CA Identity Manager™

Guia de Configuração

12.6.5

A presente documentação, que inclui os sistemas de ajuda incorporados e os materiais distribuídos eletronicamente (doravante denominada Documentação), destina-se apenas a fins informativos e está sujeita a alterações ou remoção por parte da CA a qualquer momento. Esta Documentação contém informações proprietárias da CA e não pode ser copiada, transferida, reproduzida, divulgada, modificada nem duplicada, parcial ou completamente, sem o prévio consentimento por escrito da CA.

Se o Cliente for um usuário licenciado do(s) produto(s) de software referido(s) na Documentação, é permitido que ele imprima ou, de outro modo, disponibilize uma quantidade razoável de cópias da Documentação para uso interno seu e de seus funcionários envolvidos com o software em questão, contanto que todos os avisos de direitos autorais e legendas da CA estejam presentes em cada cópia reproduzida.

O direito à impressão ou, de outro modo, à disponibilidade de cópias da Documentação está limitado ao período em que a licença aplicável ao referido software permanecer em pleno vigor e efeito. Em caso de término da licença, por qualquer motivo, fica o usuário responsável por garantir à CA, por escrito, que todas as cópias, parciais ou integrais, da Documentação sejam devolvidas à CA ou destruídas.

NA MEDIDA EM QUE PERMITIDO PELA LEI APLICÁVEL, A CA FORNECE ESTA DOCUMENTAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM NENHUM TIPO DE GARANTIA, INCLUINDO, ENTRE OUTROS, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM DETERMINADO FIM OU NÃO VIOLAÇÃO. EM NENHUMA OCASIÃO, A CA SERÁ RESPONSÁVEL PERANTE O USUÁRIO OU TERCEIROS POR QUAISQUER PERDAS OU DANOS, DIRETOS OU INDIRETOS, RESULTANTES DO USO DA DOCUMENTAÇÃO, INCLUINDO, ENTRE OUTROS, LUCROS CESSANTES, PERDA DE INVESTIMENTO, INTERRUPÇÃO DOS NEGÓCIOS, FUNDO DE COMÉRCIO OU PERDA DE DADOS, MESMO QUE A CA TENHA SIDO EXPRESSAMENTE ADVERTIDA SOBRE A POSSIBILIDADE DE TAIS PERDAS E DANOS.

O uso de qualquer software mencionado na Documentação é regido pelo contrato de licença aplicável, e tal contrato não deve ser modificado de nenhum modo pelos termos deste aviso.

O fabricante desta Documentação é a CA.

Fornecida com “Direitos restritos”. O uso, duplicação ou divulgação pelo governo dos Estados Unidos está sujeita às restrições descritas no FAR, seções 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e DFARS, seção 252.227-7014(b)(3), conforme aplicável, ou sucessores.

Copyright © 2015 CA. Todos os direitos reservados. Todas as marcas comerciais, nomes de marcas, marcas de serviço e logotipos aqui mencionados pertencem às suas respectivas empresas.

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA:

- CA Identity Manager
- CA SiteMinder®
- Diretório do CA
- CA User Activity Reporting
- CA Identity Governance

Índice

Capítulo 4: Gerenciamento de bancos de dados relacionais 103

Capítulo 5: Diretórios do CA Identity Manager 155

Capítulo 1: Introdução aos ambientes do CA Identity Manager

Esta seção contém os seguintes tópicos:

Componentes do ambiente do CA Identity Manager

Um *Ambiente* do CA Identity Manager é a exibição de um namespace de gerenciamento que permite aos administradores do CA Identity Manager gerenciar objetos, como usuários, grupos e organizações. Esses objetos recebem um conjunto de funções e tarefas associadas. O Ambiente do CA Identity Manager controla o gerenciamento e a apresentação gráfica de um diretório.

Um único repositório de usuários pode associar vários Ambientes do CA Identity Manager (na página 14) para definir diferentes exibições do diretório. No entanto, um Ambiente do CA Identity Manager é associado a apenas um repositório de usuários.

Os ambientes do CA Identity Manager contêm os seguintes elementos:

Diretório

Descreve um repositório de usuários para o CA Identity Manager. O elemento Diretório inclui:

- Um ponteiro para um repositório de usuários, que armazena objetos gerenciados, como usuários, grupos e organizações.
- Os metadados que descrevem como objetos gerenciados são armazenados no diretório e suas representações no CA Identity Manager.

Diretório de provisionamento (opcional)

Armazena dados relevantes para o Servidor de provisionamento gerenciar contas adicionais em terminais gerenciados. Somente um Diretório de provisionamento pode ser associado a um Ambiente.

Observação: para obter mais informações sobre o Servidor de provisionamento ou Diretório de provisionamento, consulte o *Guia de Instalação*.

Console de usuário

Permite que os administradores do CA Identity Manager executem tarefas em um Ambiente do CA Identity Manager.

Definições de tarefa e função

Determinam os privilégios de usuário no CA Identity Manager e em outros aplicativos. Essas definições de tarefa e função, inicialmente, estão disponíveis no Ambiente do CA Identity Manager, onde podem ser atribuídas a usuários.

Você pode personalizar as funções e tarefas padrão usando o Console de usuário.

Autoatendimento

Permite aos usuários criar e manter suas próprias contas para acessar recursos, como um site de cliente. O autoatendimento também permite que os usuários solicitem uma senha temporária, caso esqueçam a senha atual.

Definições de fluxo de trabalho

O CA Identity Manager inclui definições de fluxo de trabalho padrão que automatizam a aprovação e a notificação de tarefas de gerenciamento de usuário, como criação de perfis de usuário ou atribuição de usuários a funções ou grupos. Você pode modificar os processos de fluxo de trabalho padrão no CA Identity Manager para oferecer suporte aos requisitos de cada empresa.

Capas

Determinam a aparência da interface do usuário do CA Identity Manager.

Recursos personalizados

Você pode modificar o CA Identity Manager para atender aos requisitos de negócios usando as APIs do CA Identity Manager. Consulte o *Guia de Programação do Java*.

Cada ambiente do CA Identity Manager exige um ou mais gerentes de sistema para personalizar as funções e tarefas iniciais usando o Console de usuário. Quando um gerente do sistema cria as funções e tarefas iniciais, esse gerente pode conceder privilégios administrativos a usuários no ambiente. Esses usuários tornam-se administradores que gerenciam usuários, grupos e organizações. Consulte o *Guia de Administração*.

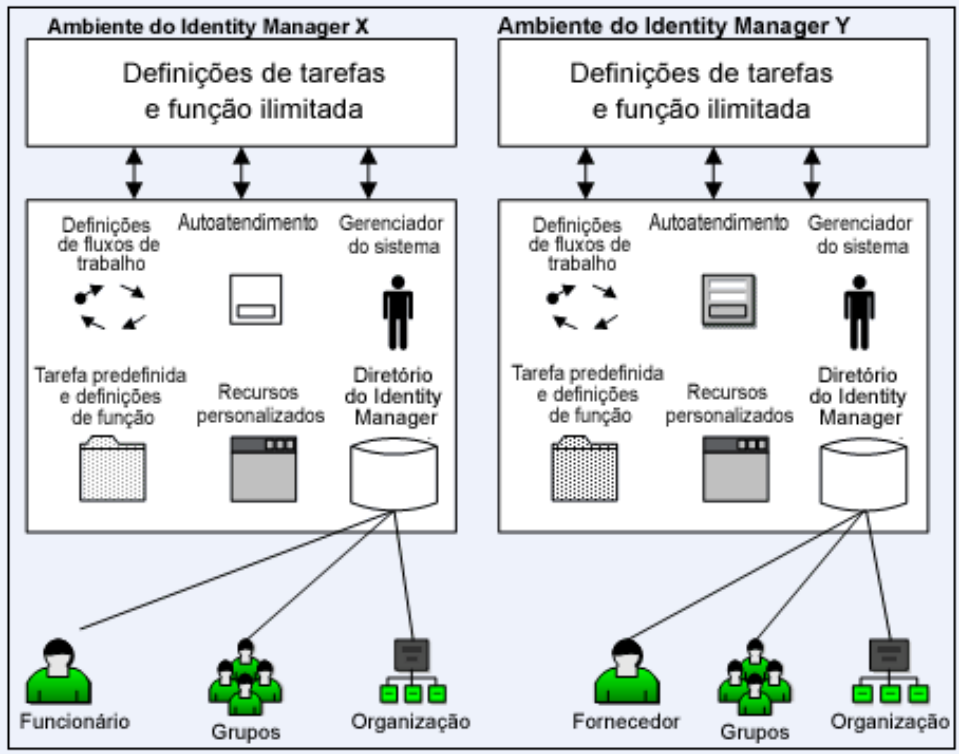
Vários ambientes do CA Identity Manager

Crie vários ambientes do CA Identity Manager quando desejar:

- Gerenciar repositórios de usuários adicionais: você pode gerenciar usuários em diferentes tipos de repositório de usuários. Por exemplo, sua empresa armazena todos os perfis de usuário em um diretório LDAP do sistema Sun Java. Você entra em uma joint venture com um parceiro que usa um banco de dados Oracle para armazenar informações de usuários. Você deseja um ambiente diferente do CA Identity Manager para cada conjunto de usuários.

- Gerenciar objetos com diferentes classes de objetos LDAP: considere que o CA Identity Manager está gerenciando um diretório LDAP. No mesmo diretório, é possível gerenciar objetos do mesmo tipo com diferentes atributos e classes de objeto. Por exemplo, a ilustração a seguir mostra um diretório que contém dois tipos de usuário:
  - Funcionários, que têm um número de ID de funcionário.
  - Fornecedores, que são identificados com um número de fornecedor.

Equation 1: Diagrama mostrando o exemplo de dois ambientes do Identity Manager com diretórios que contêm funcionários e fornecedores.



Management Console do CA Identity Manager

Como um administrador do sistema do CA Identity Manager, suas responsabilidades incluem:

- Criar um Diretório do CA Identity Manager
- Configurar um Diretório de provisionamento
- Configurar um ambiente do CA Identity Manager
- Atribuir um gerente do sistema
- Ativar recursos personalizados para uso inicial

Para configurar um ambiente do CA Identity Manager, use o Management Console, um aplicativo com base na web.

O Management Console é dividido em duas seções a seguir:

- Directories: use essa seção para criar e gerenciar Diretórios e Diretórios de provisionamento do CA Identity Manager, que descrevem repositórios de usuários para o CA Identity Manager.
- Environments: use essa seção para criar e gerenciar ambientes do CA Identity Manager, que controlam o gerenciamento e a apresentação gráfica de um diretório.

Como acessar o Management Console do CA Identity Manager

Para acessar o Management Console, digite o seguinte URL no navegador:

http://*nome_do_host*:*porta*/iam/immanage

nome do host

Define o nome de domínio totalmente qualificado ou o endereço IP do servidor em que o CA Identity Manager está instalado.

Observação: se você estiver acessando o Management Console usando o Internet Explorer 7 e o nome do host incluir um endereço IPv6, o Management Console poderá ser exibido incorretamente. Para evitar esse problema, use o nome do host totalmente qualificado ou um endereço IPv4.

porta

Define a porta do servidor de aplicativos.

Observação: se você estiver usando um Agente web para fornecer autenticação avançada do CA Identity Manager, não será necessário especificar o número da porta.

Observação: ative o JavaScript no navegador que você usa para acessar o Management Console.

Caminhos de exemplo para o Management Console:

- Para weblogs geológicos:

  http://meu_servidor.minha_empresa.org:7001/iam/immanage

- Para JBoss:

  http://meu_servidor.minha_empresa.org:8080/iam/immanage

- Para WebSphere:

  http://meu_servidor.minha_companhia.org:9080/iam/immanage

Como criar um ambiente do CA Identity Manager

Para criar um ambiente do CA Identity Manager, execute as seguintes etapas no Management Console:

1. Use o Assistente de configuração de diretório (na página 157) para criar um Diretório do CA Identity Manager.
2. Se seu ambiente incluir provisionamento, use o Assistente de configuração de diretório novamente para criar um Diretório de provisionamento (na página 171).
3. Crie um Ambiente do CA Identity Manager.
4. Acesse o Ambiente (na página 194) para verificar se ele está em execução.

Capítulo 2: Exemplo de Ambiente do CA Identity Manager

Esta seção contém os seguintes tópicos:

Visão geral da amostra de Ambiente do CA Identity Manager

O CA Identity Manager inclui uma amostra de ambiente que você pode usar para aprender sobre o CA Identity Manager e testá-lo.

A amostra de ambiente tem como base uma empresa comercial de automóveis denominada NeteAuto. Os administradores da NeteAuto usam o CA Identity Manager para gerenciar funcionários, fornecedores e concessionárias.

As configurações do repositório de usuários para usar os ambientes da NeteAuto são:

- Repositórios de usuários LDAP que oferecem suporte a organizações
- Repositórios de usuários LDAP que não oferecem suporte a organizações.
- Repositórios de usuários de banco de dados relacional que oferecem suporte a organizações
- Repositórios de usuários de banco de dados relacional que não oferecem suporte a organizações.

Observação: os recursos de provisionamento não estão disponíveis porque esse ambiente não tem nenhum diretório de provisionamento.

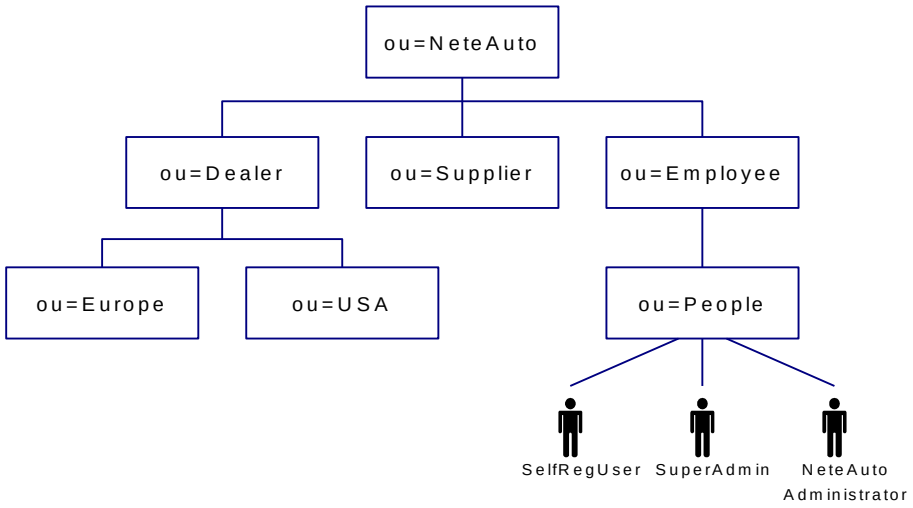
Como configurar a amostra NeteAuto com o suporte à organização

A configuração da amostra NeteAuto com o suporte à organização envolve as seguintes etapas:

- Instalar o software de pré-requisito
- Instalar o ambiente de amostra do CA Identity Manager
- Configurar um diretório de usuários LDAP
- Configurar um banco de dados relacional
- Criar o diretório do CA Identity Manager
- Criar o ambiente do CA Identity Manager para a NeteAuto

Estrutura de diretório LDAP para a NeteAuto

A ilustração a seguir descreve a amostra NeteAuto para diretórios LDAP:



A amostra de Ambiente do CA Identity Manager inclui os seguintes usuários:

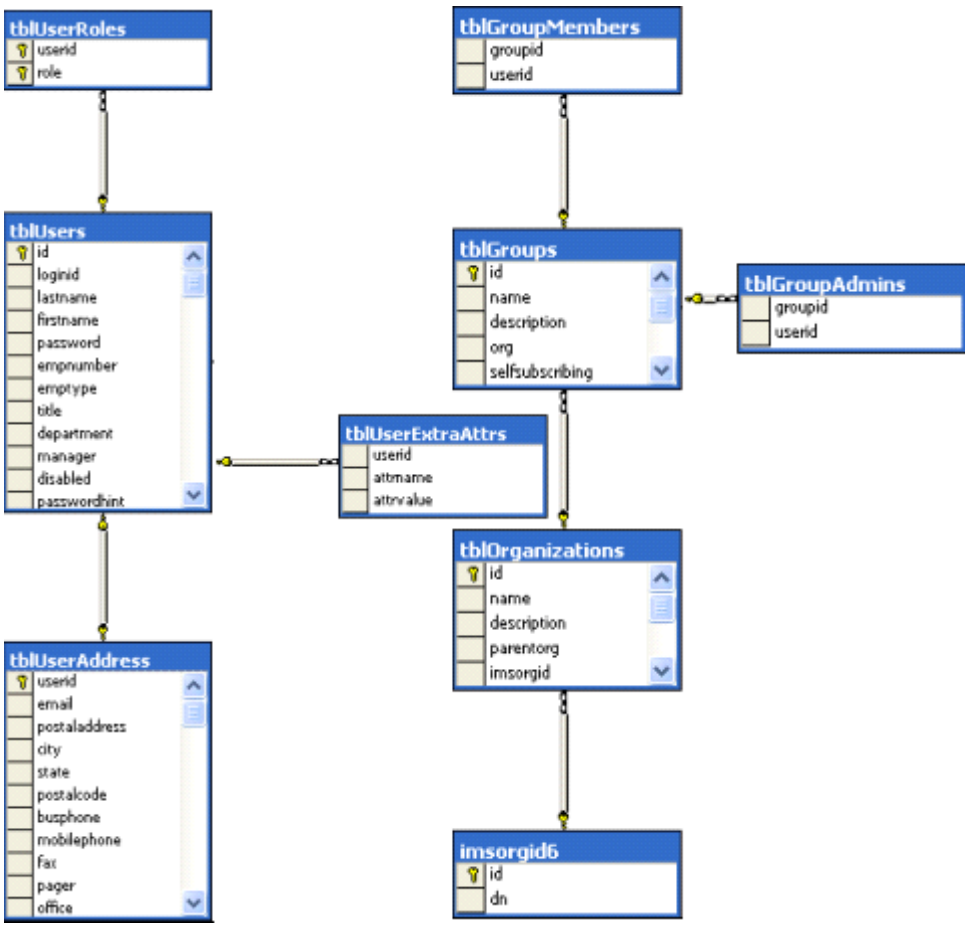
- Superadmin é a conta de administrador com a função Gerente do sistema para esse ambiente do CA Identity Manager. Como superadmin, você pode executar todas as tarefas administrativas padrão.

  Observação: para obter uma descrição das tarefas administrativas padrão, consulte o *Guia de Administração*.

- SelfRegUser é a conta de administrador que o CA Identity Manager usa para ativar o autorregistro para esse ambiente do CA Identity Manager.
- O Administrador da NeteAuto não tem privilégios quando você instala o ambiente da NeteAuto. No entanto, você pode atribuir Gerenciador do grupo como uma função de usuário, conforme descrito em Atribuir a função de Gerenciador do grupo.

Banco de dados relacional para NeteAuto

A ilustração a seguir descreve o banco de dados relacional para a amostra NeteAuto, incluindo uma tabela de organização:



Software de pré-requisito para a NeteAuto

O ambiente do CA Identity Manager para a NeteAuto tem os seguintes pré-requisitos:

- Instale o CA Identity Manager, conforme descrito no *Guia de Instalação*. Certifique-se de instalar as Ferramentas administrativas do CA Identity Manager.
- Você deve ter acesso a um Servidor de diretórios do sistema Sun Java (Sun ONE ou iPlanet) ou a um banco de dados Microsoft SQL Server.

Arquivos de instalação para o ambiente da NeteAuto

O CA Identity Manager inclui um conjunto de arquivos que podem ser usados para configurar uma amostra do ambiente do CA Identity Manager. O ambiente do CA Identity Manager é uma exibição de um namespace de gerenciamento que permite aos administradores do CA Identity Manager gerenciar objetos, como usuários, grupos e organizações. Esses objetos são gerenciados com um conjunto de funções e tarefas associadas. O ambiente do CA Identity Manager controla o gerenciamento e a apresentação gráfica de um diretório.

O ambiente de amostra do CA Identity Manager inclui:

- Amostra de objetos, como usuários e organizações
- Definições de função, tarefa e tela

  As tarefas são exibidas no Console de usuário quando você clica em uma guia, como Usuários ou Grupos. Com base nas funções atribuídas, as tarefas associadas são exibidas quando o usuário efetua logon.

  Observação: para obter mais informações sobre funções e tarefas, consulte o *Guia de Administração*.
- Uma amostra de capa que personaliza os usuários do Console de usuário para a NeteAuto.
- Um arquivo de configuração de diretório que você usa para criar um diretório do CA Identity Manager.

Os arquivos para criação da amostra do ambiente do CA Identity Manager estão instalados no seguinte local:

ferramentas_administrativas\samples\NeteAuto

Nesse caminho, *ferramentas_administrativas* se refere às Ferramentas administrativas. As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Instalar o ambiente da NeteAuto

Execute o processo a seguir para instalar o ambiente da NeteAuto.

Siga estas etapas:

1. Verifique se o software de pré-requisito está instalado (na página 22).
2. Configure o repositório de usuários e importe a amostra de dados.
   - Para usuários LDAP: configure um diretório de usuários LDAP (na página 23)
   - Para usuários de banco de dados relacional: configure um banco de dados relacional
3. Crie o diretório do CA Identity Manager para a NeteAuto.
4. Crie o ambiente do CA Identity Manager para a NeteAuto.
5. Configure a aparência da interface do usuário do CA Identity Manager para os usuários da NeteAuto (na página 38).

Configurar um diretório de usuários LDAP

O diretório LDAP está disponível de acordo com a sua instalação. Você pode usar o procedimento a seguir para verificar se o diretório existe ou para criar o diretório.

Siga estas etapas:

1. No console do servidor de diretórios, crie uma instância do LDAP com a seguinte raiz:

   ```
   dc=security,dc=com
   ```

   Anote o número da porta para referência futura.
2. Importe o arquivo NeteAuto.ldif no servidor de diretórios de samples\NeteAuto em Ferramentas administrativas.

   As Ferramentas administrativas são instaladas nos seguintes locais padrão:
   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools

Observação: se você tiver problemas ao importar o arquivo LDIF ou criar o diretório do CA Identity Manager, adicione o seguinte texto ao início do arquivo LDIF:

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

Salve o arquivo e repita as etapas 1 e 2.

Configurar um banco de dados relacional

Execute o procedimento a seguir para configurar um banco de dados relacional.

Siga estas etapas:

1. Crie uma instância do banco de dados denominada NeteAuto.
2. Crie um usuário chamado neteautoadmin com a senha test. Conceda direitos neteautoadmin (como direitos db_owner e públicos) para NeteAuto editando as propriedades do usuário.

   Observação: para criar um banco de dados NeteAuto, a função neteautoadmin função deve ter pelo menos permissões mínimas (selecionar, inserir, atualizar e excluir) para todas as tabelas criadas pelo script by.sql. Além disso, neteautoadmin deve poder executar todos os procedimentos armazenados, se houver, definidos nesses scripts.
3. Quando você edita as propriedades do usuário, torna NeteAuto o banco de dados padrão para neteautoadmin.
4. Execute os scripts a seguir na ordem em que estão listados:
   - *db_type*-rdbuserdirectory.sql — configura as tabelas para a amostra NeteAuto e cria as entradas de usuário.
   - ims_*db_type*_rdb.sql — configura o suporte para organizações

     db_type

     Define o Microsoft SQL ou Oracle, dependendo do tipo de banco de dados que você está configurando.

   Esses arquivos de script estão localizados na pasta *ferramentas_administrativas*\samples\NeteAutoRDB\Organization. Neste exemplo, *ferramentas_administrativas* refere-se às Ferramentas administrativas, que são instaladas nos seguintes locais padrão:

   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools
5. Defina uma origem de dados JDBC chamado neteautoDS que aponte para o banco de dados NeteAuto.

   O procedimento para configurar uma origem de dados depende do tipo de servidor de aplicativos em que o CA Identity Manager está instalado. A seção Como criar uma origem de dados JDBC (na página 107) inclui instruções específicas de servidor de aplicativos para criação de uma origem de dados JDBC.

Criar o diretório do CA Identity Manager

Execute o seguinte procedimento para criar um diretório do CA Identity Manager.

Siga estas etapas:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   http://*servidor_do_im:porta*/iam/immanage

   servidor_do_im

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.

   porta

   Define o número da porta do servidor de aplicativos.

2. Clique em Directories.
3. Clique em Create from Wizard para iniciar o assistente de diretório do CA Identity Manager.
4. Procure o arquivo .xml de configuração de diretório apropriado e clique em Next.

   O arquivo de configuração de diretório está localizado nas seguintes pastas:

   - Para diretórios de usuário do Servidor de diretórios do Sun Java System:

     ferramentas_administrativas\samples\NeteAuto\Organization\directory.xml

   - Para bancos de dados relacionais:

     ferramentas_administrativas\samples\NeteAutoRDB\Organization*tipo_de_db* directory.xml

     ferramentas_administrativas

     Define o local de instalação das Ferramentas administrativas.

     As Ferramentas administrativas são instaladas nos seguintes locais padrão:

     Windows: <caminho_de_instalação>\tools

     UNIX: <caminho_de_instalação2>/tools

     db_type

     Especifica o tipo de banco de dados que você está configurando: Microsoft SQL ou Oracle.

   As informações de status são exibidas na tela Directory Configuration Output.

5. Na segunda página do assistente, forneça os seguintes valores:
   - Servidor de diretórios do Sun Java System

     Nome

     Diretório da NeteAuto

     Descrição

     Amostra do diretório da NeteAuto

     Nome do objeto de conexão

     Usuários da NeteAuto

     Host

     O nome do computador ou endereço IP do sistema onde o repositório de usuários está instalado.

     Porta

     O número da porta do repositório de usuários

     Raiz de pesquisa

     dc=security, dc=com

     Nome de usuário

     O nome do usuário de uma conta que possa acessar o repositório de usuários.

     Senha e Confirmar senha

     Senha da conta de usuário

   - Bancos de dados Oracle e Microsoft SQL Server

     Nome

     Diretório do NeteAutoRDB

     Descrição

     Amostra do diretório da NeteAuto

     Nome do objeto de conexão

     NeteAutoRDB

     Origem de dados JDBC

     neteautoDS

     Nome de usuário

     Neteautoadmin

     Senha

     Test

6. Clique em Avançar.
7. Clique em Finish para sair do assistente.

Criar o ambiente do CA Identity Manager para a NeteAuto

Execute o procedimento a seguir para criar o Ambiente do CA Identity Manager para a NeteAuto.

Siga estas etapas:

1. No Management Console, clique em Environments.
2. Na tela de ambientes do CA Identity Manager, clique em New.

   O assistente de ambientes do CA Identity Manager é exibido.
3. Na primeira página do assistente, insira os valores a seguir:

   Nome do ambiente

   Ambiente da NeteAuto

   Descrição

   Amostra do ambiente

   Alias

   Neteauto

   O alias é adicionado ao URL para acessar o Ambiente do CA Identity Manager. Por exemplo, o URL para acessar o ambiente da neteauto é:

   http://*nome_do_servidor*/iam/im/neteauto

   nome_do_servidor

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado. Por exemplo:

   http://meu_servidor.minha_companhia.org/iam/im/neteauto

   Observação: o alias diferencia maiúsculas e minúsculas.

   Clique em Avançar.
4. Selecione o Diretório do CA Identity Manager a ser associado ao Ambiente que você está criando:

   - Para o Servidor de diretórios do Sun Java System, use o Diretório da NeteAuto.
   - Para banco de dados Microsoft SQL Server ou Oracle, use o Diretório do NeteAutoRDB.

   Clique em Avançar.

5. Configure o suporte para tarefas públicas, como as tarefas de autorregistro e senha esquecida, como se segue:
   a. Digite o alias a seguir para tarefas públicas:

      Neteautopublic

   b. Digite SelfRegUser como a conta de usuário anônimo.
   c. Clique em Validate para exibir o identificador exclusivo do usuário.

   Observação: os usuários não precisam efetuar logon para usar tarefas públicas.
6. Selecione as tarefas e funções a serem criadas para o Ambiente da NeteAuto:
   a. Selecione Import roles from the file.
   b. Vá até um dos seguintes locais:
      - Para um repositório de usuários do Servidor de diretórios do Sun Java System:

        ferramentas_administrativas\samples\NeteAuto\RoleDefinitions.xml
      - Para um repositório de usuários do Microsoft SQL Server:

        ferramentas_administrativas\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml
      - Para um repositório de usuários Oracle:

        ferramentas_administrativas\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

      ferramentas_administrativas refere-se às Ferramentas administrativas, que são instaladas no seguinte local por padrão:

      Windows: <caminho_de_instalação>\tools

      UNIX: <caminho_de_instalação2>/tools

7. Especifique um usuário para servir como o Gerente do sistema para este ambiente e clique em Next:
   a. Digite SuperAdmin no campo System Manager.
   b. Clique em Adicionar.

      O CA Identity Manager adiciona o identificador exclusivo do usuário Superadmin à lista de usuários.
   c. Clique em Avançar.

8. Examine as configurações do ambiente e execute as tarefas a seguir:
   - (Opcional) Clique em Previous para modificar.
   - Clique em Finish para criar o Ambiente do CA Identity Manager com as configurações atuais.

     A tela Environment Configuration Output mostra o andamento da criação do ambiente.
9. Clique em Continue para sair do assistente de ambiente do CA Identity Manager.
10. Inicie o Ambiente do CA Identity Manager.

Assim que você cria o Ambiente da NeteAuto, é possível:

- Criar uma capa para este ambiente do CA Identity Manager (na página 38).
- Acessar o ambiente (na página 36)

Como configurar a amostra da NeteAuto sem suporte à organização

Configurar a amostra da NeteAuto sem o suporte à organização envolve as seguintes etapas:

- Instalar o software de pré-requisito (na página 22)
- Instalar o ambiente de amostra do CA Identity Manager
- Configurar o banco de dados
- Criar uma origem de dados JDBC
- Criar o diretório do CA Identity Manager
- Criar o ambiente do CA Identity Manager para a NeteAuto

Descrição da amostra do ambiente do CA Identity Manager

Para bancos de dados Microsoft SQL Server e Oracle, o CA Identity Manager inclui uma versão do ambiente da NeteAuto ambiente que não inclui organizações. Esse ambiente do CA Identity Manager inclui os três usuários a seguir:

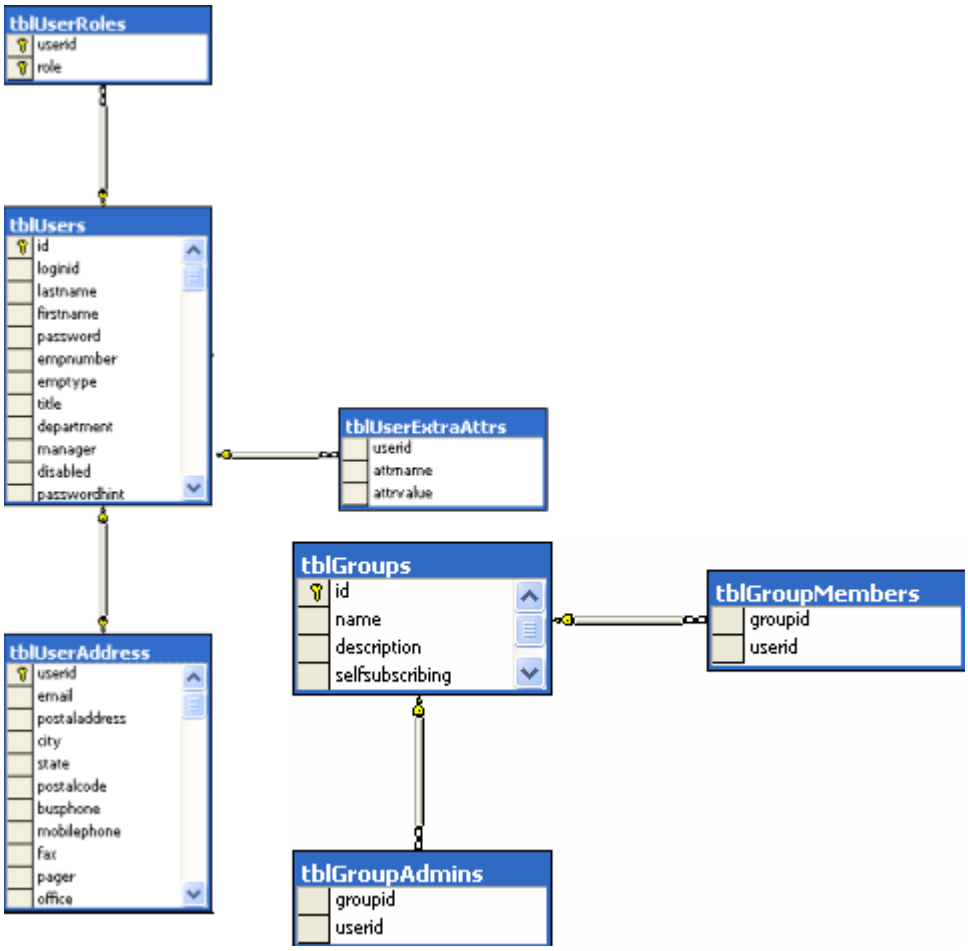
- Superadmin é a conta de administrador com a função Gerente do sistema para esse ambiente do CA Identity Manager. Como Superadmin, você pode executar todas as tarefas administrativas padrão.

  Observação: para obter uma descrição das tarefas administrativas padrão, consulte o *Guia de Administração*.
- SelfRegUser é a conta de administrador que o CA Identity Manager usa para ativar o autorregistro para esse ambiente do CA Identity Manager.

- O Administrador da NeteAuto não tem privilégios quando você instala o ambiente da NeteAuto.

  No entanto, você pode atribuir a função Gerenciador do grupo à conta Administrador da NeteAuto.

