de credenciais
- As tarefas de administração gerais utilizando o Console de Gerenciamento
- A administração do WebSEAL
- A administração do NetSEAL
- A administração do NetSEAT
- Os recursos da administração (o comando **ivadmin**)

IBM SecureWay Policy Director Programming Guide and Reference, Versão 3.0

Este manual descreve os componentes da API de Autorização e como executar estas tarefas:

- Construção de aplicativos com a API de Autorização
- Inicialização do Serviço de Autorização do Policy Director
- Autenticação de um servidor ou cliente de aplicativo
- Obtenção de credenciais de usuários
- Tomada de decisão de uma autorização
- Execução de tarefas opcionais
- Limpeza e desligamento
- Implementação de aplicativos com a API de Autorização

O arquivo README do Policy Director pode conter as informações mais recentes sobre informações do Policy Director que substituem as publicações do produto.

Para obter o arquivo README mais recente, acesse a página da biblioteca do site da Web do IBM SecureWay Policy Director.

`http://www.ibm.com/software/security/policy/library`

Documentação do IBM SecureWay FirstSecure

O manual a seguir contém informações sobre o FirstSecure:

IBM SecureWay FirstSecure Planning and Integration, Versão 2.0 (S564-8D11–00)

Este manual descreve o FirstSecure e os produtos que compõem o FirstSecure, e auxilia no planejamento da utilização de todos os produtos IBM SecureWay.

O IBM SecureWay Policy Director (Policy Director) está disponível como um componente do IBM SecureWay FirstSecure ou como um produto independente. Se a versão de seu Policy Director estiver incluída na oferta do FirstSecure, este manual será fornecido com o FirstSecure. Se a versão de seu Policy Director foi adquirida como um produto independente, este manual pode ser encontrado na página do FirstSecure na Web:

`http://www.ibm.com/software/security/firstsecure/library`

Documentação do IBM Distributed Computing Environment

Os documentos a seguir descrevem como instalar o DCE e estão disponíveis no CD do *IBM SecureWay Policy Director Security Services* em formato PDF no diretório /doc ou no site do DCE na Web:

`http://www.ibm.com/network/dce/library/`

IBM DCE para Windows NT

O *IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2* está disponível no seguinte endereço da Web:

`http://www.software.ibm.com/network/dce/library/publications/dcent.html`

Este manual descreve o DCE (Distributed Computing Environment) para Windows NT, Versão 2.2 e explica como planejar, instalar e configurar o produto.

O *IBM Distributed Computing Environment for Windows NT Quick Beginnings Version 2.2* também está disponível no CD do *IBM SecureWay Policy Director Security Services* CD em /doc/DCE22_QuickBeginnings_NT.pdf.

IBM DCE para AIX

IBM Distributed Computing for AIX Quick Beginnings Version 2.2, disponível no seguinte endereço da Web:

`http://www.software.ibm.com/network/dce/library/publications/dceaix.html`

Este manual descreve o IBM Distributed Computing Environment para AIX, Versão 2.2 e explica como planejar, instalar e configurar o produto.

O *IBM Distributed Computing Environment for AIX Quick Beginnings Version 2.2* também está disponível no CD do *IBM SecureWay Policy Director Security Services* em /doc/DCE22_QuickBeginnings_AIX.pdf.

Transarc DCE para Solaris

O *Transarc DCE Version 2.0 Release Notes* e o *Installation and Configuration Guide* estão disponíveis no seguinte endereço da Web:

`http://www.transarc.com/Library/documentation/dce/2. /index.html`

O *Transarc DCE Version 2.0 Release Notes* documenta as seguintes informações sobre o software e a documentação do Transarc DCE:

Diferenças entre o OSF DCE e o produto DCE * DFS

Diferenças entre a Versão 2.0 e a Versão 1.1 do DCE * DFS

Defeitos conhecidos e limitações associadas ao DCE * DFS

O *Transarc DCE Version 2.0 Release Notes* também está disponível no CD do *IBM SecureWay Policy Director Security Services* CD em /doc/DCE20_ReleaseNotes_Solaris.pdf.

O *Installation and Configuration Guide* fornece instruções para instalação, configuração e atualização do produto DCE DFS 2.0.

O *Installation and Configuration Guide* também está disponível no CD do *IBM SecureWay Policy Director Security Services* em /doc/DCE20_InstallGuide_Solaris.pdf.

Documentação do IBM SecureWay Directory

O manual a seguir contém informações sobre instalação e configuração do IBM SecureWay Directory (LDAP):

IBM SecureWay Directory Installation and Configuration, Versão 3.1.1

Há uma versão separada deste manual em formato HTML para cada um dos sistemas operacionais suportados. O manual para cada sistema operacional está no CD apropriado em /doc/wparent.htm. Os CDs são:

— *IBM SecureWay Directory Versão 3.1.1 para NT*

— *IBM SecureWay Directory Versão 3.1.1 para AIX*

— *IBM SecureWay Directory Versão 3.1.1 para Solaris*

Depois da instalação do LDAP, a localização do arquivo de documentação .HTM de instalação e configuração será:

```
C:\Arquivos de Programas\IBM\LDAP\nls\html\enUS1252\config\wparent.htm
```

O manual a seguir em arquivo HTML contém informações sobre como administrar o IBM SecureWay:

IBM SecureWay Directory Administration Guide, Versão 3.1.1

1. Utilizando um Navegador da web, acesse a documentação encontrada neste endereço da Web depois de uma instalação padrão do LDAP:

   ```
   C:\Arquivos de Programas\IBM\LDAP\nls\html\enUS1252\config\wparent.ht
   ```

O manual a seguir em formato HTML contém informações sobre o cliente IBM SecureWay Directory:

IBM SecureWay Directory Client SDK Programming Reference, Versão 3.1.1

Este manual contém links para estas informações sobre o LDAP:

— As informações sobre o LDAP Client SDK Plugin Programming Reference

1. Utilizando um Navegador da web, acesse a documentação encontrada neste endereço da Web depois de uma instalação padrão do LDAP:

   ```
   C:\Arquivos de Programas\IBM\doc\progref.htm
   ```

2. Abra a documentação *IBM SecureWay Directory Client SDK Programming Reference*.
3. Clique em **Apêndices**.
4. Clique em **LDAP Client SDK Plugin Programming Reference**

— As informações sobre como utilizar o GSKit e o Key Management Tool **ikmguiw** para configurar o servidor LDAP para suportar acesso SSL

1. Se este manual ainda não estiver aberto, abra a documentação *IBM SecureWay Directory Client SDK Programming Reference*.
2. Clique em **API categories**.
3. Clique em **SSL**.
4. Clique em **LDAP_SSL API**.

5. Localize e clique no link **Using IKMGUI** para abrir o arquivo HTML apropriado.

O documento a seguir também está disponível para o servidor IBM SecureWay Directory:

IBM SecureWay Directory Server Plug-ins Reference

Apêndice A. Avisos

Consulte o representante IBM local para informações sobre produtos e serviços atualmente disponíveis em sua região. Referências a produtos, programas ou serviços IBM não significam que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição ao produto, programa ou serviço. A avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM é de inteira responsabilidade do usuário.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença podem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais - IBM Brasil
Avenida Pasteur, 138-146 - Botafogo
Rio de Janeiro, RJ
CEP 22.290-240
Brasil

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO “NO ESTADO”, SEM GARANTIA DE ESPÉCIE ALGUMA, EXPLÍCITA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS DE NÃO VIOLAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM FIM ESPECÍFICO. Alguns países não permitem a exclusão de garantias explícitas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar a você.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode fazer aperfeiçoamentos e/ou alterações nos produtos e/ou programas descritos nestas informações, a qualquer momento, sem aviso prévio.

Quaisquer referências nesta publicação a sites da Web que não sejam controlados pela IBM são fornecidas apenas por conveniência e não constituem endosso desses sites da Web. Os materiais contidos nesses sites da Web não fazem parte dos materiais deste produto IBM e a utilização desses sites da Web é de inteira responsabilidade do cliente.

Quando você envia informações à IBM, concede a ela direitos não exclusivos de utilização ou distribuição das informações, da forma que julgar adequada, sem incorrer em obrigações para com você.

O programa licenciado descrito neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos de Contrato de Cliente IBM (IBM Customer Agreement), Contrato de Licença de Programa Internacional IBM (IBM International Program License Agreement) ou qualquer contrato equivalente.

Todos os dados de desempenho contidos aqui foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sito feitas em sistemas a nível de desenvolvimento e não há garantias de que estas medidas serão iguais nos sistemas normalmente disponíveis. Além disso, algumas medidas podem ter sido estimadas através da extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seus ambientes específicos.

As informações sobre produtos não-IBM foram obtidas junto aos fornecedores desses produtos, seus anúncios publicados e outras fontes disponíveis publicamente. A IBM não efetuou nenhum teste desses produtos e não pode afirmar a precisão de seu desempenho, compatibilidade ou qualquer outro requisito. Perguntas sobre recursos de produtos não-IBM devem ser endereçadas aos fornecedores dos respectivos produtos.

Todas as declarações a respeito de futuras instruções ou intenções da IBM estão sujeitas à alteração ou remoção sem aviso prévio e representam apenas objetivos e metas.

Todos os preços IBM apresentados são preços de revenda sugeridos pela IBM, são atuais e sujeitos a alterações sem aviso prévio. Os preços do revendedor podem variar.

Estas informações contêm exemplos de dados e relatórios utilizados em operações diárias da empresa. Para ilustrá-las da maneira mais completa possível, os exemplos contêm nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

Marcas

Os termos a seguir são marcas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

AIX
DB2
FirstSecure
IBM
Policy Director
SecureWay

Outros nomes de empresas, produtos ou serviços podem ser marcas ou marcas de serviço de terceiros.

AuthAPI	DASCOM, Inc.
DASCOM	DASCOM, Inc.
Internet Explorer	Microsoft Corporation
Netscape e os logotipos Netscape	Netscape Communications Corporation
Netscape Communicator	Netscape Communications Corporation
Netscape Navigator	Netscape Communications Corporation
NetSEAL	DASCOM, Inc.
NetSEAT	DASCOM, Inc.
Solaris	Sun Microsystems, Inc.
WebSEAL	DASCOM, Inc.

Java e todas as marcas e logotipos baseados em Java são marcas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo do Windows são marcas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada nos Estados Unidos e/ou em outros países, licenciada exclusivamente pela X/Open Company Limited.

Índice Remissivo

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Número da Peça: CT63KBP

Impresso no Brasil

CT63KBP