A ilustração a seguir descreve a amostra da NeteAuto para um banco de dados relacional, sem organizações:



Arquivos de instalação para o Ambiente da Neteauto

O CA Identity Manager inclui um conjunto de arquivos que podem ser usados para configurar uma amostra do ambiente do CA Identity Manager. Um ambiente do CA Identity Manager é uma exibição de um namespace de gerenciamento que permite aos administradores do CA Identity Manager gerenciar objetos. Esses objetos, como usuários e grupos, estão com um conjunto de funções e tarefas associadas. Um ambiente do CA Identity Manager controla o gerenciamento e a apresentação gráfica de um repositório de usuários.

O ambiente de amostra do CA Identity Manager inclui:

- Amostra de usuários
- Definições de função, tarefa e tela

  As tarefas são exibidas no Console de usuário quando você clica em uma categoria, como usuários ou grupos. As tarefas que são exibidas são baseadas nas funções atribuídas ao usuário.

  Observação: para obter mais informações sobre funções e tarefas, consulte o *Guia de Administração*.
- Uma amostra de capa que personaliza os usuários do Console de usuário para a NeteAuto.
- Um arquivo de configuração de diretório que você usa para criar um diretório do CA Identity Manager.

Os arquivos para criação da amostra do ambiente do CA Identity Manager estão instalados no seguinte local:

ferramentas_administrativas\samples\NeteAutoRDB\NoOrganization

Nesse caminho, *ferramentas_administrativas* se refere às Ferramentas administrativas.

As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Como instalar o Ambiente da NeteAuto — sem suporte à organização

Execute o processo a seguir para instalar o ambiente da NeteAuto.

Siga estas etapas:

1. Verifique se o software de pré-requisito (na página 32) está instalado.
2. Configure o banco de dados (na página 24).
3. Crie o Diretório do CA Identity Manager. (na página 33)
4. Crie o Ambiente do CA Identity Manager para a NeteAuto (na página 34).
5. Configure a aparência da interface do usuário do CA Identity Manager (na página 38) para os usuários da NeteAuto.

Software de pré-requisitos

O ambiente do CA Identity Manager para a NeteAuto tem os seguintes pré-requisitos:

- Instale o CA Identity Manager, conforme descrito no *Guia de Instalação*. Verifique para instalar as Ferramentas administrativas do CA Identity Manager.
- Você deve ter acesso a um banco de dados Microsoft SQL Server ou Oracle.

Configurar um banco de dados relacional

Execute o procedimento a seguir para configurar um banco de dados relacional.

Siga estas etapas:

1. Crie uma instância do banco de dados denominada NeteAuto.
2. Crie um usuário chamado neteautoadmin com a senha test. Conceda direitos neteautoadmin (como direitos db_owner e públicos) para NeteAuto editando as propriedades do usuário.

   Observação: para criar um banco de dados NeteAuto, a função neteautoadmin função deve ter pelo menos permissões mínimas (selecionar, inserir, atualizar e excluir) para todas as tabelas criadas pelo script by.sql. Além disso, neteautoadmin deve poder executar todos os procedimentos armazenados, se houver, definidos nesses scripts.
3. Quando você edita as propriedades do usuário, torna NeteAuto o banco de dados padrão para neteautoadmin.
4. Execute os scripts a seguir na ordem em que estão listados:
   - *db_type*-rdbuserdirectory.sql — configura as tabelas para a amostra NeteAuto e cria as entradas de usuário.
   - ims_*db_type*_rdb.sql — configura o suporte para organizações

     db_type

     Define o Microsoft SQL ou Oracle, dependendo do tipo de banco de dados que você está configurando.

   Esses arquivos de script estão localizados na pasta *ferramentas_administrativas*\samples\NeteAutoRDB\Organization. Neste exemplo, *ferramentas_administrativas* refere-se às Ferramentas administrativas, que são instaladas nos seguintes locais padrão:

   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools

5. Defina uma origem de dados JDBC chamado neteautoDS que aponte para o banco de dados NeteAuto.

   O procedimento para configurar uma origem de dados depende do tipo de servidor de aplicativos em que o CA Identity Manager está instalado. A seção Como criar uma origem de dados JDBC (na página 107) inclui instruções específicas de servidor de aplicativos para criação de uma origem de dados JDBC.

Criar o diretório do CA Identity Manager

Execute o seguinte procedimento para criar o diretório do CA Identity Manager.

Siga estas etapas:

1. Abra o Management Console inserindo o seguinte URL em um navegador:

   http://*servidor_do_im*:*porta*/iam/immanage

   servidor_do_im

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.

   porta

   Define o número da porta do servidor de aplicativos.

2. Clique em Directories.

   A tela de diretórios do CA Identity Manager é exibida.

3. Clique em New para iniciar o assistente de diretório do CA Identity Manager.

4. Procure um dos seguintes arquivos XML de configuração de diretório e clique em Next:

   - Sun Java Systems:

     ferramentas_administrativas\samples\NeteAuto\NoOrganization\directory.xml

   - Bancos de dados do SQL Server:

     ferramentas_administrativas\samples\NeteAuto\NoOrganization\mssql-directory.xml

   - Bancos de dados Oracle:

     ferramentas_administrativas\samples\NeteAuto\NoOrganization\oracle-directory.xml

   ferramentas_administrativas refere-se às Ferramentas administrativas, que são instaladas por padrão no seguinte local:

   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools

   As informações de status são exibidas na tela Directory Configuration Output.

5. Na segunda página do assistente, forneça os seguintes valores:

   Nome

   Diretório do NeteAutoRDB

   Descrição

   Amostra de diretório da NeteAuto sem suporte à organização

   Nome do objeto de conexão

   NeteAutoRDB

   Origem de dados JDBC

   neteautoDS

   Nome de usuário

   neteautoadmin

   Senha

   test

6. Clique em Avançar.
7. Clique em Finish para sair do assistente.

Criar o ambiente do CA Identity Manager para a NeteAuto

Execute o procedimento a seguir para criar o ambiente do CA Identity Manager para a NeteAuto.

Siga estas etapas:

1. No Management Console, clique em Environments.
2. Na tela de ambientes do CA Identity Manager, clique em New.

   O assistente de ambiente do CA Identity Manager é aberto.
3. Na primeira página do assistente, digite os valores a seguir:
   - Nome do ambiente — ambiente da NeteAuto
   - Descrição — NeteAuto é uma amostra de ambiente.

- Alias — neteautoRDB

  O alias é adicionado ao URL para acessar o ambiente do CA Identity Manager. Por exemplo, o URL para acessar o ambiente da neteauto é:

  `http://`*`domínio`*`/iam/im/neteautoRDB`

  Nesse caminho, *domínio* define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado, como no exemplo a seguir:

  `http://meu_servidor.minha_empresa.org/iam/im/neteautoRDB`

  Observação: o alias diferencia maiúsculas e minúsculas.

Clique em Avançar.

4. Selecione o diretório do CA Identity Manager Diretório do NeteAutoRDB a ser associado ao ambiente que está criando e clique em Next.
5. Configure o suporte para tarefas públicas, como as tarefas de autorregistro e senha esquecida.

   Observação: os usuários não precisam efetuar logon para acessar tarefas públicas.

   a. Digite o alias a seguir para tarefas públicas:

      neteautoRDBpublic

   b. Digite SelfRegUser como a conta de usuário anônimo.

   c. Clique em Validate para exibir o identificador exclusivo do usuário (2, neste caso).
6. Selecione as tarefas e funções a serem criadas para o ambiente da NeteAuto:

   - Selecione Import roles from the file.
   - Navegue até o seguinte local:

     dir_ferramentas_administrativas_im\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

     Nesse caminho, *dir_ferramentas_administrativas_im* define o local de instalação das ferramentas administrativas do CA Identity Manager.
7. Especifique um usuário para servir como o Gerente do sistema para esse ambiente e clique em Next:

   a. Digite SuperAdmin no campo System Manager.

   b. Clique em Adicionar.

   c. Clique em Avançar.

8. Examine as configurações do ambiente.
   - Clique em Previous para modificar.
   - Clique em Finish para criar o ambiente do CA Identity Manager com as configurações atuais.

     A tela Environment Configuration Output mostra o andamento da criação do ambiente.
9. Clique em Finish para sair do assistente de ambiente do CA Identity Manager.
10. Inicie o ambiente do CA Identity Manager.

Assim que você cria o ambiente da NeteAuto, é possível:

- Criar uma capa para esse ambiente do CA Identity Manager, conforme descrito em Configurar a capa da NeteAuto (na página 38).
- Acessar o ambiente, conforme descrito em Ambiente do CA Identity Manager para a NeteAuto.

Como usar o ambiente do CA Identity Manager para a NeteAuto

Você pode usar o Ambiente do CA Identity Manager para a NeteAuto para gerenciar as tarefas de autoatendimento e os usuários.

Gerenciamento de tarefas de autoatendimento

As tarefas de autoatendimento incluem:

- Registro como um novo usuário
- Logon como um usuário autorregistrado
- Uso do recurso de senha esquecida

Registro como um novo usuário

Execute o procedimento a seguir para se registrar como um novo usuário.

Siga estas etapas:

1. Digite o seguinte URL no navegador:

   `http://nome_do_host/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   nome do host

   Define o nome de domínio totalmente qualificado do sistema em que o CA Identity Manager está sendo executado.

   Observação: se você não configurou a capa da Neteauto (na página 38), não será possível omitir imcss do URL, como se segue:

   http://*nome_do_host*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

   Esse URL direciona você ao console padrão da ca.

   Na página Self-Registration: End-User License Agreement, o CA Identity Manager exibe o site da CA.

   Observação: é possível configurar a tarefa padrão Autorregistro para exibir o Contrato de Licença do Usuário Final personalizado. Para obter instruções, consulte o *Guia de Administração*.

2. Clique em Aceitar para continuar.
3. Na guia Perfil, forneça os seguintes detalhes:
   a. Digite os valores para os campos obrigatórios, indicados por um asterisco (*).
   b. Digite as dicas e respostas de senha.

      Para o caso de esquecer a senha, o CA Identity Manager fornece a dica de senha e solicita a resposta. Se a resposta estiver correta, o CA Identity Manager solicita que o usuário especifique e confirme uma nova senha.
4. Deixe a guia Grupos inalterada.
5. Clique em Enviar.

Logon como um usuário autorregistrado

Execute o procedimento a seguir para efetuar logon como um usuário autorregistrado.

Siga estas etapas:

1. Digite o seguinte URL para o Ambiente do CA Identity Manager para a NeteAuto em um navegador:

   `http://nome_do_host/iam/im/neteauto/imcss/index.jsp`

   nome do host

   Define o nome de domínio totalmente qualificado do sistema em que o CA Identity Manager está sendo executado.

2. Efetue logon usando o nome de usuário e a senha especificados quando se registrou.

Configurar a capa da NeteAuto

Para configurar a capa da NeteAuto, você cria uma resposta do SiteMinder no Servidor de política do SiteMinder.

Siga estas etapas:

1. Efetue logon em uma das interfaces a seguir como um administrador com privilégios de domínio:

   - No CA SiteMinder Web Access Manager r12 ou superior, efetue logon na Interface de usuário administrativa.
   - No CA eTrust SiteMinder 6.0 SP5, efetue logon na Interface de usuário do servidor de políticas.

   Observação: para obter informações sobre como usar essas interfaces, consulte a documentação da versão do SiteMinder que você está usando.

2. Abra o neteautoDomain.

3. Em neteautoDomain, selecione Realms.

   Os realms a seguir são exibidos:

   neteauto_ims_realm

   Protege o ambiente do CA Identity Manager.

   neteauto_pub_realm

   Ative o suporte para tarefas públicas, como as tarefas de autorregistro e senha esquecida.

4. Crie uma regra em cada um dos realms. Especifique os seguintes detalhes:
   - Recurso: *
   - Ações: GET, POST

   Para simplificar a administração, inclua a capa da NeteAuto no nome da regra.
5. Crie uma resposta para o domínio com os seguintes atributos de resposta:
   - Atributo: WebAgent-HTTP-Header-Variable

     Esse atributo adiciona um novo cabeçalho HTTP à resposta.
   - Tipo de atributo: Estático
   - Nome da variável: capa

     Valor da variável: neteauto
6. Modifique a política que o CA Identity Manager criou no neteautoDomain. Especifique os seguintes detalhes:
   - Usuários
     - Para LDAP: selecione ou=People, ou=Employees, ou=NeteAuto em Integrantes disponíveis e adicione-o aos Integrantes atuais. Clique em OK.
     - Para bancos de dados relacionais: procure usuários com o atributo de identificação igual a *. Selecione todos os usuários em Integrantes disponíveis e adicione-os aos Integrantes Atuais. Clique em OK.
   - Regras:
     - Adicione as regras que você criou na Etapa 4.
     - Para cada regra, clique em Set Response. Associe cada regra à resposta que você criou na Etapa 5.

Observação: a capa da neteauto tem como base o console do imcss. Para exibir a capa, acrescente /imcss/index.jsp ao URL para o Ambiente do CA Identity Manager para a NeteAuto da seguinte maneira:

http://*nome_do_host*/iam/im/neteauto/imcss/index.jsp

Acessar o Ambiente do CA Identity Manager para a NeteAuto (na página 41) fornece instruções completas para acessar o ambiente da NeteAuto.

Uso do recurso de senha esquecida

Execute o procedimento a seguir para usar o recurso de senha esquecida.

Siga estas etapas:

1. Digite o seguinte URL no navegador:

   `http://nome_do_host/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   nome do host

   Define o nome de domínio totalmente qualificado do sistema em que o CA Identity Manager está sendo executado.

2. Digite o identificador exclusivo para o usuário autorregistrado que você criou em Registro como um novo usuário (na página 37) e clique em Avançar.

3. Sempre que for solicitado, responda à pergunta de verificação. A resposta é aquela que você forneceu durante o registro.

   Observação: uma resposta correta é necessária para cada pergunta. O cancelamento da tarefa ou o fechamento do navegador contam como uma tentativa que falhou.

4. Clique em Enviar.

   O CA Identity Manager solicita que você forneça uma nova senha.

Gerenciamento de usuários

O gerenciamento de usuários inclui as seguintes operações:

- Acessar o ambiente do CA Identity Manager para a NeteAuto
- Modificar um usuário
- Atribuir a função Gerenciador do grupo
- Criar um grupo
- Gerenciar usuários autorregistrados

Acessar o Ambiente do CA Identity Manager para a NeteAuto

Execute o procedimento a seguir para acessar o ambiente do CA Identity Manager para a NeteAuto.

Siga estas etapas:

1. Digite o seguinte URL no navegador:

   `http://nome_do_host/iam/im/neteauto/imcss/index.jsp`

   nome do host

   Define o nome de domínio totalmente qualificado, como no exemplo a seguir:

   http://meu_sevidor.minha_empresa.com/iam/im/neteauto/imcss/index.jsp.

   Observação: se você não configurou a capa da Neteauto, será possível usar o seguinte URL para acessar o ambiente da Neteauto:

   http://*nome_do_host*/iam/im/neteauto

2. Na tela de logon, digite as seguintes credenciais:

   Nome de usuário

   SuperAdmin

   Senha

   test

Modificar uma senha

Execute o procedimento a seguir para modificar um usuário.

Siga estas etapas:

1. Efetue logon no ambiente da NeteAuto como SuperAdmin usando a senha test.
2. Selecione Usuários, Gerenciar usuários, Modificar usuário.

   A tela Selecionar usuário é exibida.

3. Clique em Pesquisar.

   O CA Identity Manager exibe uma lista de usuários do ambiente da NeteAuto.

4. Selecione o administrador da NeteAuto, como se segue:

   - Para diretórios LDAP, Administrador da NeteAuto
   - Para bancos de dados relacionais, Admin da NeteAuto

   Clique em Selecionar. O CA Identity Manager exibe o perfil do administrador da NeteAuto.

5. No campo Cargo, digite Gerente. Clique em Enviar.

   O CA Identity Manager confirma o envio da tarefa.

6. Clique em OK para retornar à tela principal.

Atribuir a função Gerenciador do grupo

A atribuição de uma função de gerenciador de grupo é necessária. Execute o procedimento a seguir para atribuir um gerenciador de grupo.

Siga estas etapas:

1. Como SuperAdmin, selecione a guia Funções e tarefas, em seguida, selecione Funções administrativas, Modificar funções administrativas.
2. Selecione uma função Gerenciador do grupo e clique em Selecionar.

   O perfil da função Gerenciador do grupo é exibido.

3. Clique na guia Integrantes e em Adicionar, em Políticas de integrante.

   A tela Política de integrante é exibida.

4. Em Regra de integrante, clique na seta para baixo no campo Usuários.

   Na lista suspensa, selecione com <filtro-de-usuário>.

   O campo Usuários muda para que você insira um filtro para a regra.

5. Insira uma regra de associação, como segue:
   a. No primeiro campo, selecione Cargo na lista suspensa.
   b. No segundo campo, verifique se o sinal de igual (=) está selecionado.
   c. No terceiro campo, digite Gerenciador.
6. Na seção Regras de escopo, defina as regras para usuários, grupos e organizações (quando suportado), como segue:
   a. No campo Usuários, clique na seta para baixo para ver uma lista de opções. Selecione (tudo) da lista.
   b. Repita a Etapa 'a' nos campos Grupo e Organização campos (quando suportado).
   c. Deixe o campo Tarefas de acesso em branco.
7. Clique em OK.

   O CA Identity Manager exibe a política de integrante que você criou.

8. Clique em Enviar.

   O CA Identity Manager confirma o envio da tarefa.

9. Clique em OK para retornar à tela principal.
10. Feche o CA Identity Manager.

Criar um grupo

Execute o procedimento a seguir para criar um grupo.

Siga estas etapas:

1. Efetue logon no CA Identity Manager como o administrador da NeteAuto, como se segue:
   - Para diretórios LDAP, digite o nome de usuário do Administrador da NeteAuto e a senha test.
   - Para bancos de dados relacionais, digite o nome de usuário do Admin da NeteAuto e a senha test.

   A lista de tarefas que o administrador da NeteAuto pode executar é exibida. Como o administrador da NeteAuto pode executar apenas um número limitado de tarefas, o CA Identity Manager lista as tarefas no lugar das categorias.
2. Clique em Criar grupo.
3. Verifique se a opção Criar um grupo está selecionada e clique em OK.
4. Implemente uma das etapas a seguir que seja mais adequada ao seu caso:
   - Se o ambiente da NeteAuto oferecer suporte a organizações:
     a. No campo Nome da organização, clique no símbolo de reticências (...) para selecionar a organização em que o CA Identity Manager cria o grupo.
     b. Na parte inferior da tela Selecionar organização, expanda NeteAuto.
     c. Selecione a organização do revendedor.
   - Se o ambiente da NeteAuto não oferecer suporte às organizações, passe para a próxima etapa.
5. Digite as seguintes informações para o grupo:
   - Nome do grupo: Administradores da revendedora
   - Descrição do grupo: Administradores das concessionárias NeteAuto.
6. Clique na guia Associação e em Adicionar um usuário.

   A tela Selecionar usuário é exibida.
7. Clique em Pesquisar.
8. Selecione o administrador da NeteAuto e clique em Selecionar.
9. Clique em Enviar para criar o grupo.

Gerenciar usuários autorregistrados

Execute o procedimento a seguir quando você desejar gerenciar usuários autorregistrados.

Siga estas etapas:

1. Efetue logon no CA Identity Manager como um administrador da NeteAuto usando as seguintes credenciais:

   - Para diretórios LDAP:

     Nome de usuário

     Administrador da NeteAuto

     Senha

     test

   - Para bancos de dados relacionais:

     Nome de usuário

     Admin da NeteAuto

     Senha

     test

   A lista de tarefas que o administrador da NeteAuto pode executar é exibida no lado esquerdo do Console de usuário. Como o administrador da NeteAuto pode executar apenas um número limitado de tarefas, o CA Identity Manager lista as tarefas no lugar das categorias.

2. Clique em Modificar grupo.
3. Clique em Pesquisar.

   O CA Identity Manager exibe uma lista de grupos.

4. Selecione Dealer Administrator e clique em Selecionar.
5. Clique na guia Associação e em Adicionar um usuário.

   A tela Selecionar usuário é exibida.

6. Clique em Pesquisar.
7. Na tela Pesquisa de usuário, selecione o usuário que você digitou em Registro como um novo usuário (na página 37). Clique em Selecionar.
8. Clique em Enviar.

   O CA Identity Manager confirma o envio da tarefa.

9. Clique em OK para retornar à tela principal.

Para confirmar que o usuário é integrante do grupo criado, use a tarefa Exibir grupo.

Como configurar recursos adicionais

Depois de instalar a amostra da NeteAuto e a funcionalidade básica do CA Identity Manager, use o ambiente da NeteAuto para praticar e testar recursos adicionais do CA Identity Manager, incluindo notificações por email e fluxo de trabalho.

Observação: para obter mais informações sobre esses recursos, consulte o *Guia de Administração*.

Restrição de nome de logon do SiteMinder para nome do usuário global

Se um usuário precisar efetuar logon no Servidor de políticas do SiteMinder, os seguintes caracteres ou sequências de caracteres não poderão fazer parte de um nome de usuário global:

&
*
:
( )

Solução de contorno

Evite usar esses caracteres no nome de usuário global.

Capítulo 3: Gerenciamento de repositório de usuários LDAP

Esta seção contém os seguintes tópicos:

Diretórios do CA Identity Manager

Um *diretório do CA Identity Manager* descreve como os objetos, como usuários, grupos e organizações são armazenados no diretório de usuários e como ele é representado no CA Identity Manager. Um diretório do CA Identity Manager é associado a um ou mais dos ambientes do CA Identity Manager.

Como criar um diretório do CA Identity Manager

Criar um diretório do CA Identity Manager para um repositório de usuários LDAP envolve as seguintes etapas:

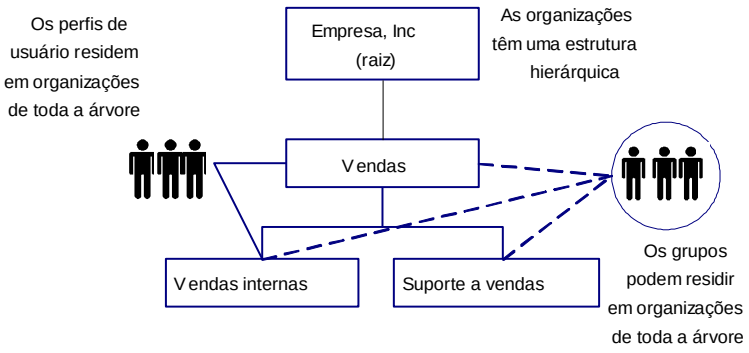
1. Determinar a estrutura de diretório.
2. Descrever os objetos no repositório de usuários modificando um arquivo de configuração de diretório (na página 53) (directory.xml).
3. Importar o arquivo de configuração de diretório e criar o diretório (na página 156).

Observação: ao usar o SiteMinder, verifique se aplicou o esquema do repositório de políticas antes da criação de um Diretório do CA Identity Manager. Para obter mais informações sobre esquemas específicos do repositório de políticas e como aplicá-los, consulte o *Guia de Instalação*.

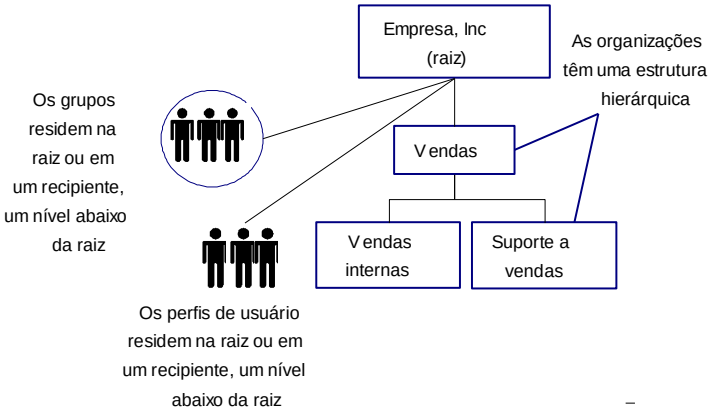
Estrutura de diretório

O CA Identity Manager oferece suporte às seguintes estruturas de diretórios:

- Hierárquica — contém uma organização pai (raiz) e suborganizações. As suborganizações também têm suborganizações, o que cria uma estrutura de vários níveis, como mostrado na ilustração a seguir:

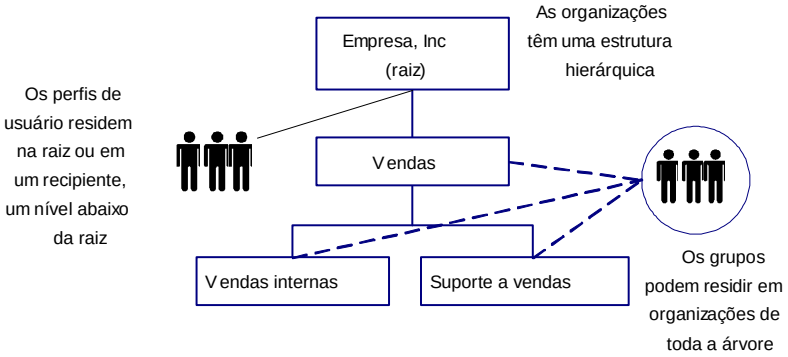


- Simples — usuários e grupos são armazenados na raiz de pesquisa ou em um recipiente um nível abaixo da raiz de pesquisa. As organizações têm uma estrutura hierárquica, como mostrado na ilustração a seguir de uma estrutura de diretório simples:



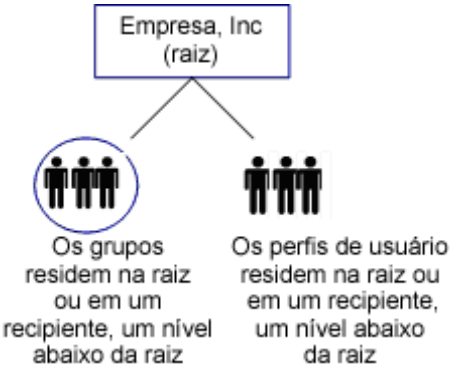
Para facilitar o gerenciamento de usuários e a delegação nas estruturas de diretórios simples, os usuários e grupos pertencem às organizações lógicas. A organização lógica é armazenada como um atributo nos perfis de usuário e grupo.

- Usuário simples — organizações e grupos são armazenados de forma hierárquica, mas os usuários são armazenados na raiz de pesquisa ou em um recipiente um nível abaixo da raiz de pesquisa. A ilustração de uma estrutura de diretório de usuários simples é mostrada no diagrama a seguir:



Em estruturas de diretórios de usuários simples, os usuários pertencem às organizações lógicas. A organização lógica de um usuário é armazenada como um atributo em um perfil de usuário.

- Sem organizações — o diretório não inclui organizações. Os usuários e grupos são armazenados na raiz de pesquisa ou em um recipiente em um nível abaixo da raiz de pesquisa. Uma estrutura de diretório sem organizações é mostrada na ilustração a seguir:



Observação: o diretório pode conter mais de um tipo de estrutura. Por exemplo, os perfis de usuário podem ser armazenados em uma estrutura simples em uma parte do diretório e hierarquicamente em outra. Para oferecer suporte a uma estrutura de diretório híbrida, crie vários ambientes do CA Identity Manager.

Arquivo de configuração de diretório

Para descrever a estrutura de um diretório de usuários do CA Identity Manager, crie um arquivo de configuração de diretório.

O arquivo de configuração de diretório contém um ou mais das seções a seguir:

Informações do diretório do CA Identity Manager

Contém informações sobre o diretório do CA Identity Manager.

Observação: não modifique as informações nesta seção. O CA Identity Manager solicita que você forneça essas informações quando você criar um diretório do CA Identity Manager no Management Console.

Validação de atributo

Define as regras de validação que se aplicam ao diretório do CA Identity Manager.

Informações do provedor

Descreve o repositório de usuários que o CA Identity Manager gerencia.

Informações de pesquisa de diretório

Permite que você especifique como o CA Identity Manager pesquisa o repositório de usuários.

Objeto do usuário

Descreve como os usuários são armazenados no repositório e como eles são representados no CA Identity Manager.

Objeto do grupo

Descreve como os grupos são armazenados no repositório e como eles são representados no CA Identity Manager.

Objeto da organização

Descreve como as organizações são armazenadas e como são representadas no CA Identity Manager. O objeto da organização fornece detalhes somente quando o repositório de usuários inclui organizações.

Objeto com autoinscrição

Configura o suporte para grupos em que os usuários de autoatendimento podem ingressar.

Comportamento de grupos de diretórios

Especifica se o diretório do CA Identity Manager oferece suporte a grupos dinâmicos e aninhados.

Para criar um arquivo de configuração de diretório, modifique um modelo de configuração.

Como selecionar um modelo de configuração de diretório

O CA Identity Manager fornece modelos de configuração de diretório que oferecem suporte a diferentes tipos de estruturas e diretório. Para criar um diretório do CA Identity Manager, modifique o modelo que mais se aproxima da sua estrutura de diretório.

Os modelos descritos na tabela a seguir são instalados com as Ferramentas administrativas:

ferramentas_administrativas\directoryTemplates*tipo_de_diretório*\

As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Os tipos de diretório e os modelos de configuração correspondentes são mostrados na tabela a seguir:

Tipo de diretório	Modelo
Diretório LDAP Active Directory (ADSI) com uma estrutura hierárquica	ActiveDirectory\directory.xml
Diretório Microsoft ADAM com uma estrutura hierárquica	ADAM\directory.xml
Diretório IBM Directory Server com uma estrutura hierárquica	IBMDirectoryServer\directory.xml
Diretório de usuários Novell eDirectory com uma estrutura hierárquica	eDirectory\directory.xml
Diretório Oracle Internet com uma estrutura hierárquica	OracleInternetDirectory\directory.xml
Diretório LDAP do Sun Java System (SunOne ou iPlanet) com uma estrutura hierárquica	IPlanetHierarchical\directory.xml
Diretório LDAP do Sun Java System (SunOne ou iPlanet) com uma estrutura simples	IPlanetFlat\directory.xml
Repositório de usuários do CA Directory com uma estrutura hierárquica	eTrustDirectory\directory.xml
Diretório de provisionamento Esse modelo configura o Diretório de provisionamento de um ambiente do CA Identity Manager. **Observação:** é possível usar esse modelo de configuração do modo que ele foi instalado. Você não precisa modificar esse modelo.	ProvisioningServer\directory.xml
Diretório personalizado	Use o modelo que mais se parece com seu diretório.

Copie o modelo de configuração em um novo diretório ou salve-o com um nome diferente para que ele não seja substituído.

Como descrever um diretório de usuários para o CA Identity Manager

Para gerenciar um diretório, o CA Identity Manager deve compreender a estrutura e o conteúdo de um diretório. Para descrever o diretório ao CA Identity Manager, modifique o arquivo de configuração de diretório (directory.xml) no diretório de modelo apropriado.

O arquivo de configuração de diretório apresenta as seguintes convenções importantes:

- ## — indica valores exigidos.

  Para fornecer todas as informações necessárias, localize todos os sinais de cerquilhas duplas (##) e as substitua por valores apropriados. Por exemplo, ##DISABLED_STATE indica que você deve fornecer um atributo para armazenar o status da conta de um usuário.

- @ — indica os valores preenchidos pelo CA Identity Manager. Não modifique esses valores no arquivo de configuração de diretório. O CA Identity Manager solicita que você forneça os valores quando importa o arquivo de configuração de diretório.

Para modificar o arquivo de configuração de diretório, você precisará das seguintes informações:

- Classes de objetos LDAP para os objetos de usuário, grupo e organização
- Lista de atributos nos perfis de usuário, grupo e organização

Como modificar o arquivo de configuração de diretório

Execute as seguintes etapas para modificar o arquivo de configuração de diretório.

Observação: as etapas necessárias são observadas adequadamente.

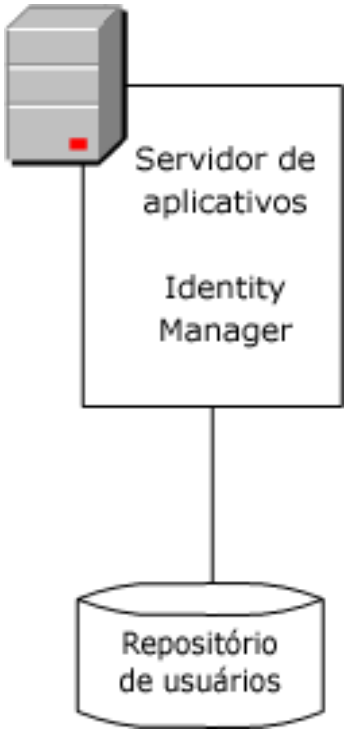
1. Limite o tamanho dos resultados da pesquisa (na página 58).
2. Modifique os objetos padrão gerenciados por usuário, organização ou grupo.
3. Altere as descrições do atributo padrão.
4. Modifique os atributos conhecidos (na página 79). (obrigatório)

   Os atributos conhecidos identificam atributos especiais, como o atributo de senha, no CA Identity Manager.

5. Configure o CA Identity Manager para a sua estrutura de diretório (na página 86) (obrigatório).
6. Permita que usuários se inscrevam em grupos (na página 87).

Conexão com o diretório de usuários

O CA Identity Manager se conecta a um diretório de usuários para armazenar informações, como informações de um usuário, um grupo ou organizacionais, como mostrado na ilustração a seguir:



Não é necessário um novo diretório ou banco de dados. No entanto, o diretório ou banco de dados existente deve estar em um sistema que tenha um FQDN (fully qualified domain name - nome de domínio totalmente qualificado).

Para obter uma lista de tipos de banco de dados e diretório suportados, consulte a matriz de suporte do CA Identity Manager no Site de suporte da CA.

É possível configurar uma conexão com o repositório de usuários quando você cria um diretório do CA Identity Manager no Management Console.

Se você exportar a configuração de diretório após a criação de um diretório do CA Identity Manager, as informações de conexão com o diretório de usuários serão exibidas no elemento Provider do arquivo de configuração de diretório.

Elemento Provider

As informações de configuração são armazenados no elemento Provider e em seus subelementos no arquivo directory.xml.

Observação: se você estiver criando um diretório do CA Identity Manager, não será necessário fornecer informações de conexão no arquivo directory.xml. Forneça informações de conexão no assistente de diretório do CA Identity Manager no Management Console. Modifique o elemento Provider apenas para atualizações.

O elemento Provider inclui os seguintes subelementos:

LDAP

Descreve o diretório de usuários ao qual você está se conectando.

Credentials

Fornece o nome de usuário e a senha para acessar o repositório de usuários LDAP.

Connection

Fornece o nome do host e a porta para o computador onde o repositório de usuários está localizado.

Provisioning Domain

Define o Domínio de provisionamento que o CA Identity Manager gerencia (apenas para usuários do provisionamento).

Um elemento Provider concluído lembra o seguinte código:

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

O elemento Provider inclui os seguintes parâmetros:

type

Especifica o tipo do banco de dados. Para todos os repositórios de usuários LDAP, especifique LDAP (padrão).

userdirectory

Especifica o nome da conexão do diretório de usuários.

Observação: não especifique um nome para a conexão com o diretório de usuários no arquivo directory.xml. O CA Identity Manager solicita que você forneça o nome na criação do diretório do CA Identity Manager no Management Console.

Observação: os parâmetros são opcionais.

Subelemento LDAP

O subelemento LDAP inclui os seguintes parâmetros:

searchroot

Especifica o local em um diretório LDAP que serve como ponto de partida para o diretório. Geralmente, uma organização (o) ou unidade organizacional (ou).

secure

Força uma conexão SSL (Secure Sockets Layer) com o diretório de usuários LDAP, como se segue:

- True — o CA Identity Manager usa uma conexão segura.
- False — o CA Identity Manager se conecta ao diretório de usuários sem SSL (padrão).

Observação: os parâmetros são opcionais.

Subelemento Credentials

Para se conectar a um diretório LDAP, o CA Identity Manager deve fornecer credenciais válidas. As credenciais são definidas no subelemento Credentials, que se parece com o seguinte código:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Se você não especificar uma senha, o subelemento Credentials solicitará a senha quando você criar o diretório do CA Identity Manager no Management Console.

Observação: é recomendável especificar a senha no Management Console.

Ao especificar a senha no Management Console, o CA Identity Manager a criptografará para você. Caso contrário, se você não quiser que a senha seja exibida em texto não criptografado, criptografe a senha usando a ferramenta de senha que é instalada com o CA Identity Manager.

Observação: é possível especificar apenas um conjunto de credenciais. Ao definir vários diretórios, conforme descrito em Subelemento Connection, as credenciais que você especifica deverão se aplicar a todos os diretórios.

O subelemento Credentials inclui os seguintes parâmetros:

user

Especifica a ID de logon de uma conta que pode acessar o diretório.

Para os usuários do provisionamento, a conta de usuário que você especifica deve ter o perfil de Administrador de domínio ou um conjunto equivalente de privilégios no Servidor de provisionamento.

Observação: não especifique um valor para o parâmetro de usuário no arquivo directory.xml. O CA Identity Manager solicita que você forneça a ID de logon criada no Diretório do CA Identity Manager no Management Console.

cleartext

Determina se a senha é exibida em texto não criptografado no arquivo directory.xml, como a seguir:

- True — a senha é exibida em texto não criptografado.
- False — a senha é criptografada (padrão).

Observação: os parâmetros são opcionais.

Subelemento Connection

O subelemento Connection descreve o local do repositório de usuários que o CA Identity Manager gerencia. O subelemento inclui os seguintes parâmetros:

host

Especifica o nome do host ou endereço IP do sistema onde o diretório de usuários está localizado.

Observação: se o sistema de conexão tiver um endereço IPv6, coloque o endereço IP entre colchetes ([ ]), como se segue:

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"

failover="[2::9255:214:22ff:fe72:525a]:20389"/>

port

Especifica o número da porta para o diretório de usuários.

failover

Especifica o nome do host e o endereço IP do sistema onde está o repositório de usuários redundante, caso o sistema principal esteja indisponível. Quando o sistema principal for disponibilizado novamente, o sistema de tolerância a falhas continuará sendo usado. Para voltar a usar o sistema principal, reinicie o sistema secundário. Se vários servidores forem listados, o CA Identity Manager tentará se conectar com os sistemas na ordem listada.

Especifique o nome do host e o endereço IP no atributo de tolerância a falhas em uma lista *separada por espaços*, da seguinte maneira:

failover="IPaddress:port IPaddress:port"

Por exemplo:

<Connection host="123.456.789.001" port="20389"

failover="123.456.789.002:20389 123.456.789.003:20389"/>

Observação: a porta 20389 é a porta padrão do Servidor de provisionamento.

Observação: os parâmetros são opcionais.

Subelemento Provisioning

Se o ambiente do CA Identity Manager incluir provisionamento, defina o Domínio de provisionamento, como se segue:

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

O subelemento Provisioning inclui o seguinte parâmetro:

domain

Define o nome do Domínio de provisionamento que o CA Identity Manager gerencia.

Ao criar o diretório do CA Identity Manager no Management Console, você será solicitado a informar o nome do domínio. Portanto, verifique se especificou um valor para o parâmetro do domínio no arquivo de configuração de diretório (directory.xml).

Parâmetros da pesquisa de diretório

É possível definir os seguintes parâmetros de pesquisa no elemento DirectorySearch:

maxrows

Especifica o número máximo de objetos que o CA Identity Manager pode retornar ao pesquisar um diretório de usuários. Quando o número de objetos exceder o limite, será exibido um erro.

Ao definir um valor para o parâmetro maxrows, é possível substituir as configurações no diretório LDAP que limitam os resultados da pesquisa. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Observação: o parâmetro maxrows não limita o número de objetos que são exibidos em uma tela de tarefas do CA Identity Manager. Para configurar as definições de exibição, modifique a definição da tela de lista no Console de usuário do CA Identity Manager. Para obter instruções, consulte o *Guia de Design do Console de Usuário*.

maxpagesize

Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

Observe os seguintes pontos ao especificar o parâmetro maxpagesize:

- Para usar a opção maxpagesize, o repositório de usuários que o CA Identity Manager gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários exigem configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte Como melhorar o desempenho para pesquisas amplas (na página 97).
- Se o repositório de usuários não oferecer suporte à paginação e um valor para maxrows for especificado, o CA Identity Manager usará apenas o valor de maxrows para controlar o tamanho da pesquisa.

timeout

Determina o número máximo de segundos que o CA Identity Manager pesquisa um diretório antes de encerrar a pesquisa.

Observação: o elemento DirectorySearch é opcional. No entanto, se o diretório oferecer suporte à paginação (na página 97), recomendamos especificar o elemento DirectorySearch.

Mais informações:

Como melhorar o desempenho da pesquisa de diretório (na página 96)
Como melhorar o desempenho de pesquisas amplas (na página 97)

Descrições de objeto gerenciado por usuário, grupo ou organização

Em um CA Identity Manager, é possível gerenciar os seguintes tipos de objeto que correspondem às entradas em um diretório de usuários:

Usuários

Representam os usuários em uma empresa. Um usuário que pertence a uma única organização.

Grupos

Representam as associações de usuários que possuem uma característica em comum.

Organizações

Representam as unidades de negócios. As organizações contém detalhes como usuários, grupos e outras organizações.

Uma descrição do objeto contém as seguintes informações:

- Informações sobre o objeto (na página 116), como a classe de objeto LDAP e o recipiente em que os objetos estão armazenados.
- Os atributos que armazenam informações sobre uma entrada (na página 121). Por exemplo, o atributo de pager armazena um número de pager.

Observação: um ambiente do CA Identity Manager oferece suporte a apenas um tipo de objeto de usuário, grupo e organização. Por exemplo, todos os objetos de usuário possuem a mesma classe de objeto.

Descrições de objeto gerenciado

Um objeto gerenciado é descrito especificando informações do objeto nas seções Objeto de usuário, Objeto de grupo e Objeto de organização do arquivo de configuração de diretório.

Observação: ao usar o modelo de configuração (arquivo directory.xml), a seção Objeto de organização estará indisponível para os diretórios de usuários que não oferecem suporte a organizações.

Cada uma dessas seções contêm os elementos ImsManagedObject, como no exemplo a seguir:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

Como alternativa, o elemento ImsManagedObject pode incluir um elemento Recipiente, como no exemplo a seguir:

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

Especificar informações do objeto

As informações do objeto são especificadas pelo fornecimento de valores para os vários parâmetros.

Siga estas etapas:

1. Localize o elemento ImsManagedObject na seção Objeto de usuário, Objeto de organização ou Objeto de grupo.
2. Forneça valores para os seguintes parâmetros:

   name

   Especifica um nome exclusivo para o objeto gerenciado.

   Observação: esse parâmetro é obrigatório.

   description

   Contém uma descrição do objeto gerenciado.

   objectclass

   Especifica o nome da classe de objeto LDAP para o tipo de objeto (usuário, grupo ou organização). A classe de objeto determina a lista de atributos disponíveis para um objeto.

   Se atributos de várias classes de objeto se aplicarem a um tipo de objeto, liste as classes de objeto em uma lista delimitada por vírgulas. Por exemplo, se um objeto contiver os atributos das classes de objeto person, organizationalperson e inetorgperson, adicione essas classes de objeto da seguinte forma:

   objectclass="top,person,organizationalperson,inetorgperson"

   Cada diretório LDAP inclui um conjunto predefinido de classes de objeto. Consulte a documentação do servidor de diretórios para obter informações sobre as classes de objeto predefinidas.

   Observação: esse parâmetro é obrigatório.

objecttype

Especifica o tipo do objeto gerenciado. Os valores válidos são os seguintes:

- Usuário
- Organização
- Grupo

Observação: esse parâmetro é obrigatório.

maxrows

Especifica o número máximo de objetos que o CA Identity Manager pode retornar ao pesquisar um diretório de usuários. Quando o número de objetos exceder o limite, será exibido um erro.

Ao definir um valor para o parâmetro maxrows, é possível substituir as configurações no diretório LDAP que limitam os resultados da pesquisa. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Observação: o parâmetro maxrows não limita o número de objetos que são exibidos em uma tela de tarefas do CA Identity Manager. Para configurar as definições de exibição, modifique a definição da tela de lista no Console de usuário do CA Identity Manager. Para obter instruções, consulte o *Guia de Design do Console de Usuário*.

maxpagesize

Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

Observe os seguintes pontos ao especificar o tamanho da página de pesquisa:

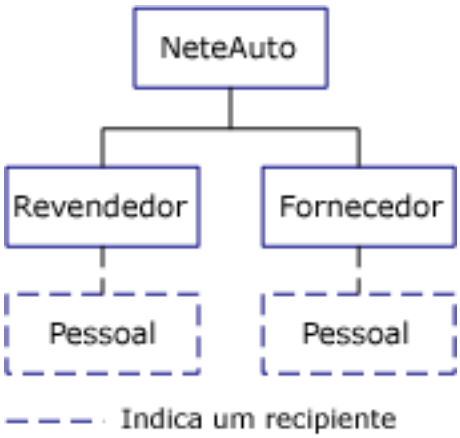
- Para usar a opção Search Page Size, o repositório de usuários que o <idmgr> gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários exigem configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte Como melhorar o desempenho de pesquisa (na página 97).
- Se o repositório de usuários não oferecer suporte à paginação e um valor para maxrows for especificado, o CA Identity Manager usará apenas o valor de maxrows para controlar o tamanho da pesquisa.

3. Se desejar, forneça informações sobre o recipiente.

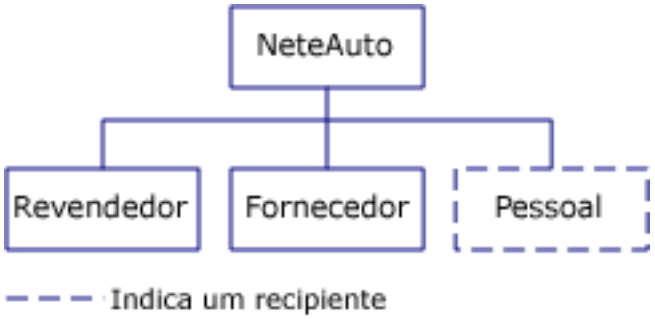
Recipientes

Para simplificar a administração, é possível agrupar objetos de um tipo específico em um recipiente. Ao especificar um recipiente no arquivo de configuração de diretório, o CA Identity Manager gerencia somente entradas do recipiente. Por exemplo, se você especificar um recipiente de usuário denominado People, o CA Identity Manager gerenciará os usuários no recipiente People, como mostrado nas ilustrações a seguir:

- Diretório hierárquico



- Diretório simples



Nesses exemplos, todos os usuários estão nos recipientes People.

Ao especificar um recipiente, observe os seguintes pontos:

- Se não houver nenhum recipiente em uma organização, o CA Identity Manager criará o recipiente assim que a primeira entrada for adicionada. Para um diretório hierárquico, o CA Identity Manager cria o recipiente da organização onde a entrada for adicionada. No caso de diretórios simples e diretórios que não oferecem suporte a organizações, o CA Identity Manager cria o recipiente sob a raiz de pesquisa, que você especifica quando cria o diretório do CA Identity Manager.
- O CA Identity Manager ignora as entradas que não estão no recipiente especificado. Por exemplo, quando você especifica o recipiente People, não é possível gerenciar os usuários existentes fora do recipiente People.

  Observação: para gerenciar os usuários que não são do recipiente especificado, é possível criar outro ambiente do CA Identity Manager.

Recipientes e atributos conhecidos

Os atributos conhecidos são atributos que têm significado especial no CA Identity Manager. Quando o CA Identity Manager gerencia um repositório de usuários, incluindo recipientes, os seguintes atributos conhecidos identificam informações sobre o recipiente:

%ORG_MEMBERSHIP%

Identifica o atributo que armazena o nome completo (DN) do recipiente.

Por exemplo, o nome completo se parece com:

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

%ORG_MEMBERSHIP_NAME%

Identifica o atributo que armazena o nome do atributo amigável ao usuário.

Por exemplo, o nome do recipiente amigável ao usuário no exemplo anterior é People.

Esses atributos conhecidos são exibidos nas descrições de atributo nas seções Objeto de usuário e Objeto de grupo do arquivo directory.xml, como se segue:

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

Para estruturas hierárquicas de repositório de usuários, os parâmetros physicalname e wellknown são mapeados para os atributos conhecidos como se segue:

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

O exemplo indica que o CA Identity Manager deriva automaticamente o DN e o nome amigável ao usuário do recipiente de outras informações no arquivo directory.xml.

Para estruturas de repositório de usuários simples, forneça os nomes dos atributos físicos.

Observação: consulte Como descrever uma estrutura simples de diretório de usuários (na página 87) para obter informações.

Especificar um recipiente de grupo ou usuário

Execute o procedimento a seguir para especificar um recipiente de usuário ou grupo.

Siga estas etapas:

1. Localize o elemento Recipiente na seção Objeto de usuário ou Objeto de grupo.
2. Forneça valores para os seguintes parâmetros:

   objectclass

   Determina a classe de objeto LDAP do recipiente no qual os objetos de um tipo específico são criados. Por exemplo, o valor padrão para o recipiente de usuário é "top,organizationalUnit", que indica que os usuários são criados nas unidades organizacionais (ou) LDAP.

   Quando você estiver gerenciando grupos dinâmicos ou aninhados, certifique-se de especificar uma objectclass que ofereça suporte a esses tipos de grupo (na página 89).

   Observação: esse parâmetro é obrigatório.

   attribute

   Especifica o atributo que armazena o nome do recipiente, por exemplo, ou.

   O atributo é emparelhado com o valor para formar o DN relativo do recipiente, como no exemplo a seguir:

   ou=People

   Observação: esse parâmetro é obrigatório.

   value

   Especifica o nome do recipiente.

   Observação: esse parâmetro é obrigatório.

Observação: não é possível especificar recipientes para organizações.

Descrições do atributo

Um atributo armazena informações sobre uma entrada, como número de telefone ou endereço. Um atributo de entrada determina seu perfil.

No arquivo de configuração de diretório, os atributos são descritos nos elementos ImsManagedObjectAttr. Nas seções Objeto de usuário, Objeto de grupo e Objeto de organização do arquivo de configuração de diretório, você pode executar as seguintes ações:

- Modificar descrições de atributo padrão para descrever os atributos no repositório de usuários.
- Criar novas descrições de atributo copiando uma descrição existente e modificando os valores conforme a necessidade.

Para cada atributo nos perfis de usuário, grupo e organização, há um elemento ImsManagedObjectAttr. Por exemplo, um elemento ImsManagedObjectAttr é descrito como uma ID de usuário.

Um elemento ImsManagedObjectAttr se parece com o seguinte código:

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%" maxlength="0" />
```

O ImsManagedObjectAttr tem os seguintes parâmetros:

physicalname

Esse parâmetro deve conter um dos seguintes itens:

- O nome do atributo LDAP em que o valor do perfil é armazenado. Por exemplo, a ID de usuário é armazenada no atributo uid no diretório de usuários.

  Observação: para melhorar o desempenho, indexe os atributos LDAP que são usados em consultas de pesquisa no Console de usuário.

- Um atributo conhecido (na página 79). Quando você fornece um atributo conhecido, o CA Identity Manager calcula o valor automaticamente. Por exemplo, para especificar um atributo conhecido %ORG_MEMBERSHIP%, o CA Identity Manager determina a organização à qual a entrada pertence, com base no DN de uma entrada.

description

Contém a descrição do atributo

displayname

Especifica um nome exclusivo para o atributo.

No Console de usuário, o nome de exibição aparece na lista de atributos que estão disponíveis para adição a uma tela de tarefas. Esse parâmetro é obrigatório.

Observação: não modifique o nome para exibição de um atributo no arquivo de configuração de diretório (directory.xml). Para alterar o nome do atributo em uma tela de tarefas, é possível especificar um rótulo para o atributo na definição da tela da tarefa. Para obter mais informações, consulte o *Guia de Administração*.

valuetype

Especifica o tipo de dados do atributo. Os valores válidos são os seguintes:

Sequência

O valor pode ser qualquer sequência de caracteres.

Esse é o valor padrão.

Inteiro

O valor deve ser um inteiro.

Observação: o tipo inteiro não oferece suporte a números decimais.

Número

O valor deve ser um inteiro. A opção de número oferece suporte a números decimais.

Data

O valor deverá ser uma data válida usando o padrão:

MM/dd/aaaa

ISODate

O valor deverá ser uma data válida usando o padrão aaaa-MM-dd.

UnicenterDate

O valor deverá ser uma data válida usando o padrão AAAAAAADDD onde:

AAAAAAA é uma representação de sete números para um ano que começa com três zeros. Por exemplo: 0002008

DDD é a representação de três números para o dia que começa com zeros, conforme a necessidade. Os valores válidos variam de 001 a 366.

Estruturado

Este tipo de atributo consiste em dados estruturados que permitem que um único valor de atributo armazene vários valores relacionados. Por exemplo, um atributo estruturado contém valores como Nome, Sobrenome e Endereço de email.

Determinados tipos de terminal usam esses atributos, mas são gerenciados pelo CA Identity Manager.

Observação: o CA Identity Manager pode exibir atributos estruturados em uma tabela no Console de usuário. Quando os usuários editam os valores na tabela, os valores são guardados no repositório de usuários, propagando-se de volta ao terminal. Para obter mais informações sobre a exibição de atributos com valores múltiplos, consulte o *Guia de Administração*.

required

Indica se o atributo é obrigatório, como se segue:

- True — o atributo é obrigatório.
- False — o atributo é opcional (padrão).

Observação: se um atributo for obrigatório para um servidor de diretórios LDAP, defina o parâmetro obrigatório como verdadeiro.

multivalued

Indica se o atributo pode ter valores múltiplos. Por exemplo, o atributo de associação de grupo é de valor múltiplo para armazenar o DN do usuário de cada integrante do grupo. Os valores válidos são os seguintes:

- True — o atributo pode ter valores múltiplos.
- False — o atributo pode ter somente um único valor (padrão).

Importante: os atributos Associação ao grupo e Funções administrativas na definição Objeto de usuário devem possuir valores múltiplos.

wellknown

Define o nome do atributo conhecido.

Os atributos conhecidos têm um significado específico no CA Identity Manager (na página 79). Eles são identificados na sintaxe:

%ATTRIBUTENAME%

maxlength

Define o comprimento máximo que um valor de um atributo pode ter. Defina o parâmetro maxlength como 0 para especificar um comprimento ilimitado.

Observação: esse parâmetro é obrigatório.

permission

Indica se o valor de um atributo pode ser modificado em uma tela de tarefas. Os valores válidos são os seguintes:

READONLY

O valor é exibido, mas não pode ser modificado.

WRITEONCE

O valor não poderá ser modificado depois que o objeto for criado. Por exemplo, uma ID de usuário não pode ser alterada após a criação do usuário.

READWRITE

O valor pode ser modificado (padrão).

hidden

Indica se um atributo é exibido nos formulários de tarefa do CA Identity Manager. Os valores válidos são os seguintes:

- True — o atributo não é exibido para os usuários.
- False — o atributo é exibido para os usuários (padrão).

Os atributos lógicos usam atributos ocultos.

Observação: para obter mais informações, consulte o *Guia de Programação do Java*.

system

Especifica apenas atributos usados do CA Identity Manager. Os usuários no Console de usuário não podem modificar os atributos. Os valores válidos são os seguintes:

- True — os usuários não podem modificar o atributo. O atributo fica oculto na interface de usuário do CA Identity Manager.
- False — os usuários podem modificar esse atributo. O atributo está disponível para adição às telas de tarefas na interface de usuário do CA Identity Manager. (padrão)

validationruleset

Associa um conjunto de regras de validação ao atributo.

Verifique se o conjunto de regras de validação que você especifica está definido em uma elemento ValidationRuleSet no arquivo de configuração de diretório.

objectclass

Indica a classe auxiliar LDAP para um atributo de usuário, grupo ou empresa quando o atributo não faz parte da objectclass principal especificada no elemento ImsManagedObject.

Por exemplo, suponha que a classe de objeto principal para usuários seja top, person e organizationalperson, que define os seguintes atributos de usuário:

- common name (cn)
- surname (sn)
- user id (uid)
- password (userPassword)

Para incluir o atributo employeeID, que é definido na classe auxiliar Employee, você deve adicionar a seguinte descrição de atributo:

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

Especificar descrições de atributo

A descrição de atributos envolve as seguintes etapas:

1. Ler as seções relevantes entre os seguintes tópicos:
   - Considerações sobre o CA Directory (na página 77)
   - Considerações sobre o Microsoft Active Directory (na página 78)
   - Considerações sobre o IBM Directory Server (na página 78)
   - Considerações sobre o Oracle Internet Directory (na página 79)
2. Nas seções Objeto de usuário, Objeto de grupo e Objeto de organização do arquivo de configuração de diretório, execute as seguintes ações:
   - Modificar descrições de atributo padrão para descrever os atributos de diretório.
   - Criar novas descrições de atributo copiando uma descrição existente e modificando os valores conforme a necessidade.

   Observação: suponha que uma nova descrição de atributo seja criada e um atributo físico seja especificado. Certifique-se de que o atributo físico deve existir na classe (ou nas classes) de objeto que você especificou para o tipo de objeto.
3. (Opcional) Altere as configurações de exibição (na página 74) do atributo para evitar a exibição de informações confidenciais, como senhas ou salários, no Console de usuário.
4. (Opcional) Configure uma ordem de classificação padrão.
5. Se estiver gerenciando um diretório com uma estrutura Simples ou Usuário simples, ou um diretório que exclui organizações, vá para Descrever a estrutura de diretório de usuários (na página 86).

Gerenciando atributos confidenciais

O CA Identity Manager oferece os seguintes métodos para gerenciamento de atributos confidenciais:

- Classificações de dados para atributos

  As classificações de dados permitem especificar as propriedades de exibição e criptografia para atributos no arquivo de configuração de diretório (directory.xml).

  Você pode definir as classificações de dados que gerenciam atributos confidenciais, como se segue:

  - Nas telas de tarefa do CA Identity Manager, exiba o valor de um atributo como uma série de asteriscos.

    Por exemplo, é possível exibir as senhas como asteriscos, em vez de exibi-las em texto não criptografado.

  - Nas telas Exibir tarefas enviadas, oculte o valor do atributo.

    Essa opção permite ocultar os atributos dos administradores. Por exemplo, ocultar os detalhes de salário, como o salário de administradores que exibirem o status da tarefa no CA Identity Manager, mas que não precisam exibir os detalhes de salário.

  - Ignore determinados atributos ao criar uma cópia de um objeto existente.
  - Criptografe um atributo

- Estilos de campo nas telas de perfil de tarefa

  Se não desejar modificar um atributo no arquivo directory.xml, defina a propriedade de exibição para o atributo nas definições de tela onde o atributo confidencial aparece.

  O estilo de campo permite exibir atributos, como senhas, como uma série de asteriscos em vez de texto não criptografado.

  Observação: para obter mais informações sobre o estilo de campo para atributos confidenciais, procure estilos de campo na ajuda do Console de usuário.

Atributos de classificação de dados

O elemento Classificação de dados fornece um meio de associar as propriedades adicionais a uma descrição do atributo. Os valores nesse elemento determinam como o CA Identity Manager trata o atributo. Esse elemento oferece suporte aos seguintes parâmetros:

- sensitive

  Faz com que o CA Identity Manager exiba o atributo como uma série de asteriscos (*) nas telas Exibir tarefas enviadas. Esse parâmetro evita que valores novos e antigos do atributo apareçam em texto não criptografado nas telas Exibir tarefas enviadas.

  Além disso, se você criar uma cópia de um usuário existente no Console de usuário, esse parâmetro evitará que o atributo seja copiado para o novo usuário.

- vst_hide

  Oculta o atributo na tela Detalhes do evento para a guia Exibir tarefas enviadas. Ao contrário dos atributos confidenciais, que são exibidos como asteriscos, os atributos vst_hidden não são exibidos.

  É possível usar esse parâmetro para evitar que alterações em um atributo, como o salário, sejam exibidas em Exibir tarefas enviadas.

- ignore_on_copy

  Faz com que o CA Identity Manager ignore um atributo quando um administrador cria uma cópia de um objeto no Console de usuário. Por exemplo, suponha que você tenha especificado ignore_on_copy para o atributo de senha em um objeto de usuário. Ao copiar um perfil de usuário, o CA Identity Manager não aplica a senha do usuário atual ao novo perfil de usuário.

- AttributeLevelEncrypt

  Criptografa os valores de atributo quando eles são armazenados no repositório de usuários. Se o CA Identity Manager for ativado para o FIPS 140-2, o CA Identity Manager usará a criptografia RC2 ou FIPS 140-2.

  Para obter mais informações sobre suporte ao FIPS 140-2 no CA Identity Manager, consulte o *Guia de Configuração*.

  Os atributos são exibidos em texto não criptografado durante o tempo de execução.

  Observação: para impedir que os atributos apareçam em texto não criptografado nas telas, você também pode adicionar um elemento de classificação de dados confidencial aos atributos criptografados. Para obter mais informações, consulte Como adicionar criptografia em nível de atributo (na página 75).

- PreviouslyEncrypted

  Faz com que o CA Identity Manager detecte e descriptografe todos os valores criptografados no atributo quando ele acessa o objeto no repositório de usuários.

  Você usa essa classificação de dados para descriptografar todos os valores criptografados anteriormente.

  O valor do texto não criptografado é salvo no repositório quando você salva o objeto.

Configurar atributos de classificação de dados

Siga estas etapas:

1. Localize o atributo no arquivo de configuração de diretório.
2. Após a descrição do atributo, adicione o seguinte atributo:

   <DataClassification name="*parameter*">

   parameter

   Representa um dos seguintes parâmetros:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Por exemplo, uma descrição do atributo que inclua o atributo de classificação de dados vst_hide se parece com o código a seguir:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Criptografia em nível de atributo

É possível criptografar um atributo no repositório de usuários especificando uma classificação de dados AttributeLevelEncypt para esse atributo no arquivo de configuração de diretório (directory.xml). Quando a criptografia em nível de atributo é ativada, o CA Identity Manager criptografa o valor do atributo antes de armazená-lo no repositório de usuários. O atributo é exibido como texto não criptografado no Console de usuário.

Observação: para impedir que os atributos apareçam em texto não criptografado nas telas, você também pode adicionar um elemento de classificação de dados confidencial aos atributos criptografados. Para obter mais informações, consulte Como adicionar criptografia em nível de atributo (na página 75).

Se o suporte ao FIPS 140-2 for ativado, o atributo será criptografado usando a criptografia RC2 ou FIPS 140-2.

Antes de implementar a criptografia em nível de atributo, observe o seguinte:

- O CA Identity Manager não pode localizar atributos criptografados em uma pesquisa.

  Suponha que um atributo criptografado seja adicionado a uma política de integrante, administrador, proprietário ou identidade. O CA Identity Manager não pode resolver a política corretamente porque não pode pesquisar o atributo.

  Considere a definição do atributo para searchable="false" no arquivo directory.xml. Por exemplo:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Se o CA Identity Manager usa um repositório de usuários compartilhado e o Diretório de provisionamento, não criptografe os atributos do Servidor de provisionamento.
- Não ative AttributeLevelEncrypt para senhas de usuário em ambientes que atendam aos seguintes critérios:
  - Inclua a integração do CA SiteMinder e
  - Armazene usuários em um banco de dados relacional.

  Quando o CA Identity Manager se integra ao CA SiteMinder, as senhas criptografadas podem provocar problemas quando novos usuários tentam efetuar logon e inserem senhas em texto não criptografado.
- Se você ativar a criptografia em nível de atributo para um repositório de usuários que é usado por aplicativos diferentes do CA Identity Manager, os outros aplicativos não poderão usar o atributo criptografado.

Como adicionar criptografia em nível de atributo

Suponha que você tenha adicionado uma criptografia em nível de atributo a um diretório do CA Identity Manager. O CA Identity Manager criptografa automaticamente os valores de atributo de texto não criptografado existentes quando você salva o objeto que é associado ao atributo. Por exemplo, a criptografia do atributo de senha criptografa a senha quando o perfil do usuário é salvo.

Observação: para criptografar o valor do atributo, a tarefa que você usa para salvar o objeto deve incluir o atributo. Para criptografar o atributo de senha no exemplo anterior, certifique-se de que o campo da senha seja adicionado à tarefa que você usa para salvar o objeto, como a tarefa Modificar usuário.

Todos os novos objetos são criados com valores criptografados no repositório de usuários.

Siga estas etapas:

1. Execute uma das tarefas a seguir:
   - Crie um diretório do CA Identity Manager
   - Atualize um diretório existente exportando as configurações de diretório.
2. Adicione os seguintes atributos de classificação de dados ao atributo que deseja criptografar no arquivo directory.xml:

   AttributeLevelEncrypt

   Persiste o valor do atributo em uma forma criptografada no repositório de usuários.

   sensitive (opcional)

   Oculta o valor do atributo em telas do CA Identity Manager. Por exemplo, uma senha é exibida como asteriscos (*).

   Por exemplo:

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Se você criou um Diretório do CA Identity Manager, associe-o a um ambiente.
4. Para forçar o CA Identity Manager a criptografar todos os valores imediatamente, modifique todos os objetos usando o Carregador de itens em massa.

   Observação: para obter mais informações sobre o Carregador de itens em massa, consulte o *Guia de Administração*.

Como remover criptografia em nível de atributo

Se você tiver um atributo criptografado no Diretório do CA Identity Manager e ele for armazenado com o valor desse atributo como texto não criptografado, será possível remover a classificação de dados AttributeLevelEncrypt.

Depois que a classificação de dados tiver sido removida, o CA Identity Manager interromperá a criptografia dos novos valores de atributos. Os valores existentes são descriptografados quando você salva o objeto associado ao atributo.

Observação: para descriptografar o valor do atributo, a tarefa que você usa para salvar o objeto deve incluir o atributo. Por exemplo, para descriptografar uma senha de um usuário existente, você salva o objeto de usuário com uma tarefa que inclui o campo de senha, como a tarefa Modificar usuário.

Para forçar o CA Identity Manager a detectar e descriptografar todos os valores criptografados que permanecem no repositório de usuários do atributo, é possível especificar outra classificação de dados, PreviouslyEncrypted. O valor do texto não criptografado é salvo no repositório de usuários quando você salva o objeto.

Observação: adicionar a classificação de dados PreviouslyEncrypted adiciona mais processamento em cada carga de objeto. Para evitar problemas de desempenho, considere a adição da classificação de dados PreviouslyEncrypted, carregando e salvando cada objeto associado a esse atributo e, em seguida, removendo a classificação de dados. Esse método converte automaticamente todos os valores criptografados armazenados em texto não criptografado armazenado.

Siga estas etapas:

1. Exporte as configurações de diretório para o Diretório adequado do CA Identity Manager.
2. No arquivo directory.xml, remova a classificação de dados, AttributeLevelEncrypt, de atributos que deseja descriptografar.
3. Se quiser forçar o CA Identity Manager a remover valores criptografados anteriormente, adicione o atributo de classificação de dados PreviouslyEncrypted.

   Por exemplo:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Para forçar o CA Identity Manager a descriptografar todos os valores imediatamente, modifique todos os objetos usando o Carregador de itens em massa.

   Observação: para obter mais informações sobre o Carregador de itens em massa, consulte o *Guia de Administração*.

Considerações sobre o CA Directory

Ao descrever atributos de um repositório de usuários do CA Directory, observe os seguintes pontos:

- Os nomes de atributo diferenciam maiúsculas de minúsculas.
- Usar o atributo seeAlso como o atributo que indica um grupo com autoinscrição pode causar erros quando os administradores criam grupos.

Usar o atributo de foto como o atributo que indica o status de uma conta de usuário (ativada ou desativada) pode causar erros quando um administrador cria um usuário.

Observação: para obter mais informações sobre os requisitos do CA Directory, consulte a documentação do CA Directory.

Considerações sobre o Microsoft Active Directory

Ao descrever atributos do Active Directory, observe os seguintes pontos:

- O caso dos atributos especificados em descrições de atributo devem corresponder ao caso dos atributos no Active Directory. Por exemplo, quando você seleciona o atributo unicodePwd como o atributo para armazenar senhas de usuários, especifique o unicodePwd (com uma letra maiúscula P) no arquivo de configuração de diretório.
- Para objetos de usuário e grupo, lembre-se de incluir o atributo sAMAccountName.

Considerações sobre o IBM Directory Server

Ao descrever atributos para um diretório de usuários do IBM Directory Server, consulte as seções a seguir:

- Grupos nos diretórios do Servidor de diretórios (na página 78)
- A objectclass "Top" na Descrição do objeto de organização (na página 79)

Grupos nos diretórios do Servidor de diretórios

O IBM Directory Server exige grupos para conter pelo menos um integrante. Para atender a esse requisito, o CA Identity Manager adiciona um *usuário fictício*, como um integrante de um novo grupo quando o grupo é criado.

Configurar um usuário fictício

Siga estas etapas:

1. Na seção Objeto de grupo do arquivo de configuração de diretório, localize os seguintes elementos:

   ```
   <PropertyDict name="DUMMY_USER">
       <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
   </PropertyDict>
   ```

   Observação: se esses elementos não existirem no arquivo de configuração de diretório, adicione-os exatamente como eles aparecem aqui.

2. Substitua ##DUMMY_USER_DN por um DN de usuário. O CA Identity Manager adiciona esse DN como um integrante de todos os novos grupos.

   Observação: se você especificar o DN de um usuário existente, esse usuário aparecerá como um integrante de todos os grupos do CA Identity Manager. Para evitar que o *usuário fictício* seja exibido como um integrante do grupo, especifique um DN que não existe no diretório.

3. Salve o arquivo de configuração de diretório.

A objectclass Top na Descrição do objeto de organização

Importante: na descrição do objeto de organização no arquivo de configuração de diretório, não inclua a objectclass top.

Por exemplo, quando a objectclass do objeto de organização for top, organizationalUnit, especifique a objectclass da seguinte maneira:

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

A inclusão de top pode causar resultados de pesquisa imprevisíveis.

Considerações sobre o Oracle Internet Directory

Ao descrever atributos para um repositório de usuários OID (Oracle Internet Directory), especifique atributos LDAP usando apenas letras minúsculas.

Atributos conhecidos para um repositório de usuários LDAP

Os atributos conhecidos têm um significado especial no CA Identity Manager. Eles são identificados como mostrado na seguinte sintaxe:

%ATTRIBUTENAME%

Nessa sintaxe, *ATTRIBUTENAME* deve ter letras maiúsculas.

Um atributo conhecido é mapeado para um atributo físico usando uma descrição de atributo (na página 121).

Na descrição de atributo a seguir, o atributo userpassword é mapeado para o atributo conhecido %PASSWORD% para que o CA Identity Manager trate o valor em userpassword como uma senha da seguinte maneira:

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Alguns atributos conhecidos são obrigatórios; outros são opcionais.

Atributos conhecidos de usuário

Veja uma lista de atributos conhecidos de usuário e os itens para os quais eles são mapeados:

%ADMIN_ROLE_CONSTRAINT%

Mapeado para a lista de funções administrativas de um administrador.

O atributo físico mapeado para %ADMIN_ROLE_CONSTRAINT% deve possuir valores múltiplos para acomodar várias funções.

Aconselhamos a indexação do atributo LDAP que é mapeado para %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

Mapeado para o status de certificação de um usuário.

Esse atributo é necessário para usar o recurso de certificação de usuário.

Observação: para obter mais informações sobre a certificação de usuário, consulte o *Guia de Administração*.

%DELEGATORS%

Mapeia para uma lista de usuários que delegou itens de trabalho ao usuário atual.

Esse atributo é exigido para usar a delegação. O atributo físico mapeado para %DELEGATORS% deve possuir valores múltiplos e ser capaz de manter as sequências de caracteres.

Importante: Editar esse campo diretamente usando as tarefas ou uma ferramenta externa do CA Identity Manager pode causar implicações de segurança significativas.

%EMAIL%

Mapeado para um endereço de email de um usuário.

Necessário para usar o recurso de notificação por email.

%ENABLED_STATE%

(obrigatório)

Mapeado para o status de um usuário.

Observação: esse atributo deve corresponder ao atributo de diretório de usuários Sinalizador desativado na conexão do diretório de usuários do SiteMinder.

%FIRST_NAME%

Mapeado para o nome de um usuário.

%FULL_NAME%

Mapeado para o nome e sobrenome de um usuário.

%IDENTITY_POLICY%

Especifica a lista de políticas de identidade que foram aplicadas a uma conta de usuário e uma lista de IDs exclusivas da política Policy Xpress que executaram ações de adição ou remoção no objeto de usuário.

O CA Identity Manager usa esse atributo para determinar se aplicar uma política de identidade a um usuário é obrigatório ou não. Suponha que a política tenha a configuração Aplicar uma vez ativada e a política esteja listada no atributo %IDENTITY_POLICY%. O CA Identity Manager não se aplica às alterações na política para o usuário.

Observação: para obter mais informações sobre políticas de identidade, consulte o *Guia de Administração*.

%LAST_CERTIFIED_DATE%

Mapeado para a data quando as funções são certificadas para um usuário.

Necessário para usar o recurso de certificação de usuário.

Observação: para obter mais informações sobre a certificação de usuário, consulte o *Guia de Administração*.

%LAST_NAME%

Mapeado para o sobrenome de um usuário.

%MEMBER_OF%

Mapeado para a lista de grupos dos quais o usuário é um integrante.

O atributo físico mapeado para %MEMBER_OF% deve possuir valores múltiplos para acomodar vários grupos.

O uso desse atributo melhora o tempo de resposta ao pesquisar grupos de um usuário.

Você pode usar esse atributo com o Active Directory ou qualquer esquema de diretórios que mantenha a associação ao grupo de um usuário no objeto de usuário.

%ORG_MEMBERSHIP%

(obrigatório)

Mapeado para o DN da organização à qual o usuário pertence.

O CA Identity Manager usa esse atributo conhecido para determinar a estrutura de um diretório (na página 86).

Esse atributo não é obrigatório quando o diretório de usuários não inclui organizações.

%ORG_MEMBERSHIP_NAME%

(obrigatório)

Mapeado para o nome amigável ao usuário da organização na qual o perfil do usuário reside.

Esse atributo não é obrigatório quando o diretório de usuários não inclui organizações.

%PASSWORD%

Mapeado para a senha de um usuário.

Esse atributo deve corresponder ao atributo de senha na conexão com o diretório de usuários do SiteMinder.

Observação: o valor do atributo %PASSWORD% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%PASSWORD_DATA%

(Necessário para suporte à política de senha)

Especifica o atributo que rastreia as informações da política de senha.

Observação: o valor do atributo %PASSWORD_DATA% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%PASSWORD_HINT%

(obrigatório)

Mapeado para um par de pergunta e resposta especificado por um usuário. O par de pergunta e resposta é usado quando os usuários esquecem suas senhas.

Para oferecer suporte a vários pares de pergunta e resposta, certifique-se de que o atributo %PASSWORD_HINT% tenha valores múltiplos.

Se estiver usando o recurso Serviços de senha do SiteMinder para gerenciar senhas, o atributo Dica de senha deve corresponder ao atributo Desafio/resposta no diretório de usuários do SiteMinder.

Observação: o valor do atributo %PASSWORD% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%USER_ID%

(obrigatório)

Mapeado para a ID de um usuário.

Atributos conhecidos de grupo

Os itens a seguir compõem a lista de atributos conhecidos de grupo:

%GROUP_ADMIN_GROUP%

Indica qual atributo armazena uma lista de grupos que são administradores do grupo. Por exemplo, quando o grupo 1 for um administrador do grupo A, o grupo 1 será armazenado no atributo %GROUP_ADMIN_GROUP%.

Observação: se você não especificar um atributo %GROUP_ADMIN_GROUP%, o CA Identity Manager armazenará grupos de administradores no atributo %GROUP_ADMIN%.

Observação: para adicionar um grupo como um administrador de outro grupo, consulte o *Guia de Administração*.

%GROUP_ADMIN%

Indica qual atributo contém os DNs de administradores de um grupo.

O atributo físico mapeado para %GROUP_ADMIN% deve possuir valores múltiplos.

%GROUP_DESC%

Indica qual atributo contém a descrição de um grupo.

%GROUP_MEMBERSHIP%

(obrigatório)

Indica qual atributo contém uma lista dos integrantes de um grupo.

O atributo físico mapeado para %GROUP_MEMBERSHIP% deve possuir valores múltiplos.

O atributo conhecido %GROUP_MEMBERSHIP% não é obrigatório para diretórios de Usuários de provisionamento.

%GROUP_NAME%

(obrigatório)

Indica qual atributo armazena um nome de grupo.

%ORG_MEMBERSHIP%

(obrigatório)

Indica qual atributo contém o DN da organização à qual o grupo pertence.

O CA Identity Manager usa esse atributo conhecido para determinar a estrutura do diretório (na página 86).

Esse atributo não é obrigatório quando o diretório de usuários não inclui organizações.

%ORG_MEMBERSHIP_NAME%

Indica qual atributo contém o nome amigável de usuário da organização na qual o grupo existe.

Esse atributo não é válido para diretórios de usuários que não incluam organizações.

%SELF_SUBSCRIBING%

Indica qual atributo determina se os usuários podem se inscrever em um grupo (na página 86).

%NESTED_GROUP_MEMBERSHIP%

Indica qual atributo armazena uma lista de grupos que são integrantes do grupo. Por exemplo, quando um grupo 1 for um integrante do grupo A, o grupo 1 será armazenado no atributo %NESTED_GROUP_MEMBERSHIP%.

Se você não especificar um atributo %NESTED_GROUP_MEMBERSHIP%, o CA Identity Manager armazenará grupos aninhados no atributo %GROUP_MEMBERSHIP%.

Para incluir grupos como integrantes de outros grupos, configure o suporte para grupos aninhados, conforme descrito em Configurando grupos dinâmicos e aninhados para obter instruções.

%DYNAMIC_GROUP_MEMBERSHIP%

Indica qual atributo armazena a consulta LDAP que gera um grupo dinâmico (na página 146).

Observação: para estender os atributos disponíveis do Objeto de grupo para incluir os atributos %NESTED_GROUP_MEMBERSHIP% e %DYNAMIC_GROUP_MEMBERSHIP%, é possível usar classes de objeto auxiliares.

Atributos conhecidos de organização

Os atributos conhecidos a seguir aplicam-se apenas a ambientes que oferecem suporte às organizações:

%ORG_DESCR%

Indica qual atributo contém a descrição de uma organização.

%ORG_MEMBERSHIP%

(obrigatório)

Indica qual atributo contém o DN da organização pai de uma organização.

%ORG_MEMBERSHIP_NAME%

Indica qual atributo contém o nome amigável ao usuário da organização pai de uma organização.

%ORG_NAME%

(obrigatório)

Indica qual atributo contém o nome da organização.

Atributo %ADMIN_ROLE_CONSTRAINT%

Ao criar uma função administrativa, você especifica uma ou mais regras de associação da função. Os usuários que atendem às regras de associação recebem a função. Por exemplo, quando a regra de associação para a função Gerenciador de usuários for title=User Manager, os usuários que possuírem o cargo Gerenciador de usuários terão a função Gerenciador de usuários.

Observação: para obter mais informações sobre regras, consulte o *Guia de Administração*.

%ADMIN_ROLE_CONSTRAINT% permite que você designe um atributo de perfil para armazenar as funções administrativas de um administrador.

Como usar o atributo %ADMIN_ROLE_CONSTRAINT%

Para usar %ADMIN_ROLE_CONSTRAINT% como a restrição para todas as funções administrativas, execute as seguintes tarefas:

- Emparelhe o atributo conhecido %ADMIN_ROLE_CONSTRAINT% com um atributo de perfil de valor múltiplo para acomodar várias funções.
- Quando você configura uma função administrativa no Console de usuário, verifique a seguinte restrição:

  `Funções administrativas igual a` *`nome da função`*

  nome da função

  Define o nome da função para a qual você está fornecendo a restrição, como no exemplo a seguir:

  `Funções administrativas igual a Gerenciador de usuários`

Observação: Funções administrativas é o nome para exibição padrão do atributo %ADMIN_ROLE_CONSTRAINT%.

Configurar atributos conhecidos

Execute o procedimento a seguir para configurar atributos conhecidos.

Siga estas etapas:

1. No arquivo de configuração de diretório, procure pelo seguinte sinal:

   ##
2. Substitua o valor que começa com ## pelo atributo LDAP apropriado.
3. Repita as Etapas 1 e 2 até que tenha substituído todos os valores necessários.
4. Mapeie os atributos conhecidos opcionais para atributos físicos, conforme a necessidade.
5. Salve o arquivo de configuração de diretório.

Descrever a estrutura de diretório de usuários

O CA Identity Manager usa o atributo conhecido %ORG_MEMBERSHIP% para determinar a estrutura de um diretório de usuários.

O procedimento para descrever a estrutura de diretório de usuários depende do tipo de estrutura do diretório.

Como descrever uma estrutura hierárquica de diretório.

O arquivo de configuração de diretório já está configurado para uma estrutura hierárquica de diretório. Como resultado, não será necessário modificar a descrição do atributo %ORG_MEMBERSHIP%.

Como descrever uma estrutura simples de diretório de usuários

Siga estas etapas:

1. Localize a descrição do atributo %ORG_MEMBERSHIP% na seção Objeto de usuário do arquivo directory.xml.
2. No parâmetro physicalname, substitua %ORG_MEMBERSHIP% pelo nome do atributo que armazena a organização à qual o usuário pertence.

Como descrever uma estrutura simples de diretório

Siga estas etapas:

1. Localize a descrição do atributo %ORG_MEMBERSHIP% na seção Objeto de usuário do arquivo directory.xml.
2. No parâmetro physicalname, substitua %ORG_MEMBERSHIP% pelo nome do atributo que armazena a organização à qual o usuário pertence.
3. Repita a Etapa 1 na seção Objeto do grupo.
4. No parâmetro physicalname, substitua %ORG_MEMBERSHIP% pelo nome do atributo que armazena a organização à qual o grupo pertence.

Como descrever um diretório de usuários que não oferece suporte a organizações

Verifique se não há descrições de objeto ou se atributos conhecidos foram definidos para organizações no directory.xml.

Como configurar grupos

Para configuração, os grupos podem ser divididos da seguinte forma:

- Grupos com autoinscrição
- Grupos dinâmicos e aninhados

Configurar grupos com autoinscrição

Você pode permitir que os usuários de autoatendimento ingressem em grupos configurando o suporte para grupos com autoinscrição no arquivo de configuração de diretório.

Quando um usuário se autorregistra, o CA Identity Manager procura grupos em organizações especificadas e, em seguida, exibe os grupos com autoinscrição para o usuário.

Siga estas etapas:

1. Na seção Grupos com autoinscrição, adicione um elemento SelfSubscribingGroups da seguinte forma:

   <SelfSubscribingGroups type=*tipo_de_pesquisa* org=*dn_org*>

2. Adicione valores para os seguintes parâmetros:

   type

   Indica onde o CA Identity Manager procura grupos com autoinscrição da seguinte maneira:

   - NONE — o CA Identity Manager não procura grupos. Especifique NONE para impedir que os usuários se autoinscrevam em grupos.
   - ALL — o CA Identity Manager começa a pesquisa por grupos na raiz. Especifique ALL quando os usuários podem se inscrever em grupos por todo um diretório hierárquico.
   - INDICATEDORG — o CA Identity Manager procura grupos com autoinscrição na organização de um usuário e em suas suborganizações. Por exemplo, quando o perfil de um usuário estiver na organização Marketing, o CA Identity Manager irá procura grupos com autoinscrição na organização Marketing e em todas as suborganizações.
   - SPECIFICORG — o CA Identity Manager faz buscas em uma organização específica. Forneça o DN (distinguished name - nome distinto) da organização específica no parâmetro org.

   org

   Especifica o identificador exclusivo da organização em que o CA Identity Manager procura grupos com autoinscrição.

   Observação: certifique-se de especificar o parâmetro org quando type=SPECIFICORG.

Assim que o suporte para grupos com autoinscrição for configurado no diretório do CA Identity Manager, os administradores do CA Identity Manager poderão especificar quais grupos têm autoinscrição no Console de usuário.

Observação: para obter mais informações sobre o gerenciamento de grupos, consulte o *Guia de Administração*.

Configurar grupos dinâmicos e aninhados

Se estiver gerenciando um repositório de usuários LDAP, você poderá configurar o suporte para os seguintes tipos de grupo no arquivo de configuração de diretório:

Grupos dinâmicos

Permite que você defina a associação ao grupo especificando uma consulta por filtro LDAP no Console de usuário de forma dinâmica. Com grupos dinâmicos, os administradores não precisam procurar e adicionar integrantes de grupo individualmente.

Grupos aninhados

Permite adicionar grupos como integrantes de outros grupos.

Você pode ativar grupos dinâmicos e aninhados usando o arquivo de configuração de diretório.

Siga estas etapas:

1. Mapeie os seguintes atributos conhecidos (na página 83) para um atributo físico do objeto gerenciado Grupo gerenciado, conforme a necessidade:
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   Observação: o atributo físico que você seleciona deve oferecer suporte a vários valores.
2. Na seção Comportamento de grupos de diretórios, adicione o seguinte elemento GroupTypes:

   `<GroupTypes type=`*`grupo`*`>`

   Observação: o GroupTypes faz distinção entre maiúsculas e minúsculas.

3. Digite um valor para o seguinte parâmetro:

   group

   Ativa suporte para grupos dinâmicos e aninhados. Os valores válidos são os seguintes:

   - NONE — o CA Identity Manager não oferece suporte a grupos dinâmicos e aninhados.
   - ALL — o CA Identity Manager oferece suporte a grupos dinâmicos e aninhados.
   - DYNAMIC — o CA Identity Manager oferece suporte somente a grupos dinâmicos.
   - NESTED — o CA Identity Manager oferece suporte somente a grupos aninhados.

Assim que o suporte a grupos dinâmicos e aninhados é configurado no diretório do CA Identity Manager, os administradores do CA Identity Manager podem especificar quais grupos são dinâmicos e aninhados no Console de usuário.

Observação: considere que você definiu o tipo de grupo para NESTED ou ALL *sem* configurar o parâmetro conhecido %NESTED_GROUP_MEMBERSHIP%. Nesse caso, o CA Identity Manager armazena os usuários e os grupos aninhados no parâmetro conhecido %GROUP_MEMBERSHIP%. O processamento da associação ao grupo pode ser ligeiramente mais lento.

Adicionar suporte para grupos como administradores de grupos

Se estiver gerenciando um repositório de usuários LDAP, você poderá ativar grupos para servirem como administradores de outros grupos. Ao atribuir um grupo como um administrador, apenas os administradores do grupo serão administradores do grupo especificado. Integrantes do grupo de administradores que você especifica não possuem privilégios para gerenciar o grupo.

Siga estas etapas:

1. Mapeie o atributo conhecido %GROUP_ADMIN_GROUP% para um atributo físico que armazena a lista de grupos que atuam como administradores.

   Observação: o atributo físico que você seleciona deve oferecer suporte a vários valores.

   Agrupar os atributos conhecidos (na página 83) fornece mais informações sobre o atributo %GROUP_ADMIN_GROUP%.

   Observação: se você definir o tipo de grupo administrativo para ALL sem configurar o atributo conhecido %GROUP_ADMIN_GROUP%, o CA Identity Manager armazenará grupos de administradores no atributo %GROUP _ADMIN%.

2. Na seção Comportamento de AdminGroups do diretório, configure o elemento AdminGroupTypes da seguinte forma:

   <AdminGroupTypes type="ALL">

   O AdminGroupTypes padrão é NENHUM.

   Observação: "AdminGroupTypes" faz distinção entre maiúsculas e minúsculas.

Assim que o suporte para grupos como administradores for configurado no diretório do CA Identity Manager, os administradores do CA Identity Manager poderão especificar grupos como administradores de outros grupos no Console de usuário.

Regras de validação

Uma regra de validação impõe requisitos em dados que um usuário digita em um campo da tela de tarefas. Os requisitos podem impor um tipo de dados ou formato. Portanto, certifique-se de que os dados sejam válidos no contexto de outros dados na tela de tarefas.

As regras de validação são associados aos atributos de perfil. O CA Identity Manager garante que os dados inseridos para um atributo de perfil cumpra quaisquer regras de validação associadas antes do processamento de uma tarefa.

É possível definir regras de validações e associá-las aos atributos de perfil no arquivo de configuração de diretório.

Propriedades adicionais do diretório do CA Identity Manager

É possível configurar as seguintes propriedades adicionais:

- A ordem de classificação dos resultados de pesquisa.
- A pesquisa pelas classes de objeto para verificar se um novo usuário já existe.
- O tempo de espera para evitar que o CA Identity Manager ultrapasse o tempo limite antes da conclusão da replicação de dados, do diretório LDAP mestre para o diretório LDAP subordinado.

Configurar ordem de classificação

Você pode especificar um atributo de classificação para cada objeto gerenciado, como usuários, grupos ou organizações. O CA Identity Manager usa esse atributo para classificar os resultados da pesquisa na lógica de negócios personalizada que você cria com as APIs do CA Identity Manager.

Observação: o atributo de classificação não afeta a maneira como os resultados da pesquisa são exibidos no Console de usuário.

Por exemplo, quando você especifica o atributo cn para o objeto do usuário, o CA Identity Manager classifica os resultados de uma pesquisa de usuários em ordem alfabética, segundo o atributo cn.

Siga estas etapas:

1. Após o último elemento IMSManagedObjectAttr na seção do objeto gerenciado para o qual a ordem de classificação se aplica, adicione as seguintes instruções:

   ```
   <PropertyDict name="SORT_ORDER">
       <Property name="ATTR">seu_atributo_de_classificação
       </Property>
   </PropertyDict>
   ```

2. Substitua *seu_atributo_de_classificação* pelo atributo no qual o CA Identity Manager classifica os resultados da pesquisa.

Observação: especifique apenas um atributo físico. Não especifique um atributo conhecido.

Por exemplo, suponha que você tenha que classificar os resultados da pesquisa do usuário com base no valor do atributo cn. Adicione os elementos a seguir após o último elemento IMSManagedObjectAttr na seção Objeto do usuário do arquivo de configuração de diretório:

```
<!-- ******************* User Object ******************* -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

Pesquisar por Objectclasses

O CA Identity Manager pesquisa o repositório de usuários para verificar se o usuário existe ou não quando você cria um usuário. Essa pesquisa é limitada aos usuários que têm objectclasses especificadas na definição do objeto do usuário no arquivo de configuração de diretório (directory.xml). Se nenhum usuário for encontrado nessas objectclasses, o CA Identity Manager tentará criar o usuário.

Se houver um usuário com o mesmo identificador exclusivo (ID de usuário), mas uma objectclass diferente, o servidor LDAP falha ao criar o usuário. O erro é reportado no servidor LDAP, mas o CA Identity Manager não reconhece o erro. O CA Identity Managerparece criar o usuário com êxito.

Para evitar esse problema, você pode configurar uma propriedade SEARCH_ACROSS_CLASSES que faz com que o CA Identity Manager procure usuários em todas as definições de objectclass ao verificar a existência de usuários.

Observação: essa propriedade afeta apenas as pesquisas por usuários duplicados ao executar tarefas como a criação de um usuário. Para todas as outras pesquisas, são aplicadas as restrições de objectclass.

Siga estas etapas:

1. No arquivo de configuração de diretório (directory.xml), localize o elemento ImsManagedObject que descreve o objeto do usuário.

2. Adicione o seguinte elemento PropertyDict:

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Observação: PropertyDict deve ser o último elemento no elemento ImsManagedObject, como no exemplo a seguir:

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber"
displayname="Department" description="Department" valuetype="String"
required="true" multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

Especificar tempo de espera da replicação

Em uma implantação que inclui a replicação entre diretórios LDAP mestre e subordinado, você pode configurar o Servidor de políticas do SiteMinder para se comunicar com um diretório subordinado. Nessa configuração, o Servidor de políticas detecta as referências que apontam para o diretório mestre durante operações que gravam dados no diretório LDAP. Os dados são armazenados no diretório LDAP mestre e reaplicado no diretório LDAP subordinado de acordo com o esquema de replicação dos recursos da rede.

Nessa configuração, quando você cria um objeto no CA Identity Manager, o objeto é criado no diretório mestre e também replicado no diretório subordinado. Um atraso pode ocorrer durante o processo de replicação, causando a falha da ação de criação no CA Identity Manager.

Para evitar que esse problema ocorra, é possível especificar a quantidade de tempo (em segundos) que o CA Identity Manager aguardará antes de atingir o tempo limite na propriedade REPLICATION _WAIT _TIME.

Siga estas etapas:

1. No arquivo de configuração de diretório (directory.xml), localize o elemento ImsManagedObject que descreve o objeto do usuário.
2. Adicione o seguinte elemento PropertyDict:

   ```
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME"><tempo em segundos></Property>
   </PropertyDict>
   ```

   Observação: PropertyDict deve ser o último elemento no elemento ImsManagedObject, como no exemplo a seguir:

   ```
   <ImsManagedObject name="User" description="My Users"
   objectclass="top,person,organizationalperson,inetorgperson,customClass"
   objecttype="USER">
   <ImsManagedObjectAttr physicalname="departmentnumber"
   displayname="Department" description="Department" valuetype="String"
   required="true" multivalued="false" maxlength="0" />
   .
   .
   .
   <PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
   for LDAP provider to allow replication to propagate from master to slave">
   <Property name=REPLICATION_WAIT_TIME">800</Property>
   </PropertyDict>
   ```

Quando o tempo de espera da replicação não for definido, será usado o valor padrão 0.

Especificar configurações de conexão LDAP

Para melhorar o desempenho, você pode especificar os seguintes parâmetros no arquivo de configuração de diretório (directory.xml):

Tempo limite da conexão

Especifica o número máximo de milissegundos que o CA Identity Manager pesquisa um diretório antes de encerrar a pesquisa.

Essa propriedade está especificada no arquivo de configuração de diretório, como segue:

com.sun.jndi.ldap.connect.timeout

Tamanho máximo do pool de conexões

Especifica o número máximo de conexões que o CA Identity Manager pode fazer com o diretório LDAP.

Essa propriedade está especificada no arquivo de configuração de diretório, como segue:

com.sun.jndi.ldap.connect.pool.maxsize

Tamanho padrão do pool de conexões

Especifica o número de conexões padrão entre o CA Identity Manager e o diretório LDAP.

Essa propriedade está especificada no arquivo de configuração de diretório, como segue:

com.sun.jndi.ldap.connect.pool.prefsize

Siga estas etapas:

1. No arquivo de configuração de diretório (directory.xml), localize o elemento ImsManagedObject que descreve o objeto do usuário.
2. Adicione o seguinte elemento PropertyDict:

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. Salve o arquivo directory.xml.

   O CA Identity Manager define essas configurações quando você cria o diretório do CA Identity Manager diretório com esse arquivo.

Como melhorar o desempenho da pesquisa de diretório

Para melhorar o desempenho das pesquisas de diretório para usuários, organizações e grupos, execute as ações a seguir:

- Indexe os atributos que os administradores podem especificar nas consultas de pesquisa.

  Observação: para o Oracle Internet Directory, uma pesquisa pode falhar quando um atributo em uma consulta de pesquisa não está indexado.

- Defina a configurações de tamanho da página e máximo de linhas (na página 97) para determinar como o CA Identity Manager trata pesquisas amplas.
- Ajuste o diretório de usuários. Consulte a documentação do diretório de usuários que você está usando.

Como melhorar o desempenho de pesquisas amplas

Quando o CA Identity Manager gerencia um grande repositório de usuários, as pesquisas que retornam muitos resultados podem fazer com que o sistema fique sem memória. Para ajudar a evitar problemas de memória, você pode definir limites para pesquisas amplas.

As duas configurações a seguir determinam como o CA Identity Manager trata as pesquisas amplas:

- Número máximo de linhas

  Especifica o número máximo de resultados que o CA Identity Manager pode retornar ao procurar um diretório de usuários. Quando o número de resultados exceder o limite, um erro será exibido.

- Tamanho da página

  Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

  Observe os seguintes pontos ao especificar o tamanho da página:

  - Para usar a opção Search Page Size, o repositório de usuários que o <idmgr> gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários exigem configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte os tópicos a seguir:

    Configurar o suporte à paginação do Servidor de diretórios do Sun Java System (na página 99)

    Configurar o suporte à paginação do Active Directory

  - Se o repositório de usuários não oferecer suporte à paginação e um valor para maxrows for especificado, o CA Identity Manager usará apenas o valor de maxrows para controlar o tamanho da pesquisa.

É possível configurar os limites máximos de linha e de tamanho da página nos seguintes locais:

- Repositório de usuários

  Na maioria dos repositórios de usuários e bancos de dados, é possível definir limites de pesquisa.

  Observação: para obter mais informações, consulte a documentação do repositório de usuários ou banco de dados que você está usando.

- Diretório do CA Identity Manager

  Você pode configurar o elemento DirectorySearch (na página 58) no arquivo de configuração de diretório (directory.xml) que usa para criar o Diretório do CA Identity Manager.

  Por padrão, o valor máximo de linhas e de tamanho da página é ilimitado para os diretórios existentes. Para novos diretórios, o valor máximo de linhas é ilimitado e o valor do tamanho de página é 2000.

- Definição de objeto gerenciado

  Para definir os limites máximos de linha e tamanhos de página que se aplicam a um tipo de objeto, e não ao diretório inteiro, configure a *definição de objeto gerenciado* (na página 61) no arquivo directory.xml que é usado para criar o Diretório do CA Identity Manager.

  A definição de limites para um tipo de objeto gerenciado permite fazer ajustes que são se baseiam nos requisitos de negócios. Por exemplo, a maioria das empresas tem mais usuários do que os grupos. As empresas podem definir limites somente para pesquisas de objeto do usuário.

- Telas de pesquisa de tarefa

  Você pode controlar o número de resultados da pesquisa que os usuários podem ver nas telas de pesquisa e lista no Console de usuário. Se o número de resultados exceder o número de resultados por página que são definidos para a tarefa, os usuários verão links para páginas adicionais de resultados.

  Essa definição não afeta o número de resultados retornados por uma pesquisa.

  Observação: para obter informações sobre como definir o tamanho da página nas telas de pesquisa e lista, consulte o *Guia de Administração*.

Se os limites máximos de linha e tamanhos de página forem definidos em vários lugares, a configuração mais específica será aplicada. Por exemplo, as configurações de objeto gerenciado têm precedência sobre as configurações de nível de diretório.

Configurar o suporte à paginação do Servidor de diretórios do Sun Java System

Os Servidores de diretório do Sun Java System oferecem suporte à VLV (Virtual List View), um método para fornecer resultados de pesquisa em uma determinada ordem ou em determinados subconjuntos. Esse método é diferente dos Simple Paged Results, que o CA Identity Manager espera.

Para usar a VLV, defina permissões e crie índices. O CA Identity Manager inclui os seguintes arquivos que você deve configurar para oferecer suporte à paginação:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Esses arquivos são incluídos como parte da amostra da NeteAuto em samples\NeteAuto em Ferramentas administrativas.

As Ferramentas administrativas são instaladas nos seguintes locais padrão:

Windows: <caminho_de_instalação>

UNIX: <caminho_de_instalação2>

Siga estas etapas:

1. Adicione o parâmetro a seguir ao elemento DirectorySearch (na página 58) no arquivo directory.xml do diretório do CA Identity Manager, como se segue:

   ```
   minsortrules="1"
   ```

   Observação: se você estiver modificando uma diretório existente do CA Identity Manager, consulte Como atualizar um diretório do CA Identity Manager (na página 184).

2. Defina as permissões para o arquivo vlvcntrl.ldif da seguinte forma:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvcntrl.ldif`

3. Importe definições de índice e pesquisa VLV da seguinte maneira:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvindex.ldif`

4. Interrompa o diretório da seguinte maneira:
   `stop-slapd`

5. Crie os índices usando runvlvindex.

6. Inicie o diretório da seguinte maneira:
   `start-slapd`

Configurar o suporte à paginação do Active Directory

Para configurar o suporte à paginação no Active Directory, execute as seguintes etapas de alto nível:

- Configure o suporte para Virtual List View (na página 100).
- Configure MaxPageSize do Active Directory (na página 101). (**Somente para Diretórios criados antes do CA Identity Manager r12.5 SP7**)

Configurar o suporte para VLV (Virtual List View)

O Active Directory oferece suporte à VLV (Virtual List View), um método para fornecer resultados de pesquisa em uma determinada ordem ou em determinados subconjuntos. Esse método é diferente dos Simple Paged Results, que o CA Identity Manager espera.

Para usar a VLV, defina permissões e crie índices. O CA Identity Manager inclui os seguintes arquivos que você deve configurar para oferecer suporte à paginação:

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

Esses arquivos são incluídos como parte da amostra da NeteAuto em samples\NeteAuto em Ferramentas administrativas.

As Ferramentas administrativas são instaladas nos seguintes locais padrão:

Windows: <caminho_de_instalação>

UNIX: <caminho_de_instalação2>

Siga estas etapas:

1. Adicione o parâmetro a seguir ao elemento DirectorySearch (na página 58) no arquivo directory.xml do diretório do CA Identity Manager, como se segue:

   ```
   minsortrules="1"
   ```

   Observação: se você estiver modificando uma diretório existente do CA Identity Manager, consulte Como atualizar um diretório do CA Identity Manager (na página 184).

2. Defina as permissões para o arquivo vlvcntrl.ldif da seguinte forma:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvcntrl.ldif`

3. Importe definições de índice e pesquisa VLV da seguinte maneira:
   `ldapmodify -D "cn=Directory Manager" -w password -p port -f vlvindex.ldif`

4. Interrompa o diretório da seguinte maneira:
   `stop-slapd`
5. Crie os índices usando runvlvindex.
6. Inicie o diretório da seguinte maneira:
   `start-slapd`

Configurar MaxPageSize do Active Directory

O Active Directory usa 1000 como MaxPageSize padrão. Pressuponha que o valor do atributo maxpagesize no directory.xml seja maior que ou igual a 1000. Nesse caso, o CA Identity Manager falha ao exibir um aviso quando o número de resultados da pesquisa excede o valor de maxrows no directory.xml. Nesse caso, os administradores que executam a pesquisa não estão cientes de que alguns resultados da pesquisa são omitidos.

Para evitar esse problema, verifique se o valor do atributo maxpagesize para o Diretório e cada objeto gerenciado é menor que o valor de MaxPageSize do Active Directory.

Suponha que você esteja criando um Diretório do CA Identity Manager usando o modelo de arquivo directory.xml que é instalado com o CA Identity Manager 12.5 SP7 ou superior. Nesse caso, não é necessário executar nenhuma etapa adicional para oferecer suporte à paginação. O atributo maxpagesize no directory.xml é definido por padrão.

Se você estiver adicionando suporte à paginação a um Diretório existente do CA Identity Manager, o atributo maxpagesize no directory.xml deverá ser menor que 1000.

Além disso, se o valor de MaxPageSize do Active Directory for 1000, certifique-se de definir o atributo maxpagesize corretamente para o Diretório do CA Identity Manager e todos os objetos gerenciados.

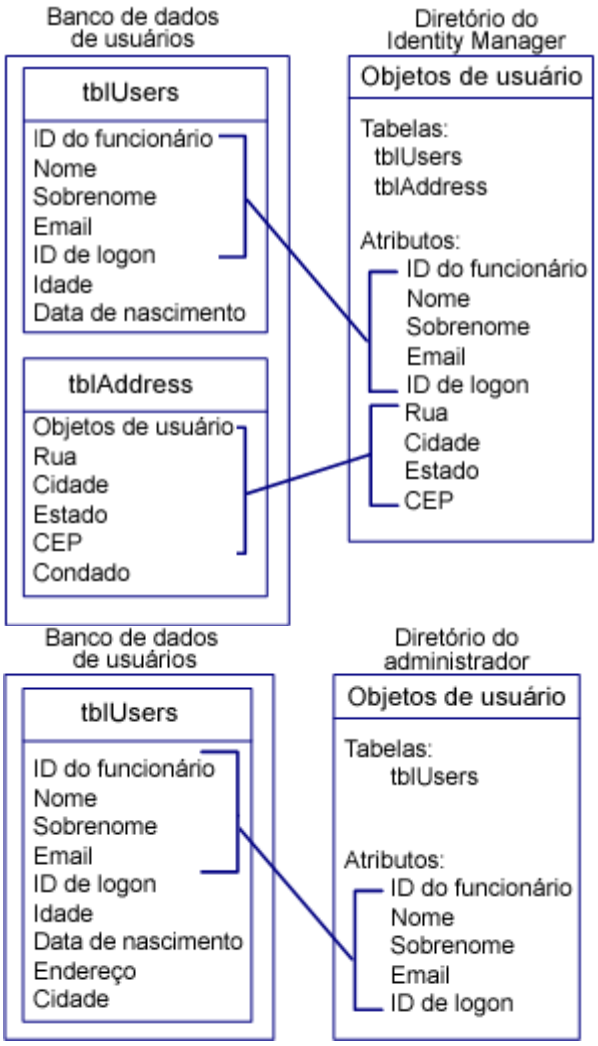
Capítulo 4: Gerenciamento de bancos de dados relacionais

Esta seção contém os seguintes tópicos:

Diretórios do CA Identity Manager

Um *diretório do CA Identity Manager* descreve como objetos, como usuários, grupos e organizações (opcional) são armazenados no diretório de usuários e como eles são representados no CA Identity Manager. Um diretório do CA Identity Manager é associado a um ou mais dos ambientes do CA Identity Manager.

A ilustração a seguir mostra como um diretório do CA Identity Manager se relaciona a um repositório de usuários:



Observação: alguns atributos de usuário no banco de dados não fazem parte do diretório do CA Identity Manager. Portanto, o CA Identity Manager não os gerencia.

Observações importantes ao configurar o CA Identity Manager para bancos de dados relacionais

Antes de configurar o CA Identity Manager para gerenciar um banco de dados relacional, certifique-se de que o banco de dados atende aos seguintes requisitos:

- O banco de dados deve poder ser acessado por meio de um driver JDBC ou de um driver ODBC (Open Database Connectivity) (quando o CA Identity Manager integra-se ao SiteMinder). O driver deve oferecer suporte a uniões externas. Se mais de duas tabelas forem usadas para representar um objeto gerenciado, o driver também deverá oferecer suporte a uniões externas aninhadas.

  Observação: se o driver não oferecer suporte a uniões externas, o CA Identity Manager usará uniões internas ao consultar o banco de dados. Isso pode gerar resultados de consulta inesperados.

- Identifique exclusivamente cada objeto que o CA Identity Manager gerencia, como usuário, grupo ou organização (quando suportado). Por exemplo, o identificador exclusivo de usuários pode ser uma ID de logon.

  Observação: certifique-se de que o identificador exclusivo esteja armazenado em uma única coluna.

- O CA Identity Manager alguns atributos com valor múltiplo, que podem ser armazenados como uma lista delimitada em uma célula única ou em várias linhas em uma tabela separada. Por exemplo, a tabela tblGroupMembers a seguir armazena os integrantes de um grupo:

ID	Integrantes
Pesquisa	dmason
Pesquisa	rsavory
Marketing	dmason
Marketing	awelch

A coluna ID contém o identificador exclusivo de um grupo e a coluna Integrantes contém o identificador exclusivo de um integrante do grupo. Por exemplo, dmason e rsavory são integrantes do grupo Pesquisa. Quando um novo integrante é adicionado a esse grupo, outra linha é adicionada a tblGroupMembers.

- Quando seu ambiente inclui organizações, execute a seguinte tarefa:
  - Edite e execute um script SQL, incluído com o CA Identity Manager, no banco de dados para configurar o suporte à organização (na página 149).
  - O CA Identity Manager exige uma organização de nível superior, chamada raiz. Todas as outras organizações se relacionam com a organização raiz.

    Para obter mais informações sobre requisitos da organização, consulte Gerenciamento de organizações (na página 148).

Criar uma origem de dados Oracle para o WebSphere

Siga estas etapas:

1. No Console administrativo do WebSphere, navegue até o provedor do JDBC criado quando você configurou o driver JDBC.
2. Crie uma origem de dados com as seguintes propriedades e clique em Apply:

   Name: Origem de dados do repositório de usuários

   JNDI Name: userstore

   URL: jdbc:oracle:thin:@*nome_do_sistema_do_db*:1521:*sid_oracle*
3. Configure um nova Entrada de dados de autenticação J2C para a Origem de dados do repositório de usuários:
   a. Insira as seguintes propriedades:

      Alias: Repositório de usuários

      User ID: *nome de usuário*

      password: *senha*

      em que *nome de usuário* e *senha* são o nome de usuário e a senha para a conta especificada quando você criou o banco de dados.

   b. Clique em OK e, em seguida, use os links de navegação na parte superior da tela para retornar à origem de dados que você está criando.
4. Selecione a Entrada de dados de autenticação J2C do Repositório de usuários que você criou na caixa de listagem dos campos a seguir:
   - Component-managed Authentication Alias
   - Container-managed Authentication Alias
5. Clique em OK e salve a configuração.

   Observação: para verificar se a origem de dados está configurada corretamente, clique em Testar conexão na tela de configuração da origem de dados. Se a conexão de teste falhar, reinicie o WebSphere e teste a conexão novamente.

Como criar um diretório do CA Identity Manager

Siga estas etapas:

1. Se você estiver usando o SiteMinder, aplique o esquema do repositório de políticas antes da criação de um Diretório do CA Identity Manager.

   Observação: para obter mais informações sobre esquemas específicos do repositório de políticas e como aplicá-los, consulte o *Guia de Instalação*.

2. Se você estiver usando o SiteMinder, crie uma origem de dados ODBC para utilização com o SiteMinder (na página 113).

3. Crie uma origem de dados para o banco de dados de usuários que o CA Identity Manager gerencia.

4. Descreva o banco de dados para o CA Identity Manager modificando um arquivo de configuração de diretório (directory.xml). Para obter mais informações, consulte Como descrever um banco de dados em um arquivo de configuração de diretório.

5. No Management Console, importe o arquivo de configuração de diretório e crie o diretório.

Como criar uma origem de dados JDBC

O CA Identity Manager exige uma origem de dados JDBC no servidor de aplicativos em que ele está instalado para se conectar ao repositório de usuários. As instruções para criar uma origem de dados são diferentes para cada servidor de aplicativos.

Criar uma origem de dados JDBC para os servidores de aplicativos JBoss

Siga estas etapas:

1. Crie uma cópia do seguinte arquivo:

   base_do_jboss\server\default\deploy\objectstore-ds.xml

   início do jboss

   O local de instalação do servidor de aplicativos Jboss em que o CA Identity Manager está instalado.

   O novo arquivo deve existir no mesmo local.

2. Renomeie o arquivo para userstore-ds.xml.

3. Edite userstore-ds.xml da seguinte maneira:
   a. Localize o elemento <jndi-name>.
   b. Altere o valor do elemento <jndi-name> de jdb/objectstore para userstore da seguinte maneira:

      <jndi-name>userstore</jndi-name>

   c. No elemento <connection-url>, altere o nome o parâmetro DatabaseName para o nome do banco de dados que atua como o repositório de usuários, como se segue:

      <connection-url>

      jdbc:sqlserver://*endereçoip:porta* selectMethod=cursor;DatabaseName=*nome_do_armazenemnto_de_ususuários*

      </connection-url>

      endereçoip

      Especifica o endereço IP da máquina onde o repositório de usuários está instalado.

      porta

      Especifica o número da porta para o banco de dados

      nome_do_repositório_de_usuários

      Especifica o nome do banco de dados que atua como o repositório de usuários.

4. Execute as etapas a seguir se você planeja criar um real de segurança do JBoss, que é necessário para oferecer suporte ao FIPS:
   a. Renomeie security-domain para <security-domain>imuserstoredb</security-domain>.
   b. Salve o arquivo.
   c. Omita as etapas restantes. Execute as etapas em Criar um realm de segurança do JBoss para a origem de dados JDBC (na página 109).
5. Faça as seguintes alterações adicionais em userstore-ds.xml:
   a. Altere o valor do elemento <user-name> para o nome de usuário de uma conta que tenha acesso de leitura e gravação no repositório de usuários.
   b. Altere o valor do elemento <password> para a senha da conta especificada no elemento <user-name>.

   Observação: os elementos user-name e password aparecem em texto não criptografado nesse arquivo. Portanto, é possível optar por criar um realm de segurança do JBoss, em vez de editar userstore-ds.xml.
6. Salve o arquivo.

Usar um realm de segurança do JBoss para a origem de dados JDBC

Assegure-se de que esteja criando uma origem de dados JDBC em um servidor de aplicativos JBoss. Você pode configurar a origem de dados para usar um nome de usuário e uma senha ou pode configurá-la para usar um realm de segurança.

Importante: certifique-se de que a opção JBoss Security Realm seja usada se o FIPS estiver sendo usado.

Siga estas etapas:

1. Execute as etapas em Criar uma origem de dados JDBC para os servidores de aplicativos JBoss (na página 107).

   Não especifique um nome de usuário e uma senha no userstore-ds.xml, conforme descrito na etapa 4.

2. Abra login-cfg.xml em *base_do_jboss*\server\default\conf.

3. Localize a entrada a seguir no arquivo:

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-
option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. Copie toda a entrada e cole-a nas tags <policy> e </policy> no arquivo login-cfg.xml> no arquivo.

5. Na entrada colada no arquivo, faça as seguintes alterações:

   a. Altere o valor do atributo de nome de imobjectstoredb para imuserstoredb da seguinte maneira:

      ```
      <application-policy name="imuserstoredb">
      ```

   b. Especifique o nome de usuário utilizado na autenticação no repositório de usuários da seguinte maneira:

      ```
      <module-option
      name="userName">usuário_do_repositório_de_usuários</module-option>
      ```

   c. Especifique a senha do usuário na etapa anterior, como se segue:

      ```
      <module-option
      name="password">senha_do_usuário_no_repositório_de_usuários</module-
      option>
      ```

Observação: para criptografar a senha do repositório de usuários, use a ferramenta de senha (pwdtools) que é instalada com o CA Identity Manager.

d. No elemento <module-option name="managedConnectionFactoryName">, forneça o jdbc.jca:name correto, como se segue:

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. Salve o arquivo.
7. Reinicie o servidor de aplicativos.

Criar uma origem de dados JDBC para WebLogic

É possível criar uma origem de dados no Console de administração do WebLogic.

Observação: consulte a Documentação do Oracle WebLogic 11 para obter informações completas sobre Pools de conexões do Weblogic.

Siga estas etapas:

1. Crie uma origem de dados JDBC com os seguintes parâmetros no Console de administração do WebLogic:

   Name: Origem de dados do repositório de usuários

   JNDI Name: userstore

2. Crie o pool de conexões para a origem de dados com as seguintes informações:

   - Para bancos de dados do SQL Server 2005, use os seguintes valores:

     URL: jdbc:sqlserver://*Nome_do_sistema_do_db*:1433

     Driver Class Name: com.microsoft.sqlserver.jdbc.SQLServerDriver

     Properties: user=*nome_de_usuário*

     databaseName=*nome do repositório de usuários*

     selectMethod=cursor

     Password: *senha*

   - No caso dos bancos de dados Oracle, use os seguintes valores:

     URL: jdbc:oracle:thin:@*nome_do_sistema_db_tp*:1521:*ID_oracle*

     Driver Class Name: oracle.jdbc.driver.OracleDriver

     Properties: user=*nome_de_usuário*

     Password: *senha*

3. Após a configuração, defina o destino do pool para a instância do servidor *wl_server_name*.

   Depois de implantar o pool, verifique o console para verificar a ocorrência de erros.

   Observação: você pode ver uma mensagem de erro que informa que a origem de dados não pode ser criada com um pool não existente. Para resolver esse erro, reinicie o WebLogic.

Origens de dados do WebSphere

As seções a seguir descrevem como criar uma origem de dados SQL ou Oracle para servidores de aplicativos WebSphere.

Criar uma origem de dados SQL Server para WebSphere

Siga estas etapas:

1. No Console administrativo do WebSphere, navegue até o provedor do JDBC criado quando você configurou o driver JDBC.
2. Selecione Data Sources na seção Additional Properties.
3. Crie uma origem de dados com as seguintes propriedades e clique em Apply:

   Name: Origem de dados do repositório de usuários

   JNDI Name: userstore

   databaseName: *nome_do_repositório_de_usuários*

   serverName: *nome_do_sistema_do_db*

4. Configure a propriedade selectMethod da seguinte maneira:
   a. Selecione Custom Properties na seção Additional Properties.
   b. Clique na propriedade personalizada selectMethod.
   c. Digite o texto a seguir no campo Value:

      cursor

   d. Clique em OK e, em seguida, use os links de navegação na parte superior da tela para retornar à origem de dados que você está criando.

5. Configure um nova Entrada de dados de autenticação J2C para a Origem de dados do repositório de usuários:
   a. Selecione J2EE Connector Architecture (J2C) authentication data entries na seção Related Items.
   b. Clique em Novo.
   c. Insira as seguintes propriedades:

      Alias: Repositório de usuários

      User ID: *nome de usuário*

      password: *senha*

      em que *nome de usuário* e *senha* são o nome de usuário e a senha para a conta especificada quando você criou o banco de dados.
   d. Clique em OK e, em seguida, use os links de navegação na parte superior da tela para retornar à origem de dados que você está criando.
6. Selecione a Entrada de dados da autenticação J2C do repositório de usuários que você criou na caixa de listagem do campo Component-managed Authentication Alias.
7. Clique em OK e salve a configuração.

   Observação: para verificar se a origem de dados está configurada corretamente, clique em Testar conexão na tela de configuração da origem de dados. Se a conexão de teste falhar, reinicie o WebSphere e teste a conexão novamente.

Criar uma origem de dados Oracle para o WebSphere

Siga estas etapas:

1. No Console administrativo do WebSphere, navegue até o provedor do JDBC criado quando você configurou o driver JDBC.
2. Crie uma origem de dados com as seguintes propriedades e clique em Apply:

   Name: Origem de dados do repositório de usuários

   JNDI Name: userstore

   URL: jdbc:oracle:thin:@*nome_do_sistema_do_db*:1521:*sid_oracle*

3. Configure um nova Entrada de dados de autenticação J2C para a Origem de dados do repositório de usuários:

   a. Insira as seguintes propriedades:

      Alias: Repositório de usuários

      User ID: *nome de usuário*

      password: *senha*

      em que *nome de usuário* e *senha* são o nome de usuário e a senha para a conta especificada quando você criou o banco de dados.

   b. Clique em OK e, em seguida, use os links de navegação na parte superior da tela para retornar à origem de dados que você está criando.

4. Selecione a Entrada de dados de autenticação J2C do Repositório de usuários que você criou na caixa de listagem dos campos a seguir:

   - Component-managed Authentication Alias
   - Container-managed Authentication Alias

5. Clique em OK e salve a configuração.

   Observação: para verificar se a origem de dados está configurada corretamente, clique em Testar conexão na tela de configuração da origem de dados. Se a conexão de teste falhar, reinicie o WebSphere e teste a conexão novamente.

Como criar uma origem de dados ODBC para uso com o SiteMinder

Se o CA Identity Manager se integrar ao SiteMinder, defina uma origem de dados ODBC na máquina do SiteMinder que aponte para o banco de dados. Anote o nome da origem de dados para uso posterior. Proceda da seguinte maneira:

- **Windows:** configure a origem de dados ODBC com um DN do sistema. Consulte a documentação do sistema operacional Windows para obter instruções.
- **UNIX:** adicione uma entrada especificando os parâmetros para a origem de dados ODBC no arquivo system_odbc.ini localizado em *instalação_do_servidor_de_políticas*/db.

Como descrever um banco de dados em um arquivo de configuração de diretório

Para gerenciar um banco de dados, o CA Identity Manager deve compreender a estrutura e o conteúdo do bancos de dados. Para descrever o banco de dados para o CA Identity Manager crie um arquivo de configuração de diretório (directory.xml).

O arquivo de configuração de diretório contém um ou mais das seções a seguir:

Informações do diretório do CA Identity Manager

Contém informações sobre o diretório do CA Identity Manager que o CA Identity Manager usa.

Validação de atributo

Define as regras de validação que se aplicam ao diretório do CA Identity Manager.

Informações do provedor

Descreve o repositório de usuários que o CA Identity Manager gerencia.

Informações de pesquisa de diretório

Permite que você especifique como o CA Identity Manager pesquisa o repositório de usuários.

Objeto do usuário (na página 116)

Descreve como os usuários são armazenadas no repositório de usuários e como eles são representados no CA Identity Manager.

Objeto do grupo (na página 116)

Descreve como os grupos são armazenados no repositório de usuários e como eles são representados no CA Identity Manager.

Objeto da organização (na página 116)

Descreve como as organizações são armazenadas e como são representadas no CA Identity Manager.

Grupos com autoinscrição

Configura o suporte para grupos em que os usuários de autoatendimento podem ingressar.

O diretório em que você instalou as ferramentas administrativas do CA Identity Manager inclui o seguinte modelo de arquivo de configuração de diretório para bancos de dados relacionais:

ferramentas_administrativas\directoryTemplates\RelationalDatabase\directory.xml

ferramentas_administrativas

Define o local de instalação das ferramentas administrativas do CA Identity Manager, como nos exemplos a seguir:

- **Windows:** <caminho_de_instalação>\tools
- **UNIX:** <caminho_de_instalação2>/tools

Observação: o modelo de arquivo de configuração de diretório em directoryTemplates\RelationalDatabase é configurado para ambientes que oferecem suporte a organizações. Para ver um arquivo de configuração de diretório para um ambiente que não inclui organizações, você pode examinar o arquivo directory.xml para a amostra da NeteAuto localizada em *ferramentas_administrativas*\samples\NeteAutoRDB\NoOrganization

Copie o modelo de configuração em um novo diretório ou salve-o com um nome diferente para que ele não seja substituído. Em seguida, você poderá modificar o modelo para refletir a estrutura do seu banco de dados.

O arquivo de configuração de diretório apresenta duas convenções importantes:

- ## — indica valores exigidos.

  Para fornecer todas as informações necessárias, localize todos os sinais de cerquilhas duplas (##) e as substitua por valores apropriados. Por exemplo, ##PASSWORD_HINT indica que você deve fornecer um atributo para armazenar uma pergunta que um usuário responde para receber uma senha temporária no caso de uma senha esquecida.

- @ — indica os valores preenchidos pelo CA Identity Manager. Não modifique esses valores no arquivo de configuração de diretório. O CA Identity Manager solicita que você forneça os valores quando importa o arquivo de configuração de diretório.

Para modificar o arquivo de configuração de diretório, você precisará das seguintes informações:

- Os nomes de tabela para os objetos de usuário, grupo e organização (quando sua estrutura inclui organizações).
- Uma lista de atributos nos perfis de usuário, grupo e organização (quando sua estrutura inclui organizações).

Modificar o arquivo de configuração de diretório

Execute o procedimento a seguir para modificar o arquivo de configuração de diretório.

Siga estas etapas:

1. Configure uma conexão com o banco de dados.
2. Especifique a quantidade de tempo que o CA Identity Manager pesquisará um diretório antes de encerrar a pesquisa.
3. Defina os objetos gerenciados de usuário e grupo que o CA Identity Manager gerencia (na página 116).
4. Modifique os atributos conhecidos.

   Os atributos conhecidos identificam atributos especiais, como o atributo de senha, no CA Identity Manager.

5. Configure o suporte a grupos com autoinscrição.
6. Se o seu ambiente incluir organizações, configure o suporte à organização.

Mais informações:

Descrições de objeto gerenciado (na página 116)
Gerenciamento da organização (na página 148)
Como configurar grupos com autoinscrição (na página 146)
Atributos conhecidos para um banco de dados relacional (na página 141)

Descrições de objeto gerenciado

No CA Identity Manager, você gerencia os tipos de objetos a seguir, correspondentes às entradas em um repositório de usuários:

- Usuários - representam os usuários em uma empresa.
- Grupos - representam as associações de usuários que possuem uma característica em comum.
- (Opcional) Organizações - representam unidades de negócios. As organizações podem conter usuários, grupos e outras organizações.

  Observação: Gerenciamento de organizações (na página 148) fornece informações sobre como configurar organizações.

Uma descrição do objeto contém as seguintes informações:

- Informações sobre o objeto (na página 116), como as tabelas na qual o objeto é armazenado.
- Os atributos que armazenam informações sobre uma entrada (na página 121). Por exemplo, o atributo de pager armazena um número de pager.

Importante: um ambiente do CA Identity Manager oferece suporte a apenas um tipo de objeto de usuário, grupo e organização.

Como descrever um objeto gerenciado

Um objeto gerenciado é descrito especificando informações do objeto nas seções Objeto de usuário, Objeto de grupo e Objeto de organização (quando o banco de dados inclui organizações) do arquivo de configuração de diretório.

Cada uma dessas seções contém um elemento ImsManagedObject, como o código a seguir:

```
<ImsManagedObject name="User" description="My Users">
```

O elemento ImsManagedObject pode incluir os seguintes elementos:

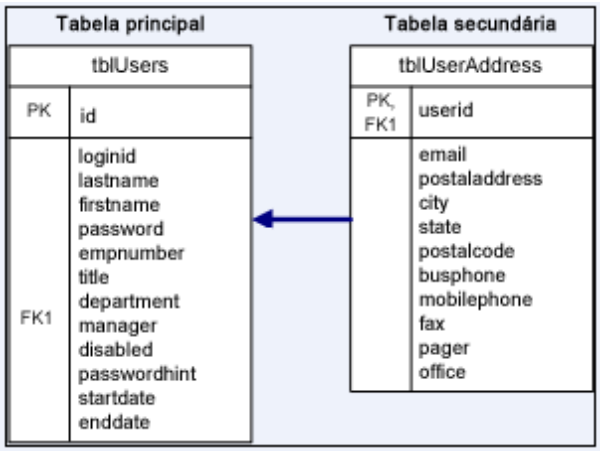
- Table (obrigatório)
- UniqueIdentifier (obrigatório)
- ImsManagedObjectAttr (obrigatório)
- RootOrg (apenas para objetos de organização)

Tabelas de banco de dados

Use o elemento Table no arquivo de configuração de diretório para definir as tabelas que armazenam informações sobre um objeto gerenciado.

Cada objeto gerenciado deve ter uma tabela principal que contém o identificador exclusivo do objeto. As informações adicionais podem ser armazenadas em tabelas secundárias.

A ilustração a seguir mostra um banco de dados que armazena informações de usuário em um tabela principal e secundária:



Se as informações de um objeto forem armazenadas em várias tabelas, crie um elemento Table para cada tabela. Use o elemento Reference no elemento Table para uma tabela secundária para definir sua relação com a tabela principal.

Por exemplo, se as informações básicas sobre um usuário forem armazenadas em tblUsers e as informações sobre o endereço forem armazenadas em tblUserAddress, as definições de tabela para o objeto gerenciado Usuário se parecerão com as seguintes entradas:

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Elementos Table

Os parâmetros de um elemento table são os seguintes:

name

(obrigatório)

Especifica o nome da tabela que armazena alguns ou todos os atributos em um perfil gerenciado de um objeto.

primary

Indica se a tabela é a tabela principal para o objeto gerenciado. A tabela principal contém o identificador exclusivo do objeto, como mostrado a seguir:

- True — a tabela é a tabela principal.
- False — a tabela é uma tabela secundária (padrão).

Se você não especificar o parâmetro principal, o CA Identity Manager assumirá a tabela como uma tabela secundária.

Observação: apenas uma tabela pode ser a tabela principal.

filter

Identifica um subconjunto das entradas de tabela que se aplicam ao objeto gerenciado.

O parâmetro de filtro opcional pode se parecer com o seguinte exemplo:

```
filter="ORG=2"
```

Observação: o filtro se aplica apenas às consultas que o CA Identity Manager gera. Se você substituir uma consulta gerada por uma consulta personalizada, especifique o filtro na consulta personalizada.

fullouterjoin

Indica se a união externa é uma união externa completa.

- True — a união externa é uma união externa completa. Nesse caso, a condição que é necessária para retornar uma linha válida é encontrada em ambas as tabelas na união de uma linha retornada.
- False — a união externa é uma união externa abandonada em relação à tabela principal. Nesse caso, apenas as linhas em uma tabela na consulta devem atender à condição (padrão).

Observação: os parâmetros são opcionais, a menos que especificado em contrário.

O parâmetro Table pode conter um ou mais elementos Reference para vincular uma tabela principal às tabelas secundárias.

Elemento Reference

Os parâmetros no elemento Reference são os seguintes:

childcol

Indica a coluna na tabela secundária (especificada no elemento Table correspondente) que é mapeada para a coluna na tabela principal.

primarycol

Indica a coluna na tabela principal que é mapeada para a coluna na tabela secundária.

Observação: os parâmetros são opcionais, a menos que especificado em contrário.

Especificar informações do objeto

As informações do objeto são especificadas pelo fornecimento de valores para os vários parâmetros.

Siga estas etapas:

1. Localize o elemento ImsManagedObject na seção Objeto de usuário, Objeto de grupo ou Objeto de organização.
2. Forneça valores para os seguintes parâmetros:

   name

   (obrigatório)

   Fornece um nome exclusivo para o objeto gerenciado.

   description

   Fornece a descrição do objeto gerenciado.

   objecttype

   (obrigatório)

   Especifica o tipo de objeto gerenciado. Os valores válidos são os seguintes:

   - USER
   - GROUP
   - ORGANIZATION

   O elemento ImsManagedObject deve se parecer com o seguinte código:

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```

3. Forneça informações de tabela, conforme descrito em Tabelas de banco de dados (na página 117).

4. Especifique a coluna que contém o identificador exclusivo do objeto (na página 120).
5. Descreva os atributos que constituem o perfil do objeto (na página 121).
6. Se você estiver configurando um objeto de organização, vá para Gerenciamento de organizações (na página 148).

Como especificar o identificador exclusivo de um objeto gerenciado

Cada objeto que o CA Identity Manager gerencia deve ter um identificador exclusivo. Certifique-se de que o identificador exclusivo esteja armazenado em uma única coluna da tabela principal do objeto gerenciado. As tabelas principais são descritas em Tabelas de banco de dados (na página 117).

Use os elementos UniqueIdentifier e UniqueIdentifierAttr para definir o identificador exclusivo como se segue:

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="nome_da_tabela.nome_da_coluna" />
</UniqueIdentifier>
```

O elemento UniqueIdentifierAttr exige o parâmetro de nome. O valor do parâmetro de nome é o atributo no qual o identificador exclusivo está armazenado. O valor pode ser um atributo físico ou um atributo conhecido (na página 79).

Ao especificar um atributo físico, observe os seguintes pontos:

- Certifique-se de que o atributo especificado já exista no banco de dados e que esteja definido no arquivo de configuração de diretório, conforme descrito em Como modificar descrições de atributo (na página 121). Na descrição do atributo, não se esqueça de especificar a permissão somente leitura ou gravar uma vez para impedir que o identificador exclusivo mude durante uma sessão.
- Use a sintaxe a seguir para especificar um atributo físico:

  nome_da_tabela.nome_da_coluna

  nome_da_tabela

  Define o nome da tabela onde o atributo está localizado. A tabela que você especifica deve ser a tabela principal.

  nome_da_coluna

  Define o nome da coluna que armazena o atributo.

- Se o banco de dados gerar o identificador exclusivo, especifique uma operação personalizada para o atributo (na página 131). Por exemplo, pode ser necessário especificar uma operação que busque o último identificador gerado no banco de dados.

Como modificar as descrições de atributo

Um atributo armazena informações sobre uma entidade de usuário, grupo ou organização, como número de telefone ou endereço. Os atributos de uma entidade determinam seu perfil.

No arquivo de configuração de diretório, os atributos são descritos nos elementos ImsManagedObjectAttr. Nas seções Objeto de usuário, Objeto de grupo e Objeto de organização do arquivo de configuração de diretório:

- Modifique as descrições de atributo padrão para descrever os atributos do seu banco de dados.
- Criar novas descrições de atributo copiando uma descrição existente e modificando os valores conforme a necessidade.

Para cada atributo nos perfis de usuário, grupo e organização, há apenas um elemento ImsManagedObjectAttr. Por exemplo, um elemento ImsManagedObjectAttr pode descrever uma ID de usuário.

Um elemento ImsManagedObjectAttr se parece com o seguinte código:

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

Observação: quando você estiver usando um banco de dados Oracle, observe os seguintes pontos ao configurar os atributos de objeto gerenciado:

- Bancos de dados Oracle, por padrão, diferenciam maiúsculas e minúsculas. As maiúsculas e minúsculas de atributos e nomes de tabela no arquivo de configuração de diretório devem corresponder às maiúsculas e minúsculas dos atributos no Oracle.

  Não se esqueça de especificar um tamanho máximo para tipos de dados de sequência de caracteres para evitar o truncamento. Para limitar o tamanho das sequências de caracteres, você pode criar uma regra de validação para exibir um erro quando um usuário digitar uma sequência de caracteres que exceda o comprimento máximo.

Os parâmetros ImsManagedObjectAttr seguem abaixo.

Observação: os parâmetros são opcionais, a menos que especificado em contrário.

physicalname

(obrigatório)

Especifica o nome físico do atributo e deve conter um dos seguintes detalhes:

- O nome e o local em que o valor está armazenado.

  Formato: *nome_da_tabela.nome_da_coluna*

  Por exemplo, quando um atributo é armazenado na coluna ID na tabela tblUsers, o nome físico do atributo é o seguinte:

  tblUsers.id

  Também é necessário definir cada tabela que contém um atributo de um elemento Table (na página 117).

- Um atributo conhecido.

  Um atributo conhecido pode representar um valor calculado. Por exemplo, você pode usar um atributo conhecido para fazer referência a um atributo calculado usando uma operação personalizada (na página 131).

displayname

(obrigatório)

Especifica um nome exclusivo para o atributo.

No Console de usuário, o nome de exibição aparece na lista de atributos que estão disponíveis para adição a uma tela de tarefas.

Observação: não modifique o nome para exibição de um atributo no arquivo de configuração de diretório (directory.xml). Para alterar o nome do atributo em uma tela de tarefas, é possível especificar um rótulo para o atributo na definição da tela da tarefa. Para obter mais informações, consulte o *Guia de Administração*.

description

Fornece a descrição do atributo.

valuetype

Especifica o tipo de dados do atributo. Os valores válidos são os seguintes:

Sequência

O valor pode ser qualquer sequência de caracteres.

Esse é o valor padrão.

Inteiro

O valor deve ser um inteiro.

Observação: o tipo inteiro não oferece suporte a números decimais.

Número

O valor deve ser um inteiro. A opção de número oferece suporte a números decimais.

Data

O valor deverá ser uma data válida usando o padrão:

MM/dd/aaaa

ISODate

O valor deverá ser uma data válida usando o padrão aaaa-MM-dd.

UnicenterDate

O valor deverá ser uma data válida usando o padrão AAAAAAADDD onde:

AAAAAAA é uma representação de sete números de um ano que começa com três zeros. Por exemplo: 0002008

DDD é a representação de três números para o dia que começa com zeros, conforme a necessidade. Os valores válidos vão de 001 a 366.

Se o valuetype de um atributo está incorreto, as consultas do CA Identity Manager podem falhar.

Para verificar se um atributo foi armazenado corretamente no banco de dados, você poderá associá-lo a uma regra de validação.

required

Indica se um valor é necessário para especificar o atributo, conforme indicado a seguir:

- True — obrigatório
- False — opcional (padrão)

multi-valued

Indica se o atributo pode ter valores múltiplos, como se segue:

- True — um atributo pode ter valores múltiplos.
- False — um atributo pode ter apenas um único valor (padrão).

Por exemplo, o atributo de associação ao grupo em um perfil de usuário tem valores múltiplos para armazenar os grupos aos quais um usuário pertence.

Para armazenar atributos de valores múltiplos em uma lista delimitada, em vez de em uma tabela com várias linhas, você precisa definir o caractere delimitador no parâmetro correspondente.

Verifique se o número de valores possíveis e o comprimento de cada valor que a coluna permite são suficientes.

Importante: tenha certeza de que o atributo Associação ao grupo na definição de Objeto de usuário tem valores múltiplos.

wellknown

Fornece o nome do atributo conhecido.

Os atributos conhecidos têm um significado específico no CA Identity Manager.

Formato: %*NOME_DO_ATRIBUTO*%

Observação: quando uma operação personalizada é associada a um atributo, é necessário especificar um atributo conhecido (na página 79).

maxlength

Determina o tamanho máximo da coluna.

permission

Indica se o valor de um atributo pode ser modificado em uma tela, como se segue:

READONLY

O valor é exibido, mas não pode ser modificado.

WRITEONCE

O valor não poderá ser modificado depois que o objeto for criado. Por exemplo, uma ID de usuário não pode ser alterada após a criação do usuário.

READWRITE

O valor pode ser modificado (padrão).

hidden

Indica se um atributo será exibido nas telas de tarefas do CA Identity Manager, como se segue:

- True — o atributo não é exibido para os usuários.
- False — o atributo é exibido para os usuários (padrão).

Os atributos lógicos usam atributos ocultos.

Observação: para obter mais informações sobre os atributos lógicos, consulte o *Guia de Programação do Java*.

system

Indica que apenas o CA Identity Manager usou atributos. Os usuários não devem modificar os atributos no Console de usuário, como segue:

- True — os usuários não podem modificar o atributo. O atributo não será exibido no Console de usuário.
- False — os usuários podem modificar esse atributo, que está disponível para ser adicionado à telas de tarefas no Console de usuário (padrão).

validationruleset

Associa um conjunto de regras de validação ao atributo.

Verifique se o conjunto de regras de validação que você especifica está definido em uma elemento ValidationRuleSet no arquivo de configuração de diretório.

delimiter

Define o caractere que separa os valores quando vários valores são armazenados em uma única coluna.

Importante: certifique-se de que o parâmetro com valores múltiplos esteja definido como verdadeiro para que o parâmetro delimitador se aplique.

Observação: para evitar a exibição de informações confidenciais, como senhas ou os salários, no Console de usuário, você pode especificar os parâmetros DataClassification (na página 74).

Gerenciando atributos confidenciais

O CA Identity Manager oferece os seguintes métodos para gerenciamento de atributos confidenciais:

- Classificações de dados para atributos

  As classificações de dados permitem especificar as propriedades de exibição e criptografia para atributos no arquivo de configuração de diretório (directory.xml).

  Você pode definir as classificações de dados que gerenciam atributos confidenciais, como se segue:

  - Nas telas de tarefa do CA Identity Manager, exiba o valor de um atributo como uma série de asteriscos.

    Por exemplo, é possível exibir as senhas como asteriscos, em vez de exibi-las em texto não criptografado.

  - Nas telas Exibir tarefas enviadas, oculte o valor do atributo.

    Essa opção permite ocultar os atributos dos administradores. Por exemplo, ocultar os detalhes de salário, como o salário de administradores que exibirem o status da tarefa no CA Identity Manager, mas que não precisam exibir os detalhes de salário.

- Ignore determinados atributos ao criar uma cópia de um objeto existente.
- Criptografe um atributo

- Estilos de campo nas telas de perfil de tarefa

  Se não desejar modificar um atributo no arquivo directory.xml, defina a propriedade de exibição para o atributo nas definições de tela onde o atributo confidencial aparece.

  O estilo de campo permite exibir atributos, como senhas, como uma série de asteriscos em vez de texto não criptografado.

  Observação: para obter mais informações sobre o estilo de campo para atributos confidenciais, procure estilos de campo na ajuda do Console de usuário.

Atributos de classificação de dados

O elemento Classificação de dados fornece um meio de associar as propriedades adicionais a uma descrição do atributo. Os valores nesse elemento determinam como o CA Identity Manager trata o atributo. Esse elemento oferece suporte aos seguintes parâmetros:

- sensitive

  Faz com que o CA Identity Manager exiba o atributo como uma série de asteriscos (*) nas telas Exibir tarefas enviadas. Esse parâmetro evita que valores novos e antigos do atributo apareçam em texto não criptografado nas telas Exibir tarefas enviadas.

  Além disso, se você criar uma cópia de um usuário existente no Console de usuário, esse parâmetro evitará que o atributo seja copiado para o novo usuário.

- vst_hide

  Oculta o atributo na tela Detalhes do evento para a guia Exibir tarefas enviadas. Ao contrário dos atributos confidenciais, que são exibidos como asteriscos, os atributos vst_hidden não são exibidos.

  É possível usar esse parâmetro para evitar que alterações em um atributo, como o salário, sejam exibidas em Exibir tarefas enviadas.

- ignore_on_copy

  Faz com que o CA Identity Manager ignore um atributo quando um administrador cria uma cópia de um objeto no Console de usuário. Por exemplo, suponha que você tenha especificado ignore_on_copy para o atributo de senha em um objeto de usuário. Ao copiar um perfil de usuário, o CA Identity Manager não aplica a senha do usuário atual ao novo perfil de usuário.

- AttributeLevelEncrypt

  Criptografa os valores de atributo quando eles são armazenados no repositório de usuários. Se o CA Identity Manager for ativado para o FIPS 140-2, o CA Identity Manager usará a criptografia RC2 ou FIPS 140-2.

  Para obter mais informações sobre suporte ao FIPS 140-2 no CA Identity Manager, consulte o *Guia de Configuração*.

  Os atributos são exibidos em texto não criptografado durante o tempo de execução.

  Observação: para impedir que os atributos apareçam em texto não criptografado nas telas, você também pode adicionar um elemento de classificação de dados confidencial aos atributos criptografados. Para obter mais informações, consulte Como adicionar criptografia em nível de atributo (na página 75).

- PreviouslyEncrypted

  Faz com que o CA Identity Manager detecte e descriptografe todos os valores criptografados no atributo quando ele acessa o objeto no repositório de usuários.

  Você usa essa classificação de dados para descriptografar todos os valores criptografados anteriormente.

  O valor do texto não criptografado é salvo no repositório quando você salva o objeto.

Configurar atributos de classificação de dados

Siga estas etapas:

1. Localize o atributo no arquivo de configuração de diretório.
2. Após a descrição do atributo, adicione o seguinte atributo:

   <DataClassification name="*parameter*">

   parameter

   Representa um dos seguintes parâmetros:

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   Por exemplo, uma descrição do atributo que inclua o atributo de classificação de dados vst_hide se parece com o código a seguir:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

Criptografia em nível de atributo

É possível criptografar um atributo no repositório de usuários especificando uma classificação de dados AttributeLevelEncypt para esse atributo no arquivo de configuração de diretório (directory.xml). Quando a criptografia em nível de atributo é ativada, o CA Identity Manager criptografa o valor do atributo antes de armazená-lo no repositório de usuários. O atributo é exibido como texto não criptografado no Console de usuário.

Observação: para impedir que os atributos apareçam em texto não criptografado nas telas, você também pode adicionar um elemento de classificação de dados confidencial aos atributos criptografados. Para obter mais informações, consulte Como adicionar criptografia em nível de atributo (na página 75).

Se o suporte ao FIPS 140-2 for ativado, o atributo será criptografado usando a criptografia RC2 ou FIPS 140-2.

Antes de implementar a criptografia em nível de atributo, observe o seguinte:

- O CA Identity Manager não pode localizar atributos criptografados em uma pesquisa.

  Suponha que um atributo criptografado seja adicionado a uma política de integrante, administrador, proprietário ou identidade. O CA Identity Manager não pode resolver a política corretamente porque não pode pesquisar o atributo.

  Considere a definição do atributo para searchable="false" no arquivo directory.xml. Por exemplo:

  <ImsManagedObjectAttr physicalname="title" description="Title" displayname="Title" valuetype="String" maxlength="0" searchable="false">

  <DataClassification name="AttributeLevelEncrypt"/>

  </ImsManagedObjectAttr>

- Se o CA Identity Manager usa um repositório de usuários compartilhado e o Diretório de provisionamento, não criptografe os atributos do Servidor de provisionamento.
- Não ative AttributeLevelEncrypt para senhas de usuário em ambientes que atendam aos seguintes critérios:
  - Inclua a integração do CA SiteMinder e
  - Armazene usuários em um banco de dados relacional.

  Quando o CA Identity Manager se integra ao CA SiteMinder, as senhas criptografadas podem provocar problemas quando novos usuários tentam efetuar logon e inserem senhas em texto não criptografado.
- Se você ativar a criptografia em nível de atributo para um repositório de usuários que é usado por aplicativos diferentes do CA Identity Manager, os outros aplicativos não poderão usar o atributo criptografado.

Como adicionar criptografia em nível de atributo

Suponha que você tenha adicionado uma criptografia em nível de atributo a um diretório do CA Identity Manager. O CA Identity Manager criptografa automaticamente os valores de atributo de texto não criptografado existentes quando você salva o objeto que é associado ao atributo. Por exemplo, a criptografia do atributo de senha criptografa a senha quando o perfil do usuário é salvo.

Observação: para criptografar o valor do atributo, a tarefa que você usa para salvar o objeto deve incluir o atributo. Para criptografar o atributo de senha no exemplo anterior, certifique-se de que o campo da senha seja adicionado à tarefa que você usa para salvar o objeto, como a tarefa Modificar usuário.

Todos os novos objetos são criados com valores criptografados no repositório de usuários.

Siga estas etapas:

1. Execute uma das tarefas a seguir:
   - Crie um diretório do CA Identity Manager
   - Atualize um diretório existente exportando as configurações de diretório.
2. Adicione os seguintes atributos de classificação de dados ao atributo que deseja criptografar no arquivo directory.xml:

   AttributeLevelEncrypt

   Persiste o valor do atributo em uma forma criptografada no repositório de usuários.

   sensitive (opcional)

   Oculta o valor do atributo em telas do CA Identity Manager. Por exemplo, uma senha é exibida como asteriscos (*).

   Por exemplo:

```
<ImsManagedObjectAttr physicalname="salary"
displayname="Salary" description="salary" valuetype="String"
required="false" multivalued="false" maxlength="0"
searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. Se você criou um Diretório do CA Identity Manager, associe-o a um ambiente.
4. Para forçar o CA Identity Manager a criptografar todos os valores imediatamente, modifique todos os objetos usando o Carregador de itens em massa.

   Observação: para obter mais informações sobre o Carregador de itens em massa, consulte o *Guia de Administração*.

Como remover criptografia em nível de atributo

Se você tiver um atributo criptografado no Diretório do CA Identity Manager e ele for armazenado com o valor desse atributo como texto não criptografado, será possível remover a classificação de dados AttributeLevelEncrypt.

Depois que a classificação de dados tiver sido removida, o CA Identity Manager interromperá a criptografia dos novos valores de atributos. Os valores existentes são descriptografados quando você salva o objeto associado ao atributo.

Observação: para descriptografar o valor do atributo, a tarefa que você usa para salvar o objeto deve incluir o atributo. Por exemplo, para descriptografar uma senha de um usuário existente, você salva o objeto de usuário com uma tarefa que inclui o campo de senha, como a tarefa Modificar usuário.

Para forçar o CA Identity Manager a detectar e descriptografar todos os valores criptografados que permanecem no repositório de usuários do atributo, é possível especificar outra classificação de dados, PreviouslyEncrypted. O valor do texto não criptografado é salvo no repositório de usuários quando você salva o objeto.

Observação: adicionar a classificação de dados PreviouslyEncrypted adiciona mais processamento em cada carga de objeto. Para evitar problemas de desempenho, considere a adição da classificação de dados PreviouslyEncrypted, carregando e salvando cada objeto associado a esse atributo e, em seguida, removendo a classificação de dados. Esse método converte automaticamente todos os valores criptografados armazenados em texto não criptografado armazenado.

Siga estas etapas:

1. Exporte as configurações de diretório para o Diretório adequado do CA Identity Manager.
2. No arquivo directory.xml, remova a classificação de dados, AttributeLevelEncrypt, de atributos que deseja descriptografar.
3. Se quiser forçar o CA Identity Manager a remover valores criptografados anteriormente, adicione o atributo de classificação de dados PreviouslyEncrypted.

   Por exemplo:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. Para forçar o CA Identity Manager a descriptografar todos os valores imediatamente, modifique todos os objetos usando o Carregador de itens em massa.

   Observação: para obter mais informações sobre o Carregador de itens em massa, consulte o *Guia de Administração*.

Operações personalizadas

Você pode definir operações personalizadas para que determinados objetos gerenciados executem as seguintes tarefas:

- Usar procedimentos armazenados
- Otimizar consultas para sua estrutura de banco de dados.
- Recuperar um identificador exclusivo gerado pelo banco de dados.

As operações personalizadas se aplicam somente a atributos.

Ao especificar operações personalizadas, lembre-se dos seguintes pontos:

- Os usuários que especificam operações personalizadas devem estar familiarizados com o SQL.
- O CA Identity Manager não valida operações personalizadas. Até o tempo de execução, os erros de sintaxe e as consultas inválidas não são reportados.
- Se você especificar uma operação personalizada para um atributo, não será possível usar esse atributo nos filtros de pesquisa em tarefas do CA Identity Manager.
- As operações personalizadas devem estar de acordo com os padrões XML. Represente caracteres especiais usando a sintaxe XML. Por exemplo, especifique aspas simples (') como '

Para especificar uma operação personalizada, use o elemento Operation.

Elemento Operation

O elemento Operation define uma instrução SQL que pode executar uma consulta personalizada ou chama um procedimento armazenado para criação, recuperação, modificação ou exclusão de um atributo. O elemento Operation é um subelemento do elemento IMSManagedObjectAttr, conforme mostrado no exemplo a seguir:

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Os parâmetros do elemento Operation são os seguintes:

name

Especifica um nome predefinido para uma operação. As operações válidas são as seguintes:

- Criar
- Obter
- Definir
- Excluir
- GetDB

  A operação GetDB recupera um identificador exclusivo do banco de dados durante uma tarefa de criação, quando o identificador exclusivo é gerado por meio do banco de dados ou de um procedimento armazenado.

value

Define a instrução SQL ou o procedimento armazenado a ser executado. Os valores válidos são os seguintes:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (para procedimentos armazenados)

Observação: os parâmetros são opcionais, a menos que especificado em contrário.

O elemento Operation pode conter um ou mais elementos Parameter.

Elemento Parameter

Um elemento Parameter especifica os valores que são passados à consulta. Quando vários elementos Parameter são definidos, os valores são passados à consulta em uma determinada ordem listada.

Um elemento Parameter exige o parâmetro de nome. O valor do parâmetro de nome pode ser um atributo físico ou um atributo conhecido (na página 79).

Observação: o CA Identity Manager deve entender os valores que são passados a uma consulta no elemento Parameter. Por exemplo, o valor pode ser um nome físico ou um atributo conhecido que é definido nos atributos ImsManagedObjectAttr.

Ao especificar um atributo físico, observe os seguintes pontos:

- Use a sintaxe a seguir para especificar um atributo físico:

  nome_da_tabela.nome_da_coluna

  - *nome_da_tabela*

    Fornece o nome da tabela onde o atributo está localizado. A tabela que você especifica deve ser a tabela principal.

  - *nome_da_coluna*

    Fornece o nome da coluna que armazena o atributo.

- O atributo que você especifica deve existir no banco de dados e é definido no arquivo de configuração de diretório, conforme descrito em Como modificar descrições de atributo (na página 121).

Exemplo: operações personalizadas para o atributo Business Number

No exemplo a seguir, o atributo Business Number é gerado com uma chamada a um procedimento armazenado; ele não é um atributo físico no banco de dados.

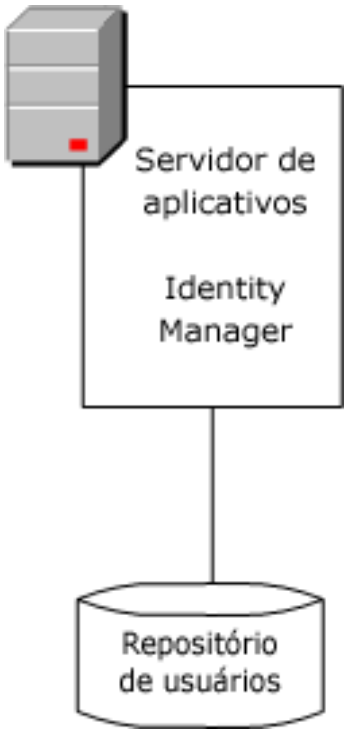
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

Observe os seguintes pontos:

- sp_getbusinessnumber, sp_setbusinessnumber e sp_deletebusinessnumber são procedimentos armazenados definidos pelo usuário.
- O valor retornado da operação Get é mapeado para o atributo %BUSINESS_NUMBER%.
- O ponto de interrogação (?) indica substituições feitas no tempo de execução antes da execução da consulta. Por exemplo, na operação Get, o atributo conhecido %USER_ID% é passado ao procedimento armazenado sp_getbusinessnumber.

Conexão com o diretório de usuários

O CA Identity Manager se conecta a um diretório de usuários para armazenar informações, como informações de um usuário, um grupo ou organizacionais, como mostrado na ilustração a seguir:



Não é necessário um novo diretório ou banco de dados. No entanto, o diretório ou banco de dados existente deve estar em um sistema que tenha um FQDN (fully qualified domain name - nome de domínio totalmente qualificado).

Para obter uma lista de tipos de banco de dados e diretório suportados, consulte a matriz de suporte do CA Identity Manager no Site de suporte da CA.

É possível configurar uma conexão com o repositório de usuários quando você cria um diretório do CA Identity Manager no Management Console.

Se você exportar a configuração de diretório após a criação de um diretório do CA Identity Manager, as informações de conexão com o diretório de usuários serão exibidas no elemento Provider do arquivo de configuração de diretório.

Descrição de uma conexão com o banco de dados

Para descrever uma conexão com o banco de dados, use o elemento Provider e seus subelementos no arquivo directory.xml.

Observação: se você estiver criando um diretório do CA Identity Manager, não será necessário fornecer informações de conexão no arquivo directory.xml. Forneça informações de conexão no assistente de diretório do CA Identity Manager no Management Console.

Modifique o elemento Provider apenas para atualizações.

Elemento Provider

O elemento Provider inclui os seguintes subelementos:

JDBC (obrigatório)

Identifica a origem de dados JDBC a ser usada ao conectar-se ao repositório de usuários. Especifique o nome JNDI que você forneceu ao criar a origem de sados JDBC (na página 107).

Credentials (obrigatório)

Fornece o nome de usuário e a senha para acessar o banco de dados.

DSN

Identifica a origem de dados ODBC a ser usada ao conectar-se ao repositório de usuários.

Observação: esse subelemento se aplica apenas quando o CA Identity Manager integra-se ao SiteMinder. Em ambientes do CA Identity Manager que não incluem o SiteMinder, esse subelemento é ignorado.

SiteMinderQuery

Especifica esquemas de consulta personalizados para localização de informações do usuário em um banco de dados relacional.

Observação: esse subelemento se aplica apenas quando o CA Identity Manager integra-se ao SiteMinder. Em ambientes do CA Identity Manager que não incluem o SiteMinder, esse subelemento é ignorado.

Uma conexão com o banco de dados concluída é semelhante ao seguinte exemplo:

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Os atributos do elemento Provider são os seguintes:

type

Especifica o tipo de banco de dados. Para os bancos de dados Microsoft SQL Server e Oracle, especifique RDB (padrão).

userdirectory

Especifica o nome da conexão do diretório de usuários. Esse parâmetro corresponde ao nome do Objeto de conexão que você fornece durante a criação do diretório.

Se o CA Identity Manager integrar-se ao SiteMinder para autenticação, ele criará uma conexão com o diretório de usuários no SiteMinder usando o nome que você especifica para o Objeto de conexão durante a instalação. Se você quiser se conectar a um diretório de usuários existente do SiteMinder, digite o nome desse diretório quando solicitado pelo Objeto de conexão. O CA Identity Manager preenche o parâmetro userdirectory com o nome que você especifica.

Se o CA Identity Manager não se integrar ao SiteMinder, o valor do parâmetro userdirectory será qualquer nome que você fornecer a uma conexão JDBC com o repositório de usuários.

Observação: não especifique um nome para a conexão com o diretório de usuários no arquivo directory.xml. O CA Identity Manager solicita que você forneça o nome durante a criação do diretório.

Credenciais de banco de dados

Para se conectar ao banco de dados, o CA Identity Manager deve fornecer credenciais válidas para a origem de dados. As credenciais são definidas no subelemento Credentials, que se parece com o seguinte exemplo:

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Se você não especificar uma senha no elemento Credentials e tentar criar o diretório do CA Identity Manager no Management Console, ele solicitará as credenciais da senha.

Observação: é recomendável especificar a senha no Management Console.

Ao especificar a senha no Management Console, o CA Identity Manager a criptografará para você. Caso contrário, se você não quiser que a senha seja exibida em texto não criptografado, criptografe a senha usando a ferramenta de senha que é instalada com o CA Identity Manager. As Senhas do SiteMinder apresentam instruções sobre como usar a senha.

Observação: é possível especificar apenas um conjunto de credenciais. Ao definir várias origens de dados, as credenciais que você especifica devem se aplicar a todas as origens de dados.

Os parâmetros de credencial seguem abaixo:

user

Define a ID de logon de uma conta que pode acessar a origem de dados.

Não especifique um valor para o parâmetro de usuário no arquivo directory.xml. O CA Identity Manager solicita que você forneça a ID de logon criada no diretório do CA Identity Manager no Management Console.

cleartext

Determina se a senha é exibida em texto não criptografado no arquivo directory.xml:

- True — a senha é exibida em texto não criptografado.
- False — a senha é criptografada (padrão).

Observação: esses parâmetros são opcionais.

DSN (Data Source Name - nome da origem de dados)

O elemento DSN no arquivo directory.xml tem um parâmetro — o nome da origem de dados ODBC que o CA Identity Manager usa para se conectar ao banco de dados. O valor do parâmetro de nome deve corresponder ao nome de uma origem de dados existente.

Observação: esse elemento se aplica apenas quando o CA Identity Manager integra-se ao SiteMinder. Se o CA Identity Manager não se integrar ao SiteMinder, esse elemento será ignorado.

Se o valor do parâmetro de nome for @SmDirDSN, não será necessário especificar um nome DSN no arquivo directory.xml. O CA Identity Manager solicita o nome DSN quando você importa o arquivo directory.xml.

Para configurar uma tolerância a falhas, defina vários elementos DSN. Se a origem de dados principal falhar ao responder a uma solicitação, a próxima origem de dados definida responderá à solicitação.

Por exemplo, suponha que você tenha configurado a tolerância a falhas da seguinte maneira:

```
<DSN name="DSN1">
<DSN name="DSN2">
```

O CA Identity Manager usa a origem de dados DSN1 para se conectar ao banco de dados. Se houver um problema com DSN1, o CA Identity Manager tentará se conectar ao banco de dados usando DSN2.

Observação: as credenciais especificadas no elemento Credentials (na página 137) devem se aplicar a todos os DSNs que você define.

Esquemas de consulta SQL

O CA Identity Manager usa esquemas de consulta para localizar informações de usuários e grupos em um banco de dados relacional.

Observação: esse elemento se aplica apenas quando o CA Identity Manager integra-se ao SiteMinder. Em ambientes que não incluem o SiteMinder, esse parâmetro é ignorado.

Quando você cria um diretório do CA Identity Manager no Management Console, o CA Identity Manager gera um conjunto de esquemas de consulta que têm com base os esquemas de consulta necessários no SiteMinder. (Para obter informações completas sobre os esquemas de consulta do SiteMinder, consulte o *Guia de Configuração do Servidor de Políticas do CA SiteMinder Web Access Manager*.) Os nomes de tabela e coluna nos esquemas de consulta do SiteMinder são substituídos por dados especificados no arquivo de configuração de diretório.

Como definir esquemas de consulta personalizados

Os esquemas de consulta são definidos nos elementos SiteMinderQuery no arquivo de configuração de diretório. Um elemento SiteMinderQuery é semelhante a este:

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

Observação: na amostra de consulta, ' é a sintaxe XML para as aspas simples (’).

O elemento SiteMinderQuery se aplica apenas quando o CA Identity Manager integra-se ao SiteMinder.

Os parâmetros do esquema de consulta são os seguintes:

name

Especifica o nome redefinido de um esquema de consulta do SiteMinder.

Não o modifique esse valor.

query

Especifica a instrução SQL ou o procedimento armazenado a ser executado. Os valores válidos são os seguintes:

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL (para procedimentos armazenados)

Observação: esses parâmetros são obrigatórios para o elemento SiteMinderQuery.

Antes de personalizar esquemas de consulta, faça o seguinte:

- Familiarize-se com os esquemas de consulta padrão.

  Observação: para obter mais informações sobre esquemas de consulta SQL, consulte o *Guia de Configuração do Servidor de Políticas do CA SiteMinder Web Access Manager*.

- Adquira uma vasta experiência em desenvolvimento de consultas SQL.

Modificar esquemas de consulta padrão

Execute o procedimento a seguir para modificar os esquemas de consulta padrão.

Siga estas etapas:

1. Exporte o arquivo de configuração de diretório.

   O CA Identity Manager gera um arquivo de configuração de diretório que contém todas as configurações atuais para o diretório do CA Identity Manager, incluindo os esquemas de consulta gerados.

2. Salve o arquivo de configuração de diretório.

   Observação: se desejar criar um backup do arquivo de configuração de diretório original, salve o arquivo com outro nome ou em outro local antes de salvar o arquivo exportado.

3. Localize o esquema de consulta gerado pelo CA Identity Manager que você deseja modificar.

4. Insira o esquema de consulta ou o procedimento armazenado a ser executado no parâmetro de consulta.

   Observação: não modifique o nome da consulta.

5. Depois de fazer as alterações necessárias, salve o arquivo de configuração de diretório.

   Importe o arquivo para atualizar o Diretório do CA Identity Manager (na página 184).

Atributos conhecidos para um banco de dados relacional

Os atributos conhecidos têm um significado especial no CA Identity Manager. Eles são identificados pela seguinte sintaxe:

%ATTRIBUTENAME%

Nessa sintaxe, *ATTRIBUTENAME* deve ter letras maiúsculas.

Um atributo conhecido é mapeado para um atributo físico usando uma descrição de atributo (na página 121).

Na descrição de atributo a seguir, o atributo tblUsers.password é mapeado para o atributo conhecido %PASSWORD% para que o CA Identity Manager trate o valor em tblUsers.password como uma senha:

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Alguns atributos conhecidos são obrigatórios; outros são opcionais.

Atributos conhecidos de usuário

Veja a seguir uma lista de atributos conhecidos de usuário:

%ADMIN_ROLE_CONSTRAINT%

Contém a lista de funções administrativas (na página 145) que são atribuídas ao administrador (na página 145).

O atributo físico que é mapeado para %ADMIN_ROLE_CONSTRAINT% deve possuir valores múltiplos para acomodar várias funções.

Aconselhamos a indexação do atributo que é mapeado para %ADMIN_ROLE_CONSTRAINT%.

%CERTIFICATION_STATUS%

(Obrigatório para usar o recurso de certificação de usuário)

Contém o status de certificação de um usuário.

Observação: para obter mais informações sobre a certificação de usuário, consulte o *Guia de Administração*.

%DELEGATORS%

Mapeia para uma lista de usuários que delegou itens de trabalho ao usuário atual.

Esse atributo é exigido para usar a delegação. O atributo físico mapeado para %DELEGATORS% deve possuir valores múltiplos e ser capaz de manter as sequências de caracteres.

Importante: Editar esse campo diretamente usando as tarefas ou uma ferramenta externa do CA Identity Manager pode causar implicações de segurança significativas.

%EMAIL%

(Obrigatório para ativar o recurso de notificação por email)

Armazena o endereço de email de um usuário.

%ENABLED_STATE%

(obrigatório)

Rastreia o status de um usuário.

Observação: o tipo de dados do atributo físico que é mapeado para %ENABLED_STATE% deve ser uma sequência de caracteres.

%FIRST_NAME%

Contém o nome de um usuário.

%FULL_NAME%

(obrigatório)

Contém o nome e o sobrenome de um usuário.

%IDENTITY_POLICY%

Contém a lista de políticas de identidade que foram aplicadas a uma conta de usuário.

O CA Identity Manager usa esse atributo para determinar se uma política de identidade deve ser aplicada a um usuário. Se a política tiver a configuração Aplicar uma vez ativada e a política estiver listada no atributo %IDENTITY_POLICY%, o CA Identity Manager não aplicará as alterações na política para o usuário.

Observação: para obter mais informações sobre políticas de identidade, consulte o *Guia de Administração*.

%LAST_CERTIFIED_DATE%

(Obrigatório para usar o recurso de certificação de usuário)

Contém a data em que a função de um usuário foi certificada.

Observação: para obter mais informações sobre a certificação de usuário, consulte o *Guia de Administração*.

%LAST_NAME%

Contém o sobrenome de um usuário.

%ORG_MEMBERSHIP%

(Obrigatório quando as organizações são suportadas)

Contém o identificador exclusivo da organização à qual o usuário pertence.

%ORG_MEMBERSHIP_NAME%

(Obrigatório quando as organizações são suportadas)

Contém o nome amigável da organização à qual o usuário pertence.

%PASSWORD%

Contém a senha de um usuário.

Observação: o valor do atributo %PASSWORD% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%PASSWORD_DATA%

(Necessário para suporte à política de senha)

Especifica o atributo que rastreia as informações da política de senha.

Observação: o valor do atributo %PASSWORD_DATA% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%PASSWORD_HINT%

(obrigatório)

Contém os pares de pergunta e resposta especificados pelo usuário. Os pares de pergunta e resposta são usados no caso de esquecimento de senhas.

Observação: o valor do atributo %PASSWORD_HINT% é sempre exibido como uma série de asteriscos (*) nas telas do CA Identity Manager, mesmo quando o atributo ou campo não é definido para ocultar senhas.

%USER_ID%

(obrigatório)

Armazena uma ID de logon de usuário.

Atributos conhecidos de grupo

Veja a seguir uma lista de atributos conhecidos de grupo:

%GROUP_ADMIN%

Contém os administradores de um grupo.

Observação: o atributo %GROUP_ADMIN % deve ter valores múltiplos.

%GROUP_DESC%

Contém a descrição de um grupo.

%GROUP_ID%

Contém o identificador exclusivo de um grupo.

%GROUP_MEMBERSHIP%

(obrigatório)

Contém uma lista de integrantes de um grupo.

Observação: o atributo %GROUP_MEMBERSHIP% deve ter valores múltiplos.

%GROUP_NAME%

(obrigatório)

Armazena o nome de um grupo.

%ORG_MEMBERSHIP%

(Obrigatório quando as organizações são suportadas).

Contém o identificador exclusivo da organização à qual o grupo pertence.

%ORG_MEMBERSHIP_NAME%

(Obrigatório quando as organizações são suportadas).

Contém o nome amigável da organização à qual o grupo pertence.

%SELF_SUBSCRIBING%

Determina se os usuários podem se inscrever em um grupo.

Atributo %Admin_Role_Constraint%

Ao criar uma função administrativa, você especifica uma ou mais regras de associação da função. Os usuários que atendem às regras de associação têm a função. Por exemplo, se a regra de associação para a função Gerenciador de usuários for title=User Manager, os usuários que possuírem o cargo Gerenciador de usuários terão a função Gerenciador de usuários.

Observação: para obter mais informações sobre regras, consulte o *Guia de Administração*.

%ADMIN_ROLE_CONSTRAINT% permite designar um atributo de perfil para armazenar todas as funções administrativas de um administrador.

Como usar o atributo %ADMIN_ROLE_CONSTRAINT%

Para usar %ADMIN_ROLE_CONSTRAINT% como a restrição para todas as funções administrativas, execute as seguintes tarefas:

- Emparelhe o atributo conhecido %ADMIN_ROLE_CONSTRAINT% com um atributo de perfil de valor múltiplo para acomodar várias funções.
- Quando você configura uma função administrativa na interface de usuário do CA Identity Manager, o seguinte cenário pode ser uma restrição:

  Funções administrativas igual a *nome da função*

  nome da função

  Define o nome da função para a qual você está fornecendo a restrição.

  Por exemplo, Funções administrativas igual a Gerenciador de usuários

Observação: Funções administrativas é o nome para exibição padrão do atributo %ADMIN_ROLE_CONSTRAINT%.

Configurar atributos conhecidos

Execute o procedimento a seguir para configurar atributos conhecidos.

Siga estas etapas:

1. No arquivo de configuração de diretório, procure pelo seguinte sinal:

   ##

   Os valores obrigatórios são identificados por dois sinais de cerquilha (##).

2. Substitua o valor que é iniciado por ## pelo nome físico do atributo que você deseja, como ele existe no banco de dados. Forneça o nome do atributo usando o seguinte formato:

   nome_da_tabela.nome_da_coluna

   Por exemplo, se o atributo de senha for armazenado na coluna de senha na tabela tblUsers, especifique-o da seguinte forma:

   `tblUsers.password`

3. Repita as Etapas 1 e 2 até que tenha substituído todos os valores necessários e incluído os valores opcionais que deseja.

4. Mapeie os atributos conhecidos opcionais para atributos físicos, conforme a necessidade.

5. Salve o arquivo de configuração de diretório.

Como configurar grupos com autoinscrição

Você pode permitir que os usuários de autoatendimento ingressem em grupos configurando o suporte para grupos com autoinscrição no arquivo de configuração de diretório.

Siga estas etapas:

1. Na seção Grupos com autoinscrição, adicione um elemento SelfSubscribingGroups da seguinte forma:

   `<SelfSubscribingGroups type=`*`tipo_de_pesquisa`* `org=`*`dn_org`*`>`

2. Digite valores para os seguintes parâmetros:

   type

   Indica onde o CA Identity Manager procura grupos com autoinscrição. Os valores válidos são os seguintes:

   - NONE — o CA Identity Manager não procura grupos. Especifique NONE para impedir que os usuários se inscrevam em grupos.
   - ALL — o CA Identity Manager pesquisa todos os grupos no repositório de usuários. Especifique ALL quando os usuários puderem se inscrever em todos os grupos.
   - INDICATEDORG (*somente para ambientes que oferecem suporte a organizações*) — o CA Identity Manager pesquisa grupos com autoinscrição na organização de um usuário e em suas suborganizações. Por exemplo, quando o perfil de um usuário estiver na organização Marketing, o CA Identity Manager irá procura grupos com autoinscrição na organização Marketing e em todas as suborganizações.
   - SPECIFICORG (*somente para ambientes que oferecem suporte a organizações*) — o CA Identity Manager pesquisa em uma organização específica. Forneça o identificador exclusivo da organização específica no parâmetro org.

   org

   Define o identificador exclusivo da organização em que o CA Identity Manager procura grupos com autoinscrição.

   Observação: certifique-se de especificar o parâmetro org se type=SPECIFICORG.

3. Reinicie o Servidor de políticas do SiteMinder, caso tenha alterado algum dos seguintes itens:
   - O parâmetro de tipo para ou de SPECIFICORG
   - O valor do parâmetro org

Assim que o suporte para grupos com autoinscrição for configurado no diretório do CA Identity Manager, os administradores do CA Identity Manager poderão especificar quais grupos têm autoinscrição no Console de usuário.

Quando um usuário se autorregistra, o CA Identity Manager procura grupos nas organizações especificadas e exibe os grupos com autoinscrição para o usuário.

Regras de validação

Uma regra de validação impõe requisitos em dados que um usuário digita em um campo da tela de tarefas. Os requisitos podem aplicar um tipo de dados ou um formato, ou podem garantir que os dados sejam válidos no contexto de outros dados na tela de tarefas.

As regras de validação são associados aos atributos de perfil. Para que uma tarefa seja processada, o CA Identity Manager garante que os dados inseridos para um atributo de perfil atendam a todas as regras de validação associadas.

É possível definir regras de validação e associá-las aos atributos de perfil no arquivo de configuração de diretório.

Gerenciamento da organização

Para bancos de dados relacionais, o CA Identity Manager tem a opção de gerenciamento das organizações. Quando o banco de dados oferece suporte às organizações, os seguintes pontos são verdadeiros:

- As organizações têm uma estrutura hierárquica.
- Todos os objetos gerenciados, como usuários, grupos e outras organizações pertencem a uma organização.
- Quando você exclui uma organização, os objetos pertencentes a ela são excluídos também.

Configure o objeto de organização do mesmo modo que configura os objetos de usuário e grupo com algumas etapas adicionais.

Como configurar o suporte à organização

Implemente as seguintes etapas para configurar o suporte à organização:

1. Configure o suporte à organização no banco de dados (na página 149).
2. Descreva o objeto de organização no ImsManagedObject (na página 116).

   Não se esqueça de configurar os subelementos Table e UniqueIdentifier.
3. Configure a organização de nível superior (na página 149).
4. Descreva os atributos (na página 121) que constituem uma organização.
5. Defina os atributos conhecidos para o objeto de organização (na página 150).

Configurar o suporte à organização no banco de dados

Siga estas etapas:

1. Abra um dos seguintes scripts SQL em um editor:
   - Bancos de dados do Microsoft SQL Server:

     ims_mssql_rdb.sql
   - Bancos de dados Oracle:

     ims_oracle_rdb.sql

     Esses arquivos estão localizados no seguinte diretório:

     ferramentas_administrativas\directoryTemplates\RelationalDatabase

     ferramentas_administrativas se refere ao local de instalação das Ferramentas administrativas que são instalados por padrão em um dos seguintes locais:

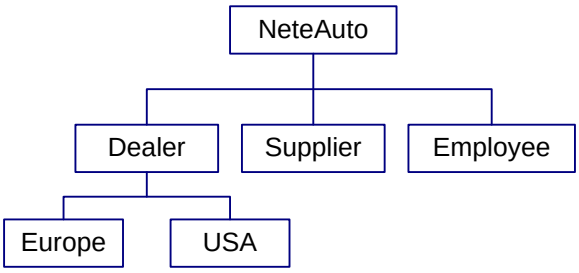
     Windows: <caminho_de_instalação>\tools

     UNIX: <caminho_de_instalação2>/tools
2. No script SQL, procure e substitua <@primary organization table@> pelo nome da tabela principal para o objeto da organização. Salve o script SQL.
3. Execute o script SQL no banco de dados.

Especificação da organização raiz

A organização raiz atua como nível mais alto ou pai da organização, no diretório. Todas as organizações se relacionam à organização raiz.

Na ilustração a seguir, NeteAuto é a organização raiz. As outras organizações são suborganizações da NeteAuto:



A definição de uma organização raiz completa se parece com o seguinte exemplo:

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

Após definir as informações básicas do objeto de organização, incluindo as tabelas que constituem o perfil da organização e o identificador exclusivo do objeto de organização, especifique a raiz de sua organização no arquivo directory.xml:

- No parâmetro de valor do elemento RootOrg, defina a consulta que o CA Identity Manager usa para recuperar a organização raiz, como no exemplo a seguir:

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- No parâmetro de nome do elemento Result, digite o identificador exclusivo da organização, como no exemplo a seguir:

  ```
  <Result name="%ORG_ID%" />
  ```

  Observação: o valor do parâmetro de nome deve ser o identificador exclusivo do objeto de organização.

Atributos conhecidos de organizações

Defina os atributos conhecidos para os atributos de um perfil de organização, conforme descrito em Atributos conhecidos (na página 79).

Os atributos conhecidos obrigatórios e opcionais da organização são os seguintes:

%ORG_DESCR%

Contém a descrição de uma organização.

%ORG_MEMBERSHIP%

(obrigatório)

Contém a organização pai de uma organização.

Observação: consulte Definindo a hierarquia organizacional para obter mais informações sobre o atributo %ORG_MEMBERSHIP%.

%ORG_MEMBERSHIP_NAME%

(obrigatório)

Contém o nome amigável ao usuário da organização pai (na página 151) de uma organização.

%ORG_NAME%

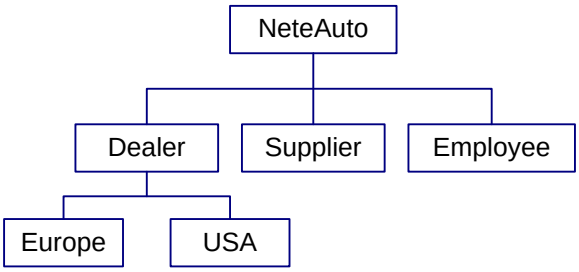
(obrigatório)

Contém o nome da organização.

Como definir a hierarquia organizacional

No CA Identity Manager, as organizações têm uma estrutura hierárquica que inclui uma organização raiz e suborganizações. As suborganizações também podem ter suborganizações.

Cada organização, exceto a organização raiz, tem uma organização pai. Por exemplo, na ilustração a seguir, Dealer é a organização pai das organizações USA e Europe:



O identificador exclusivo da organização pai é armazenado em um atributo no perfil de uma organização. Usando as informações desse atributo, o CA Identity Manager pode construir a hierarquia organizacional.

Para especificar o atributo que armazena a organização pai, use os atributos conhecidos %ORG_MEMBERSHIP% e %ORG_MEMBERSHIP_NAME% com o atributo físico que armazena o nome da organização pai em uma descrição de atributo, como se segue:

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0"
/>
```

Como melhorar o desempenho da pesquisa de diretório

Para melhorar o desempenho das pesquisas de diretório para usuários, organizações e grupos, execute as tarefas a seguir:

- Indexe os atributos que os administradores podem especificar nas consultas de pesquisa.

- Substitua a configuração de tempo limite do diretório padrão especificando valores para os parâmetros de pesquisa de tempo limite em um arquivo de configuração de diretório (directory.xml).
- Ajuste o diretório de usuários. Consulte a documentação do banco de dados que você está usando.

Configure opções específicas de banco de dados na origem de dados ODBC. Para obter mais informações, consulte a documentação da origem de dados.

Como melhorar o desempenho de pesquisas amplas

Quando o CA Identity Manager gerencia um grande repositório de usuários, as pesquisas que retornam muitos resultados podem fazer com que o sistema fique sem memória.

As duas configurações a seguir determinam como o CA Identity Manager trata as pesquisas amplas:

- Número máximo de linhas

  Especifica o número máximo de resultados que o CA Identity Manager pode retornar ao procurar um diretório de usuários. Quando o número de resultados exceder o limite, um erro será exibido.

- Tamanho da página

  Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

  Observação: se o repositório de usuários não oferecer suporte à paginação e um valor para maxrows for especificado, o CA Identity Manager usará apenas o valor de maxrows para controlar o tamanho da pesquisa.

É possível configurar os limites máximos de linha e de tamanho da página nos seguintes locais:

- Repositório de usuários

  Na maioria dos repositórios de usuários e bancos de dados, é possível definir limites de pesquisa.

  Observação: para obter mais informações, consulte a documentação do repositório de usuários ou banco de dados que você está usando.

- Diretório do CA Identity Manager

  Você pode configurar o elemento DirectorySearch (na página 58) no arquivo de configuração de diretório (directory.xml) que usa para criar o Diretório do CA Identity Manager.

  Por padrão, o valor máximo de linhas e de tamanho da página é ilimitado para os diretórios existentes. Para novos diretórios, o valor máximo de linhas é ilimitado e o valor do tamanho de página é 2000.

- Definição de objeto gerenciado

  Para definir os limites máximos de linha e tamanhos de página que se aplicam a um tipo de objeto, e não ao diretório inteiro, configure a *definição de objeto gerenciado* (na página 61) no arquivo directory.xml que é usado para criar o Diretório do CA Identity Manager.

  A definição de limites para um tipo de objeto gerenciado permite fazer ajustes que são se baseiam nos requisitos de negócios. Por exemplo, a maioria das empresas tem mais usuários do que os grupos. As empresas podem definir limites somente para pesquisas de objeto de usuário.

- Telas de pesquisa de tarefa

  Você pode controlar o número de resultados da pesquisa que os usuários podem ver nas telas de pesquisa e lista no Console de usuário. Se o número de resultados exceder o número de resultados por página que são definidos para a tarefa, os usuários verão links para páginas adicionais de resultados.

  Essa definição não afeta o número de resultados retornados por uma pesquisa.

  Observação: para obter informações sobre como definir o tamanho da página nas telas de pesquisa e lista, consulte o *Guia de Administração*.

Se os limites máximos de linha e tamanhos de página forem definidos em vários lugares, a configuração mais específica será aplicada. Por exemplo, as configurações de objeto gerenciado têm precedência sobre as configurações de nível de diretório.

Capítulo 5: Diretórios do CA Identity Manager

Um diretório do CA Identity Manager fornece informações sobre um diretório de usuários que o CA Identity Manager gerencia. Essas informações descrevem como os objetos, como usuários, grupos e organizações, estão armazenados no repositório de usuários e são exibidos no CA Identity Manager.

Você pode criar, exibir, exportar, atualizar e excluir diretórios do CA Identity Manager na seção de diretórios do CA Identity Manager do Management Console.

Observação: se o CA Identity Manager usa um cluster de Servidores de políticas do SiteMinder, interrompa o cluster, deixando apenas um Servidor de políticas antes de criar o atualizar diretórios do CA Identity Manager.

Esta seção contém os seguintes tópicos:

Pré-requisitos para criação de um diretório do CA Identity Manager

Antes de criar um diretório do CA Identity Manager, você deve executar este procedimento:

- Deixe apenas um nó do CA Identity Manager em atividade, interrompendo todos os outros, antes de criar ou modificar um diretório do CA Identity Manager.

  Observação: quando você tem um cluster de nós do CA Identity Manager, somente um nó desses nós poderá ser ativado quando você fizer alterações no Management Console.

- Deixe apenas um Servidor de políticas funcionando, interrompendo todos os outros, antes da criação ou atualização diretórios do CA Identity Manager.

  Observação: quando você tem um cluster de Servidores de políticas do SiteMinder, somente um desses servidores poderá ser ativado quando você fizer alterações no Management Console.

Como criar um diretório

No Management Console, você cria um Diretório do CA Identity Manager, que descreve a estrutura e o conteúdo do repositório de usuários, e o Diretório de provisionamento, que armazena informações necessárias do Servidor de provisionamento. Esses diretórios são associados ao ambiente do CA Identity Manager.

Você pode usar um dos métodos a seguir para criar diretórios:

- Usar o Assistente de configuração do diretório

  Orienta os administradores pelo processo de criação de um diretório para o repositório de usuários. Esse método ajuda a reduzir possíveis erros de configuração.

  Observação: use o Assistente de configuração de diretório para criar novos diretórios apenas para repositórios de usuários LDAP. Para criar um diretório para um banco de dados relacional ou atualizar um diretório existente, importe um arquivo directory.xml diretamente.

- Usar um arquivo de configuração XML

  Permite aos administradores selecionar um arquivo XML totalmente configurado para criar ou modificar o repositório de usuários ou o Servidor de provisionamento.

  Selecione esse método se você estiver criando um diretório para um banco de dados relacional ou se estiver atualizando um diretório existente.

Mais informações:

Criar um diretório com um arquivo de configuração XML (na página 168)
Criando um diretório usando o Assistente de configuração de diretório (na página 157)

Criando um diretório usando o Assistente de configuração de diretório

O Assistente de configuração de diretório guia os administradores pelo processo de criação de um diretório para o respectivo repositório de usuários, além de ajudar a reduzir os erros de configuração. Antes de iniciar o assistente, primeiramente você deve fazer o upload do modelo de configuração de diretório LDAP do CA Identity Manager. Esses modelos são pré-configurados com atributos conhecidos e obrigatórios. Depois de inserir os detalhes da conexão para o repositório de usuários ou Diretório de provisionamento LDAP, você pode selecionar os atributos LDAP, mapear atributos conhecidos e inserir metadados para os atributos. Quando tiver terminado de mapear os atributos, clique em Concluir para criar o diretório.

Iniciar o Assistente de configuração de diretório

O Assistente de configuração de diretório permite que um administrador selecione um modelo do CA Identity Manager e modifique-o para uso no seu ambiente.

Siga estas etapas:

1. No Management Console, clique em Directories e selecione Create from Wizard.

   É solicitado que você selecione um arquivo de configuração de diretório para configurar o repositório de usuários.

2. Clique em Browse para selecionar o arquivo de configuração para configurar o repositório de usuários ou o Servidor de provisionamento no seguinte local padrão e clique em Next.

   ```
   ferramentas_administrativas\directoryTemplates\diretório\
   ```

   Observação: ferramentas_administrativas especifica o diretório onde as Ferramentas administrativas estão instaladas e diretório especifica o nome do fornecedor LDAP.

   As Ferramentas administrativas são colocadas nos seguintes locais padrão:

   - Windows: <caminho_de_instalação>\tools
   - UNIX: <caminho_de_instalação2>/tools

3. Na tela Connection Details, especifique as informações de conexão do diretório LDAP ou Servidor de provisionamento, os parâmetros de pesquisa de diretório e as informações de conexões de tolerância a falhas e clique em Next.

4. Na tela Configure Managed Object, especifique os objetos a serem configurados e clique em Next. É possível selecionar entre os seguintes objetos:

   - Configure User Managed Object
   - Configure Group Managed Object
   - Configure Organization Object
   - Show summary and deploy directory

     Observação: escolha summary and deploy directory somente quando você tiver concluído a configuração do diretório.

   a. Na tela Select Attribute, exiba e modifique as classes estruturais e auxiliares, conforme a necessidade, e clique em Next.

   b. Na tela Select Attributes: Mapping Well-Knowns, mapeie os aliases conhecidos do CA Identity Manager para os atributos LDAP selecionados e clique em Next.

   c. (Opcional) Na tela Describe User Attributes, exiba e modifique as definições de atributo e clique em Next. É possível modificar o nome de exibição e a descrição.

   d. (Opcional) Na tela User Attribute Details, defina os metadados para cada atributo selecionado a ser gerenciado e clique em Next.

      A tela Managed Object Selection é exibida.

      Para configurar grupos ou organizações, selecione o objeto gerenciado e clique em Next para percorrer pelas telas de atributos desses objetos.

5. Selecione Show summary and deploy directory na lista e clique em Next.

   A tela de confirmação é exibida.

6. Exiba os detalhes do diretório.

   Se houver algum erro, clique no botão Back para fazer modificações nas telas adequadas. Clique em Finish para aplicar as alterações.

   O CA Identity Manager valida as configurações e cria o diretório. Em seguida, você é levado de volta à página Directories listing em que é possível exibir o novo diretório.

Tela Select Directory Template

Use essa tela para selecionar um arquivo XML de diretório para LDAP de modo a configurar um repositório de usuários ou Servidor de provisionamento.

Clique no botão Procurar para selecionar o arquivo de configuração para configurar o repositório de usuários ou o Servidor de provisionamento no seguinte local padrão:

```
ferramentas_administrativas\directoryTemplates\diretório\
```

Observação: ferramentas_administrativas especifica o diretório onde as Ferramentas administrativas estão instaladas e diretório especifica o nome do fornecedor LDAP.

As Ferramentas administrativas são colocadas nos seguintes locais padrão:

- Windows: <caminho_de_instalação>\tools
- UNIX: <caminho_de_instalação2>/tools

Depois de selecionar o arquivo XML de diretório, clique em Avançar para continuar até a tela Detalhes da conexão.

Tela Detalhes da conexão

Use essa tela para inserir as credenciais de configuração para seu repositório de usuários. Você também pode inserir os parâmetros de pesquisa de diretório e adicionar conexões de tolerância a falhas. Depois de digitar as informações de conexão, clique em Avançar para selecionar os objetos a serem gerenciados.

Observação: os campos que aparecem nessa tela dependem do tipo de repositório de usuários, e se você está criando a conexão usando o assistente de configuração de diretório ou importando diretamente um arquivo XML.

Os seguintes campos estão disponíveis nessa tela:

Nome

Especifica o nome do diretório do usuário ao qual você está se conectando.

Descrição

Especifica uma descrição do diretório do usuário.

Host

Especifica o nome de host do computador em que o repositório de usuários está localizado.

Porta

Especifica a porta do computador em que o repositório de usuários está localizado.

DN do usuário

Especifica o nome de domínio do usuário para acessar o repositório de usuários LDAP.

Nome JNDI da origem de dados JDBC

Especifica o nome de uma origem de dados JDBC existente que o CA Identity Manager usa para se conectar ao banco de dados.

Nome de usuário

Especifica o nome de usuário para acessar o Servidor de provisionamento.

Observação: apenas para Servidores de provisionamento.

Domínio

Especifica o nome do domínio para acessar o Servidor de provisionamento.

Observação: apenas para Servidores de provisionamento.

Senha

Especifica a senha para acessar o repositório de usuários/Servidor de provisionamento LDAP.

Confirmar senha

Confirma a senha para acessar o repositório de usuários/Servidor de provisionamento LDAP.

Conexão segura

Quando selecionado, força uma conexão SSL (Secure Sockets Layer) com o diretório de usuários LDAP.

Raiz de pesquisa

Especifica o local em um diretório LDAP que serve como ponto de partida para o diretório. Geralmente, uma organização (o) ou unidade organizacional (ou).

Observação: apenas para repositórios de usuários LDAP.

Número máximo de linhas de pesquisa

Especifica o número máximo de resultados que o CA Identity Manager pode retornar ao procurar um diretório de usuários. Quando o número de resultados exceder o limite, um erro será exibido.

A configuração do máximo de linhas pode substituir as configurações no diretório LDAP que limitam os resultados da pesquisa. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Search Page Size

Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

Observe os seguintes pontos ao especificar o tamanho da página de pesquisa:

- Para usar a opção Search Page Size, o repositório de usuários que o CA Identity Manager gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários podem exigir configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte o *Guia de Configuração*.
- Se o repositório de usuários não oferecer suporte à paginação e um valor máximo de linhas de pesquisa for especificado, o CA Identity Manager usará apenas o valor máximo de linhas de pesquisa para controlar o tamanho da pesquisa.

Search Timeout

Especifica o número máximo de segundos que o CA Identity Manager pesquisa um diretório antes de encerrar a pesquisa.

Failover Host

Especifica o nome do host do sistema em que existe um repositório de usuários redundante ou um Servidor de provisionamento alternativo, caso o sistema principal esteja indisponível. Se vários servidores forem listados, o CA Identity Manager tentará se conectar aos sistemas na mesma ordem listada.

Failover Port

Especifica a porta do sistema em que existe um repositório de usuários redundante ou um Servidor de provisionamento alternativo, caso o sistema principal esteja indisponível. Se vários servidores forem listados, o CA Identity Manager tentará se conectar aos sistemas na mesma ordem listada.

Botão Adicionar

Clique para adicionar mais números da porta e o nome do host de tolerância a falhas.

Tela Configure Managed Objects

Use essa tela para selecionar um objeto a ser configurado.

Veja a seguir a lista de campos nessa tela:

Configure User Managed Object

Descreve como os usuários são armazenadas no repositório de usuários e como eles são representados no CA Identity Manager.

Configure Group Managed Object

Descreve como os grupos são armazenados no repositório de usuários e como eles são representados no CA Identity Manager.

Configure Organization Managed Object

Se o repositório de usuários incluir organizações, descreve como as organizações são armazenados e representadas no CA Identity Manager.

Show Summary and Deploy Directory

Especifica que todos os objetos gerenciados foram definidos e você deseja implantar o diretório. Depois de selecionar a opção Show summary and the deploy directory, clique em Avançar e você é levado a uma página de resumo.

Botão Salvar

Clique para salvar o arquivo xml.

Botão Voltar

Clique para voltar para a tela Detalhes da conexão para fazer modificações.

Botão Avançar

Clique para continuar e acesse a tela Selecionar atributos para selecionar os atributos do usuário, grupo ou organização a serem configurados.

Tela Selecionar atributos

Use essa tela para alterar ou adicionar classes estruturais e auxiliares para objetos do Usuário, Grupo ou Organização. Essa tela é pré-configurada com os valores que tem como base esquemas comuns de diretório e práticas recomendadas para o tipo de diretório que você está usando. Um administrador pode alterar a classe estrutural selecionando uma nova classe no menu suspenso. A seleção de uma classe atualiza a tabela com atributos pertencentes à nova classe estrutural.

Uma classe auxiliar pode ser adicionada ao ser selecionada no menu suspenso. A seleção de uma classe auxiliar atualiza a tabela com atributos pertencentes à nova classe auxiliar.

Veja a seguir a lista de campos nessa tela:

Structural Class Name

Especifica a classe estrutural do atributo a ser configurada.

Botão Alterar

Clique para alterar a classe estrutural.

Auxiliary Class Name

Especifica a classe auxiliar do atributo a ser configurada.

Botão Adicionar

Clique para adicionar uma classe auxiliar a ser configurada.

Classe de objeto

Especifica o recipiente da classe de objeto.

ID

Especifica a ID do recipiente.

Nome

Especifica o nome do recipiente.

Attributes Table

Especifica o nome físico, a classe do objeto, se o atributo tem valores múltiplos e os tipos de dados dos atributos selecionados. Os atributos dessa tabela podem ser classificados por Selecionado, Classe de objeto, Valores múltiplos e Tipo de dados.

Botão Voltar

Clique para voltar à tela Configured Managed Objects.

Avançar

Clique para continuar e acessar a tela Well-Known Mapping para mapear os aliases conhecidos obrigatórios e opcionais.

Tela Well-Known Mapping

Use essa tela para mapear atributos conhecidos do CA Identity Manager para atributos LDAP selecionados. Um administrador pode fazer adições à lista de atributos conhecidos (se códigos personalizados forem exigidos) digitando um novo atributo conhecido no campo de texto e clicando no botão Adicionar. A tela é atualizada para que você possa continuar adicionando quantos atributos conhecidos forem necessários.

Veja a seguir a lista de campos nessa tela:

Required Well-Knowns

Especifica os atributos conhecidos para Usuários, Grupos ou Organizações (se aplicável) que devem ser mapeados para os atributos LDAP.

Optional Well-Knowns

Especifica os atributos conhecidos para Usuários, Grupos ou Organizações (se aplicável) que podem ser mapeados opcionalmente.

New Well-Known

Especifica um atributo conhecido conforme referenciado pelo código personalizado.

Botão Adicionar

Clique para adicionar um novo atributo conhecido à tabela Optional Well-Knows.

Botão Voltar

Clique para voltar para a tela Select User Attributes para selecionar mais atributos. Os mapeamentos já feitos são salvos e disponibilizados quando você retorna para essa tela.

Botão Avançar

Clique para continuar e acessar a tela Basic Object Attribute Definition para especificar definições básicas de atributo.

Mais informações

Atributos conhecidos para um repositório de usuários LDAP (na página 79)
Atributos conhecidos de grupo (na página 83)
Atributos conhecidos de usuário (na página 80)
Atributos conhecidos de organização (na página 85)

Tela Basic Object Attribute Definition

Use essa tela para exibir e modificar as definições em comum: Nome de exibição e Descrição.

Veja a seguir a lista de campos nessa tela:

Managed Object Table

Especifica o nome de exibição, o nome físico, o nome conhecido e a descrição do objeto gerenciado. Use o menu suspenso para alterar a descrição, se necessário. Depois de fazer as alterações, clique em Avançar para continuar.

Botão Voltar

Clique para voltar para a tela Well-Known Mapping para modificar os detalhes dos mapeamentos.

Botão Avançar

Clique para continuar e acessar a tela Detailed Object Attribute Definition, onde é possível especificar mais definições de atributo.

Tela Detailed Object Attribute Definition

Use essa tela para especificar outras definições de atributo. Um administrador pode definir os metadados para cada atributo selecionado modificando o nome de exibição, gerenciando o atributo na telas do Console de usuário, o tipo de dado do valor, o tamanho máximo e o conjunto de regras de validação. Depois de especificar as definições de atributo, clique em Avançar para continuar.

Os campos dessa tela são listados abaixo:

Nome de exibição

Especifica o nome exclusivo para o atributo de objeto gerenciado. Esse é o nome que é exibido no Console de usuário.

Qualificadores

Especifica os qualificadores de classificação de dados para o valor do atributo de objeto gerenciado. Os qualificadores são todos opcionais e padronizados para falso, exceto os pesquisáveis. Os qualificadores a seguir podem ser selecionados:

Obrigatório

Indica se o atributo é obrigatório na criação de objetos.

Valores múltiplos

Indica que o atributo é exibido como valores múltiplos.

Oculto

Indica que o atributo está oculto.

Sistema

Indica que o atributo é um atributo do sistema e não foi adicionado às telas de tarefa.

Pesquisável

Indica que o atributo foi adicionado aos filtros de pesquisa. Padronizado para verdadeiro.

Criptografia confidencial

Indica que o atributo é confidencial e é exibido como uma série de asteriscos (*).

Oculto em VST

Indica que o atributo fica oculto na tela Detalhes do evento para Exibir tarefas enviadas.

Não copiar

Indica que o atributo deve ser ignorado quando um administrador criar uma cópia de um objeto.

Criptografado anteriormente

Indica que o atributo que está sendo acessado no repositório de usuários foi anteriormente criptografado e requer descriptografia. O valor do texto não criptografado é salvo no repositório de usuários quando o objeto é salvo.

Untagged encrypted

Indica que o atributo foi criptografado anteriormente no repositório de usuários e não tem o nome de qualificador do algoritmo de criptografia no início do texto criptografado.

Tipo de dado

Especifica o tipo de dado do valor para o atributo de objeto gerenciado no Console de usuário. É possível selecionar na seguinte lista:

- READONLY
- WRITEONCE
- READWRITE

Comprimento máximo

Especifica o tamanho máximo do valor para o atributo de objeto gerenciado

Padrão: 0

Conjunto de regras de validação

Especifica os conjuntos de regras de validação para validar o valor do atributo de objeto gerenciado. É possível selecionar na seguinte lista:

- Validação do usuário
- Formato do número de telefone
- Formato de número de telefone internacional

Botão Voltar

Clique nesse botão para voltar à tela Basic Object Attribute Definition e fazer modificações.

Botão Avançar

Clique nesse botão para continuar e acessar a tela Configure Managed Objects. Nessa tela, você pode selecionar o próximo objeto gerenciado a ser configurado. Depois de configurar os objetos gerenciados, selecione a opção Show summary and the deploy directory para exibir suas informações de diretório e implantar o diretório.

Mais informações

Gerenciando atributos confidenciais (na página 71)

Tela Confirmação

Essa tela mostra um resumo dos detalhes do diretório.

Veja a seguir a lista de campos nessa tela:

Detalhes da conexão

Especifica os detalhes da conexão para o diretório do usuário.

User/Group/Organization Details

Especifica as alterações feitas no directory.xml.

Botão Voltar

Clique para modificar os detalhes no assistente.

Botão Salvar

Clique para salvar as seleções.

Botão Concluir

Clique se todos os detalhes de diretório estiverem corretos para sair do assistente.

A configuração é validada e o diretório é criado. Você é levado de volta à página Directories listing, onde o novo diretório está listado. Para editar ou exportar o novo diretório, selecione-o na lista de diretórios.

Criar um diretório com um arquivo de configuração XML

Você pode criar ou atualizar um Diretório do CA Identity Manager importando um arquivo directory.xml completo no Management Console.

Observação: se você estiver criando um diretório usando um arquivo directory.xml, e não o Assistente de configuração de diretório, verifique se modificou o modelo de configuração padrão. Para obter mais informações, consulte o *Guia de Configuração*.

Siga estas etapas:

1. Abra o Management Console digitando o seguinte URL em um navegador:

   http://*nome_do_host*:*porta*/iam/immanage

   nome do host

   Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.

   porta

   Define o número da porta do servidor de aplicativos.

2. Clique em Directories.

   A janela CA Identity Manager Directories é exibida.

3. Clique em Create ou Update from XML.

4. Digite o caminho e o nome do arquivo XML de configuração de diretório para criar o Diretório do CA Identity Manager, ou procure pelo arquivo. Clique em Avançar.

5. Forneça valores para os campos nessa janela, como se segue:

   Observação: os campos que aparecem nessa janela dependem do tipo de repositório de usuários e das informações fornecidas no arquivo de configuração de diretório na Etapa 4. Se você forneceu valores para algum desses campos no arquivo de configuração de diretório, o CA Identity Manager não solicitará que você forneça esses valores novamente.

   Nome

   Determina o nome do Diretório do CA Identity Manager que você está criando.

   Descrição

   (Opcional) Descreve o Diretório do CA Identity Manager.

   Nome do objeto de conexão

   Especifica o nome do diretório de usuários que o Diretório do CA Identity Manager descreve. Insira *um* dos seguintes detalhes:

   - Se o CA Identity Manager não se integrar ao SiteMinder, especifique um nome significativo para o objeto que o CA Identity Manager usa para se conectar ao repositório de usuários.
   - Se o CA Identity Manager se integrar ao SiteMinder e você desejar criar um objeto de conexão de diretório de usuários no SiteMinder, especifique um nome significativo. O CA Identity Manager cria o objeto de conexão de diretório de usuários no SiteMinder com o nome que você especificar.
   - Se o CA Identity Manager se integrar ao SiteMinder e você desejar se conectar a um diretório de usuários existente do SiteMinder, especifique o nome do objeto de conexão de diretório de usuários do SiteMinder exatamente como ele aparece na interface de usuário do Servidor de políticas.

JDBC Data Source JNDI Name (apenas para diretórios relacionais)

Especifica o nome de uma origem de dados JDBC existente que o CA Identity Manager usa para se conectar ao banco de dados.

Host (apenas para diretórios LDAP)

Especifica o nome do host ou endereço IP do sistema onde o diretório de usuários está instalado.

Para repositórios de usuários do CA Directory, use o nome do domínio completo do sistema de host. Não use o localhost.

Para repositórios de usuários do Active Directory, especifique o nome de domínio, não o endereço IP.

Port (apenas para diretórios LDAP)

Especifica o número da porta do diretório de usuários.

Provisioning Domain

Domínio de provisionamento que o CA Identity Manager gerencia.

Observação: o nome do Domínio de provisionamento diferencia maiúsculas e minúsculas.

Username/User DN

Especifica o nome de usuário de uma conta que pode acessar o repositório de usuários.

Para Provisionamento de repositórios de usuários, a conta de usuário que você especifica deve ter o perfil de Administrador de domínio ou um conjunto de privilégios equivalente para o Domínio de provisionamento.

Senha

Especifica a senha para a conta de usuário que você especificou no campo Username (para bancos de dados relacionais) ou User DN (para diretórios LDAP).

Confirmar senha

Digite novamente a senha que você digitou no campo Senha para confirmação.

Conexão segura (apenas para diretórios LDAP)

Indica se o CA Identity Manager usa uma conexão segura.

Certifique-se de selecionar essa opção para repositórios de usuários do Active Directory.

Clique em Avançar.

6. Revise as configurações do Diretório do CA Identity Manager. Clique em Finish para criar o Diretório do CA Identity Manager com as configurações atuais ou clique em Previous para modificar.

   As informações de status são exibidas na janela Directory Configuration Output.

7. Clique em Continuar para sair.

   O CA Identity Manager cria o diretório.

Ativar o acesso ao Servidor de provisionamento

Você ativa o acesso ao Servidor de provisionamento usando o link Directories no Management Console.

Observação: um pré-requisito para este procedimento é instalar o Diretório de provisionamento no CA Directory. Para obter mais informações, consulte o *Guia de Instalação*.

Siga estas etapas:

1. Abra o Management Console digitando o seguinte URL em um navegador:

   `http://`*`nome_do_host`*`:`*`porta`*`/iam/immanage`

   nome do host

   Define o nome de host totalmente qualificado do sistema em que o servidor do CA Identity Manager está instalado.

   porta

   Define o número da porta do servidor de aplicativos.

2. Clique em Directories.

   A janela CA Identity Manager Directories é exibida.

3. Clique em Create from Wizard.

4. Digite o caminho e o nome do arquivo XML de diretório para configuração do Diretório de provisionamento. Ele é armazenado em directoryTemplates\ProvisioningServer na pasta Ferramentas administrativas. O local padrão dessa pasta é:

   - Windows: <caminho_de_instalação>\tools
   - UNIX: <caminho_de_instalação2>/tools

   Observação: você pode usar esse arquivo de configuração de diretório como foi instalado, sem modificação.

5. Clique em Avançar.

6. Forneça valores para os campos nessa janela, como se segue:

Nome

É um nome para o Diretório de provisionamento que está associado ao Servidor de provisionamento que você está configurando.

- Se o CA Identity Manager não se integrar ao SiteMinder, especifique um nome significativo para o objeto que o CA Identity Manager usa para se conectar ao diretório de usuários.
- Se o CA Identity Manager se integrar ao SiteMinder, você terá duas opções:

  Se desejar criar um objeto de conexão de diretório de usuários no SiteMinder, especifique um nome significativo. O CA Identity Manager cria esse objeto no SiteMinder com o nome especificado.

  Se desejar se conectar a um diretório de usuários existente do SiteMinder, especifique o nome do objeto de conexão de diretório de usuários do SiteMinder exatamente como ele aparece na interface de usuário do Servidor de políticas.

Descrição

(Opcional) Descreve o Diretório do CA Identity Manager.

Host

Especifica o nome do host ou endereço IP do sistema onde o diretório de usuários está instalado.

Porta

Especifica o número da porta do diretório de usuários.

Domínio

Especifica o nome do domínio de provisionamento que o CA Identity Manager gerencia.

Importante: ao criar um Diretório de provisionamento usando o Management Console com os caracteres de idioma estrangeiro como o nome de domínio, haverá falha na criação do Diretório de provisionamento.

O nome deve corresponder ao nome do domínio de provisionamento que você especificou durante a instalação.

Observação: o nome do domínio diferencia maiúsculas e minúsculas.

Nome de usuário

Especifica o usuário que pode efetuar logon no Gerenciador de provisionamento.

O usuário deve ter o perfil de Administrador de domínio ou um conjunto de privilégios equivalente para o Domínio de provisionamento.

Senha

Especifica a senha para o usuário global especificado no campo Username.

Confirmar senha

Digite novamente a senha que você digitou no campo Senha para confirmação.

Conexão segura

Indica se o CA Identity Manager usa uma conexão segura.

Certifique-se de selecionar essa opção para repositórios de usuários do Active Directory.

Parâmetros da pesquisa de diretório

maxrows define o número máximo de resultados que o CA Identity Manager pode retornar ao pesquisar um diretório de usuários. Esse valor substitui qualquer limite definido no diretório LDAP. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Observação: o parâmetro maxrows não limita o número de resultados que são exibidos na tela de tarefas do CA Identity Manager. Para configurar as definições de exibição, modifique a definição da tela de lista no Console de usuário do CA Identity Manager. Para obter instruções, consulte o *Guia de Design do Console de Usuário*.

timeout determina o número máximo de segundos que o CA Identity Manager pesquisa um diretório antes de encerrar a pesquisa.

Failover Connections

O nome do host e o número da porta de um ou mais sistemas opcionais que são Servidores de provisionamento alternativos. Se vários servidores forem listados, o CA Identity Manager tentará estabelecer uma conexão com os sistemas na ordem em que estão listados.

Os Servidores de provisionamento alternativos serão usados se o Servidor de provisionamento principal falhar. Quando o Servidor de provisionamento principal se tornar disponível novamente, o alternativo continuará sendo usado. Se desejar voltar a usar o Servidor de provisionamento, reinicie os Servidores de provisionamento alternativo.

7. Clique em Avançar.
8. Selecione os objetos a serem gerenciados, como usuários ou grupos.
9. Após configurar os objetos de acordo com a necessidade, clique em Show summary deploy directory e verifique as configurações do Diretório de provisionamento.
10. Clique em uma destas ações:
    a. Clique em Back para modificar.
    b. Clique em Save para salvar as informações de diretório se quiser retornar mais tarde para fazer a implantação.
    c. Clique em Finish para concluir esse procedimento e começar a configurar um ambiente com provisionamento (na página 195).

Exibir um Diretório do CA Identity Manager

Execute o procedimento a seguir para exibir um Diretório do CA Identity Manager.

Siga estas etapas:

1. No Management Console do CA Identity Manager, clique em Directories.
2. Clique no nome do diretório do CA Identity Manager a ser exibido. A janela Directory Properties é exibida, mostrando as propriedades de diretório do CA Identity Manager.

Propriedades de diretório do CA Identity Manager

As Propriedades de diretório do CA Identity Manager são as seguintes:

Observação: as propriedades que são exibidas dependem do tipo de banco de dados ou diretório que está associado ao diretório do CA Identity Manager.

Nome

Define o nome exclusivo do Diretório do CA Identity Manager.

Descrição

Fornece uma descrição para o Diretório do CA Identity Manager.

Tipo

Define o tipo de provedor de diretório.

Nome do objeto de conexão

Exibe o nome do diretório de usuários que o Diretório do CA Identity Manager descreve.

Se o CA Identity Manager se integrar ao SiteMinder, o nome do objeto de conexão corresponderá ao nome da conexão diretório de usuários do SiteMinder.

Organização raiz (para repositórios de usuários que incluem organizações)

Especifica o ponto de entrada no repositório de usuários.

Para diretórios LDAP, a organização raiz é especificada como um DN. Para bancos de dados relacionais, o identificador exclusivo para a organização raiz é exibida.

Origem de dados JDBC

Especifica o nome da origem de dados JDBC que o CA Identity Manager usa para se conectar ao banco de dados.

URL

Fornece o URL ou endereço IP do repositório de usuários.

Nome de usuário

Especifica o nome de usuário de uma conta que pode acessar o repositório de usuários.

Número máximo de linhas de pesquisa

Indica o número máximo de linhas retornadas como o resultado de uma pesquisa.

Search Page Size

Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

Observação: o repositório de usuários que o CA Identity Manager gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários podem exigir configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte o *Guia de Configuração*.

Oferece suporte à paginação

Indica que o diretório oferece suporte à paginação.

Tempo limite de pesquisa (apenas para diretórios LDAP)

Especifica o número máximo de segundos que o CA Identity Manager pesquisa um repositório de usuários antes de encerrar a pesquisa.

Domínio de provisionamento (apenas para diretórios do Servidor de provisionamento)

Domínio de provisionamento que o CA Identity Manager gerencia.

Janela Propriedades do diretório do CA Identity Manager

As informações gerais sobre um diretório do CA Identity Manager são apresentadas na janela de propriedades do diretório que você seleciona. A janela Propriedades do diretório é dividido nas seguintes seções:

Propriedades do diretório

Exibe propriedades básicas do diretório do CA Identity Manager, incluindo o Domínio de provisionamento associado, se o Provisionamento for ativado para o Ambiente.

Objetos gerenciados (na página 177)

Fornece as descrições do tipo de objetos de repositório de usuários que o CA Identity Manager gerencia.

Conjuntos de regras de validação (na página 182)

Lista os conjuntos de regras de validação que se aplicam ao diretório do CA Identity Manager.

Ambientes

Lista os ambientes que são associados ao diretório do CA Identity Manager. Um diretório pode ser associado a vários ambientes do CA Identity Manager.

Para exibir mais informações sobre um ambiente do CA Identity Manager, clique no nome do ambiente.

Para modificar as propriedades em um diretório do CA Identity Manager, importe um arquivo de configuração de diretório, conforme descrito em Atualizar um diretório do CA Identity Manager (na página 184).

Além da exibição de propriedades, também é possível executar as seguintes ações:

Atualizar autenticação

Permite que os administradores alterem o diretório que o CA Identity Manager usa para autenticar os administradores do Management Console. Os administradores também podem adicionar mais administradores do Management Console no diretório de autenticação existente.

Observação: as opções Atualizar autenticação se aplicam apenas quando a segurança nativa do CA Identity Manager protege o Management Console. Para obter informações sobre como ativar a segurança nativa ou sobre como usar outro método de segurança, consulte o *Guia de Configuração.*

Exportar (na página 184)

Exporta a definição do diretório como um arquivo XML. Após exportar as configurações de diretório, é possível modificar o arquivo XML e, em seguida, reimportá-lo para atualizar o diretório. Também é possível importar o arquivo XML em outro diretório para definir as mesmas configurações para esse diretório.

Atualizar (na página 184)

Permite que os administradores adicionem ou alterem as definições de objeto gerenciado, como os atributos de um objeto, definam os parâmetros de pesquisa e alterem as propriedades do diretório.

Como exibir propriedades e atributos do objeto gerenciado

Um objeto gerenciado descreve um tipo de entrada no repositório de usuários, como um usuário, grupo ou organização. As propriedades e os atributos que se aplicam a um objeto gerenciado aplicam-se a todas as entradas desse tipo. Por exemplo, um perfil de usuário é composto por todos os atributos e propriedades do objeto gerenciado Usuário.

Para exibir os detalhes de um objeto gerenciado, clique no nome do objeto para abrir a janela Propriedades do objeto gerenciado.

Propriedades do objeto gerenciado

A janela Propriedades do objeto gerenciado descreve as propriedades e atributos para um tipo de objeto gerenciado.

As informações sobre a janela Propriedades do objeto gerenciado dependem do tipo de repositório de usuários que você está gerenciando. As propriedades de um objeto gerenciado são as seguintes:

Descrição

Fornece uma descrição do objeto gerenciado.

Tipo

Indica o tipo de entrada que o objeto gerenciado representa. Um tipo de objeto pode ser um dos seguintes:

- Usuário
- Grupo
- Organização

Classe do objeto (apenas para diretórios LDAP)

Especifica as classes de objeto para o objeto gerenciado. Um objeto gerenciado pode ter várias classes de objeto.

Ordem de classificação (apenas para diretórios LDAP)

Especifica o atributo que o CA Identity Manager usa para classificar os resultados da pesquisa na lógica de negócios personalizada. A Ordem de classificação não afeta a ordem dos resultados da pesquisa no Console de usuário.

Por exemplo, quando você especifica o atributo cn para o objeto do usuário, o CA Identity Manager classifica os resultados de uma pesquisa de usuários em ordem alfabética, segundo o atributo cn.

Tabela principal (apenas para bancos de dados relacionais)

Especifica a tabela que contém o identificador exclusivo do objeto gerenciado.

Máximo de linhas

Especifica o número máximo de resultados que o CA Identity Manager pode retornar ao pesquisar objetos desse tipo. Quando o número de resultados exceder o limite, um erro será exibido.

A configuração do máximo de linhas pode substituir as configurações no diretório LDAP que limitam os resultados da pesquisa. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Tamanho da página

Especifica o número de objetos que podem ser retornados em uma única pesquisa. Se o número de objetos exceder o tamanho da página, o CA Identity Manager executará várias pesquisas.

Observação: o repositório de usuários que o CA Identity Manager gerencia deve oferecer suporte à paginação. Alguns tipos de repositório de usuários podem exigir configuração adicional para oferecer suporte à paginação. Para obter mais informações, consulte o *Guia de Configuração*.

Propriedades do recipiente (apenas para diretórios LDAP)

Em um diretório LDAP, os grupos de *recipientes* contêm objetos de um tipo específico. Quando um recipiente é especificado, o CA Identity Manager gerencia somente entradas no recipiente. Por exemplo, quando você especifica o recipiente ou=People, o CA Identity Manager trata os usuários existentes apenas no recipiente People.

Observação: os usuários e grupos existentes no diretório LDAP, mas não no recipiente definido, podem aparecer no Console de usuário. Você pode enfrentar problemas durante o gerenciamento desses usuários e grupos.

Os recipientes agrupam apenas usuários e grupos. Não é possível especificar um recipiente para organizações.

As propriedades de um recipiente são as seguintes:

objectclass

Especifica a classe de objeto LDAP do recipiente no qual os objetos de um tipo específico são criados. Por exemplo, o valor padrão para o recipiente de usuário é "top,organizationalUnit", que indica que os usuários são criados nas unidades organizacionais (ou) LDAP.

ID

Especifica o atributo que armazena o nome do recipiente, por exemplo, ou. O atributo é emparelhado com o valor Name para formar o DN relativo do recipiente, como no exemplo a seguir:

ou=People

Nome

Especifica o nome do recipiente.

Propriedades da tabela secundária (apenas para os bancos de dados relacionais)

As tabelas secundárias contêm atributos adicionais para um objeto gerenciado. Por exemplo, uma tabela secundária denominada tblUserAddress pode conter os atributos de rua, cidade, estado e CEP para o objeto gerenciado Usuário.

As propriedades a seguir são exibidas para tabelas secundárias:

Table

Especifica o nome da tabela.

Reference

Descreve o mapeamento entre a tabela principal e a tabela secundária.

A referência é exibida usando o seguinte formato:

tabela_principal.atributo=tabela_secundária.atributo

Por exemplo, tblUsers.id=tblUserAddress.userid indica que o atributo id na tabela principal, tblUsers, é mapeado para o atributo userid na tabela tblUserAddress.

Propriedades do atributo na janela Propriedades do objeto gerenciado

As propriedades a seguir são exibidas para atributos na janela Propriedades do objeto gerenciado:

Nome de exibição

O nome amigável ao usuário do atributo. Esse nome aparece na lista de atributos disponíveis ao projetar uma janela da tarefa para uma tarefa específica no Console de usuário.

Nome físico

O nome do atributo no repositório de usuários.

Nome conhecido

Os nomes conhecidos indicam atributos com um significado especial no CA Identity Manager, como o atributo usado para armazenar senhas de usuário.

Propriedades do atributo nas janelas Propriedades do atributo

Para ver detalhes adicionais sobre um atributo, clique em seu nome para abrir a janela Propriedades do atributo.

As propriedades de atributo a seguir são exibidas na janela Propriedades do atributo:

Descrição

Fornece uma descrição para o atributo.

Nome físico

Especifica o nome do atributo no repositório de usuários.

Classe de objeto (apenas atributos de usuário, grupo e organização em diretórios LDAP)

A classe auxiliar LDAP para um atributo de usuário, quando o atributo não faz parte da classe de objeto principal especificada para o Objeto de usuário.

Você pode especificar uma classe de objeto auxiliar apenas para objetos de Usuário e Grupo.

Nome conhecido

Indica atributos com um significado especial no CA Identity Manager, como o atributo usado para armazenar senhas de usuário.

Obrigatório

Indica se é necessário um valor para o atributo, como se segue:

- True indica que o atributo deve ter um valor.
- False indica que um valor é opcional.

Somente leitura

Indica o nível de permissão de um atributo, como se segue:

- True indica que o atributo não pode ser modificado.
- False indica que o atributo pode ser modificado.

Oculto

Indica se um atributo pode ser exibido em uma janela de tarefas para uma tarefa específica.

Os atributos ocultos geralmente são usados nos esquemas de atributos lógicos.

Observação: para obter mais informações, consulte o *Guia de Programação do Java*.

Oferece suporte a valores múltiplos

Indica se o atributo pode ter vários valores ou não, como pode ser visto a seguir (por exemplo, o atributo que é usado para armazenar os integrantes de um grupo tem valores múltiplos):

- True indica que o atributo pode oferecer suporte a valores múltiplos.
- False indica que o atributo pode ter somente um único valor.

Delimitador de valores múltiplos (apenas para bancos de dados relacionais)

O caractere que separa valores quando vários valores são armazenados em uma única coluna.

Atributo do sistema

Indica se o atributo é usado apenas pelo CA Identity Manager ou não, como se segue:

- True indica se o atributo é um atributo do sistema. O atributo não está disponível para ser adicionado às janelas de tarefas.
- False indica que os usuários podem usar esse atributo. O atributo pode aparecer nas janelas de tarefas.

Tipo de dado

Especifica o tipo de dados do atributo. O valor padrão é Sequência de caracteres.

Comprimento máximo

Especifica o tamanho máximo que um valor de atributo pode ter. Se definido como 0, não haverá limite para o comprimento do valor.

Conjunto de regras de validação

Especifica o nome de um conjunto de regras de validação, quando o atributo está associado a um.

Conjuntos de regras de validação

Uma regra de validação aplica requisitos sobre dados que um usuário digita em um campo de janela de tarefas. Os requisitos podem aplicar um tipo de dados ou um formato, ou podem garantir que os dados sejam válidos no contexto de outros dados na janela de tarefas.

Uma ou mais regras de validação são agrupadas em um conjunto de regras de validação. Um conjunto de regras de validação é, então, associado a um atributo de perfil. Por exemplo, você pode criar um conjunto de regras de validação que contenha uma regra de validação de Formato de data, que aplique um formato de data de mm-dd-aaaa. Desse modo, é possível associar o conjunto de regras de validação ao atributo que armazena a data de início de um funcionário.

Observação: você pode criar regras de validação e conjuntos de regras no arquivo de configuração de diretório ou no Console de usuário.

A janela Propriedades do objeto gerenciado exibe uma lista de conjuntos de regras de validação que se aplicam ao diretório do CA Identity Manager. Para exibir os detalhes de um conjunto de regras de validação, clique no nome do conjunto de regras para abrir a janela Propriedades do conjunto de regras de validação.

Propriedades da regra de validação

As informações a seguir são exibidas na janela Propriedades da regra de validação:

Nome

Fornece o nome da regra de validação.

Descrição

Fornece uma descrição da regra.

Classe

Fornece o nome da classe Java que implementa a regra de validação.

Esse campo não será exibido, a menos que a regra de validação seja definida em uma classe Java.

Nome do arquivo

Fornece o nome do arquivo que contém a implementação da regra de validação JavaScript.

Esse campo não será exibido, a menos que a regra de validação seja definida em um arquivo.

Expressão regular

Fornece a expressão regular que implementa a regra de validação.

Esse campo não será exibido, a menos que a regra de validação seja definida como uma expressão regular.

Propriedades do conjunto de regras de validação

As informações a seguir são exibidas na janela Propriedades do conjunto de regras de validação:

Nome

Especifica o nome do conjunto de regras de validação.

Descrição

Fornece uma descrição para o conjunto de regras de validação.

A página Propriedades do conjunto de regras de validação também inclui uma lista de regras de validação no conjunto. Você pode clicar no nome da regra de validação para abrir a janela Propriedades da regra de validação.

Como atualizar as configurações de um diretório do CA Identity Manager

Para exibir as configurações atuais de um diretório do CA Identity Manager, exporte as configurações de diretório e salve-as como um arquivo XML.

Após exportar as configurações de diretório, é possível modificá-las e importá-las no arquivo XML para atualizar o diretório. Também é possível importar o arquivo XML em outro diretório para definir as mesmas configurações para esse diretório.

Exportar um diretório do CA Identity Manager

Execute o procedimento a seguir para exportar um diretório do CA Identity Manager.

Siga estas etapas:

1. Clique em Diretórios.

   A lista de diretórios do CA Identity Manager é exibida.

2. Clique no nome do diretório a ser exportado.

   A janela Propriedades do diretório do CA Identity Manager é exibida.

3. Na parte inferior da janela de propriedades, clique em Exportar.

4. Quando solicitado, salve o arquivo XML.

Atualizar um diretório do CA Identity Manager

A finalidade de atualizar um diretório do CA Identity Manager é:

- Adicionar ou alterar as definições de objeto gerenciado, incluindo os atributos de um objeto.
- Definir parâmetros de pesquisa
- Alterar as propriedades do diretório

Observação: o CA Identity Manager não exclui definições de objeto ou atributo.

O arquivo de configuração de diretório pode conter apenas as alterações que você deseja fazer. Você não precisa incluir atributos ou propriedades que já estão definidos.

Observação: quando você tem um cluster de nós do CA Identity Manager, somente um nó desses nós poderá ser ativado quando você fizer alterações no Management Console. Deixe apenas um nó do CA Identity Manager em atividade, interrompendo todos os outros, antes de criar ou modificar um diretório do CA Identity Manager.

Siga estas etapas:

1. Exporte as configurações atuais de diretório do CA Identity Manager para um arquivo XML.
2. Modifique o arquivo XML para refletir suas alterações.
3. Clique em Diretórios.

   A lista de diretórios do CA Identity Manager é exibida.
4. Clique no nome do diretório a ser atualizado.

   As propriedades do diretório do CA Identity Manager são exibidas.
5. Na parte inferior da janela de propriedades, clique em Atualizar.
6. Digite o caminho e o nome do arquivo XML para atualizar o diretório do CA Identity Manager, ou procure pelo arquivo. Clique em Finalizar.

   As informações de status são exibidas no campo Directory Configuration Output.
7. Clique em Continuar.

Excluir um diretório do CA Identity Manager

Antes de excluir um diretório do CA Identity Manager, exclua os ambientes do CA Identity Manager que estão associados a ele.

Siga estas etapas:

1. No Management Console, clique em Directories.

   A lista de diretórios do CA Identity Manager é exibida.
2. Marque a caixa de seleção à esquerda dos diretórios a serem excluídos.
3. Clique em Excluir.

   Uma mensagem de confirmação é exibida.
4. Clique em OK para confirmar a exclusão.

Capítulo 6: Ambientes do CA Identity Manager

Esta seção contém os seguintes tópicos:

Ambientes do CA Identity Manager

Um ambiente do CA Identity Manager é uma exibição de um repositório de usuários. Em um ambiente do CA Identity Manager, você pode gerenciar usuários, grupos, organizações, tarefas e funções. Você também pode fornecer aos usuários contas em terminais gerenciados, como contas de email ou outros aplicativos.

Usando o Management Console, você pode executar as seguintes tarefas:

- Criar, modificar ou excluir um ambiente do CA Identity Manager.
- Exportar e importar um ambiente do CA Identity Manager.
- Definir configurações avançadas
- Importar funções e tarefas
- Redefinir a conta do Gerente do sistema

Pré-requisitos para criação de um ambiente do CA Identity Manager

Antes de começar, use a planilha da tabela a seguir para coletar as informações necessárias:

Planilha de configuração do ambiente do CA Identity Manager	
Informações necessárias	**Valor**
Um nome de ambiente do CA Identity Manager significativo que você escolher. Por exemplo: MeuAmbiente.	
O URL base que o CA Identity Manager usa para formar o URL de redirecionamento para a política de senha padrão do ambiente. Por exemplo: http://servidor.sua_empresa.org	
Um alias que é adicionado ao URL para acessar tarefas protegidas no ambiente. Por exemplo: http://servidor.sua_empresa.org/iam/im/alias	
Um alias que é adicionado ao URL para acesso a tarefas públicas, como tarefas de senha esquecida e autorregistro. Por exemplo: http://servidor.sua_empresa.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **Observação:** quando o seu ambiente não incluir tarefas públicas, não será necessário especificar um alias público.	
Se você forneceu um alias público, o nome de um usuário existente que atua como o usuário público. O CA Identity Manager usa as credenciais do usuário público no lugar das credenciais fornecidas pelo usuário ao acessar tarefas públicas.	
O nome de um CA Identity Manager (na página 103)	
O nome do diretório de provisionamento, quando o ambiente do CA Identity Manager oferece suporte ao provisionamento.	

Planilha de configuração do ambiente do CA Identity Manager	
Informações necessárias	**Valor**
O identificador exclusivo para um usuário que administra o ambiente do CA Identity Manager. Por exemplo: myadmin	
O nome do agente ou grupo de agentes do SiteMinder que protege o ambiente do CA Identity Manager se o CA Identity Manager integrar-se ao SiteMinder.	

Criar um ambiente do CA Identity Manager

Os ambientes do CA Identity Manager permitem gerenciar objetos em um diretório com um conjunto de funções e tarefas. Use o assistente do ambiente do CA Identity Manager para guiá-lo pelas etapas de criação de um ambiente do CA Identity Manager.

Observe os seguintes pontos antes de criar um ambiente do CA Identity Manager:

- Suponha que você esteja usando um repositório de usuários LDAP e que configurou um recipiente de usuários como ou=People no arquivo de configuração de diretório (directory.xml) para o seu diretório do CA Identity Manager. Verifique se os usuários que você seleciona ao criar o ambiente do CA Identity Manager existem nesse recipiente. A seleção de uma conta de usuário que não existe no recipiente de usuários pode causar falhas.
- Ao configurar um ambiente do CA Identity Manager para gerenciar um diretório de usuários LDAP com uma estrutura simples ou uma estrutura de usuários simples, o perfil do usuário selecionado deve incluir a organização do usuário. Para ajudar a garantir que o perfil de um usuário seja configurado corretamente, adicione o nome da organização do usuário ao atributo físico correspondente ao atributo conhecido %ORG_MEMBERSHIP% no arquivo directory.xml (na página 86). Por exemplo, quando a descrição do atributo físico é mapeada para o atributo conhecido %ORG_MEMBERSHIP% no arquivo directory.xml e o usuário pertence à organização Funcionários, o perfil do usuário deve conter o par atributo/valor descrição=Funcionários.

Siga estas etapas:

1. Se o CA Identity Manager usar um cluster de Servidores de políticas, interrompa todos, exceto um Servidor de políticas.
2. Se você tiver um cluster de nós do CA Identity Manager, interrompa todos, exceto um nó do CA Identity Manager.
3. No Management Console, clique em Environments.

4. Clique em Novo.

   O assistente de ambiente do CA Identity Manager é aberto.

5. Forneça as seguintes informações:

   - **Nome do ambiente**

     Especifique um nome exclusivo para o ambiente

   - **Descrição**

     Descreve o ambiente

   - **Alias protegido**

     Especifica um nome exclusivo, como funcionários. Um alias é adicionado ao URL para acessar tarefas protegidas no ambiente do CA Identity Manager. Por exemplo, quando o alias for funcionários, o URL para acessar o ambiente do funcionário será
     http://meu_*servidor.minha_empresa.com*/iam/im/funcionarios

     Observação: o alias diferencia maiúsculas de minúsculas e não pode conter espaços. É recomendável usar letras minúsculas sem sinais de pontuação ou espaços ao especificar o alias.

   - **URL base**

     Especifica o URL do CA Identity Manager. O URL exige um nome de host; ele pode incluir localhost. Além disso, não inclua o alias, por exemplo, http://*meu_servidor.minha_empresa.com*/iam/im.

     Se você estiver usando um Agente web, certifique-se de que o URL base seja alterado para refletir o URL do Agente web.

     Observação: se você estiver usando um Agente web para proteger os recursos do CA Identity Manager, não especifique um número de porta no campo URL base. Se você estiver usando um Agente web e o URL base contiver um número de porta, os links para tarefas do CA Identity Manager não funcionarão corretamente.

     Para obter mais informações sobre como proteger os recursos do CA Identity Manager, consulte o *Guia de Instalação* do seu servidor de aplicativos.

     Clique em Avançar.

6. Selecione um diretório do CA Identity Manager para associar ao ambiente que você está criando e clique em Avançar.

7. Quando o ambiente do CA Identity Manager oferecer suporte ao provisionamento, selecione o servidor de provisionamento apropriado a ser usado.

   Observação: não há solicitação para selecionar um servidor de provisionamento se você tiver selecionado um diretório de provisionamento como o diretório do CA Identity Manager.

8. Configure o suporte para tarefas públicas. Em geral, essas tarefas são as tarefas de autoatendimento, como de autorregistro ou senha esquecida. Os usuários não precisam efetuar logon para acessar tarefas públicas.

   Observação: para permitir que os usuários usem as tarefas de autoatendimento, configure o suporte a tarefas públicas.

   a. Especifique um nome exclusivo que é adicionado ao URL para acesso a tarefas públicas.

      Exemplo: você pode usar o URL a seguir para acessar a tarefa de autorregistro padrão:

      http://*meu_servidor.minha_empresa.com*/iam/im/*alias*/index.jsp?task.tag=Self Registration

      Nesse URL, o *alias* é o nome exclusivo que você fornece.

   b. Especifique uma das contas de usuário existentes a seguir que serve como conta de usuário pública. O CA Identity Manager usa essa conta para permitir que os usuários desconhecidos acessem tarefas públicas sem a necessidade de fornecer credenciais.

      - Os usuários LDAP inserem o identificador exclusivo ou DN relativo da conta de usuário pública. Certifique-se de que esse valor é mapeado para o atributo conhecido %USER_ID% (na página 79). Por exemplo, se o DN do usuário DN for uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digite Admin1.
      - Os usuários do banco de dados relacional digitam o valor que é mapeado para o atributo conhecido %USER_ID% no arquivo de configuração de diretório ou identificador exclusivo para o usuário.

   Clique em Validar para exibir o identificador completo do usuário.

9. Selecione as tarefas e funções a serem criadas para esse ambiente. É possível executar as seguintes tarefas:

   - **Criar funções padrão**

     Criar um conjunto de tarefas e funções padrão que inicialmente são disponibilizadas no ambiente. Os administradores podem usar essas tarefas e funções como modelos para a criação de novas tarefas e funções no Console de usuário.

   - **Criar apenas a função de gerente do sistema**

     Criar somente a função Gerente do sistema e as tarefas que são associadas a ele.

     A função Gerente do sistema é necessária para acessar o ambiente.

     O Gerente do sistema pode criar tarefas e funções novas no Console de usuário.

- **Importar funções do arquivo**

  Importa um arquivo de definição de função que você exportou de outro ambiente do CA Identity Manager.

  Observação: para usar o ambiente do CA Identity Manager, o arquivo de definições de função deve incluir pelo menos a função Gerente do sistema ou uma função que inclua tarefas semelhantes.

  Selecione o botão de opção Import roles from the file e digite o caminho e o nome do arquivo das definições de função ou procure o arquivo a ser importado.

10. Selecione os arquivos de Definições de função para criar conjuntos de tarefas padrão para seu ambiente e clique em Avançar.

    Os arquivos de Definições de função são arquivos XML que definem um conjunto de tarefas e funções que são exigidas para oferecer suporte a recursos específicos. Por exemplo, se você deseja gerenciar terminais do Active Directory e UNIX NIS, selecione esses arquivos de Definições de função.

    Observação: essa etapa é opcional. Se não desejar criar tarefas padrão adicionais para oferecer suporte à nova funcionalidade, ignore esta tela.

11. Defina um usuário para atuar como Gerente do sistema para esse ambiente, como se segue:

    a. No campo Gerente do sistema, digite o valor que é mapeado para o atributo conhecido %USER_ID% no arquivo de configuração de diretório ou especifique uma das seguintes contas de usuário:

       - Os usuários LDAP inserem o identificador exclusivo ou DN relativo do usuário. Por exemplo, se o DN do usuário DN for uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digite Admin1.
       - Os usuários do banco de dados relacional digitam o identificador exclusivo do usuário.

    b. Clique em Adicionar.

       O CA Identity Manager adiciona o identificador completo do usuário à lista de usuários.

    c. Clique em Avançar.

    Observe os seguintes pontos ao especificar o Gerente do sistema:

    - O Gerente do sistema *não* deve ser o mesmo usuário que o administrador do repositório de usuários.
    - Você pode especificar múltiplos Gerentes de sistema para o ambiente. Entretanto, é possível especificar somente o Gerente do sistema inicial no Management Console. Para especificar mais Gerentes de sistema, atribua a função Gerente do sistema aos usuários apropriados no Console de usuário.

12. No campo Inbound Administrator, especifique uma conta de administrador do CA Identity Manager que possa executar tarefas administrativas que são mapeadas para mapeamentos de entrada.

    O usuário deve ser capaz de executar todas as tarefas em qualquer usuário. A função Gerenciador de sincronização de provisionamento contém as tarefas de provisionamento que são incluídas nos mapeamentos de entrada padrão.

13. Insira uma senha para o keystore, o banco de dados de chaves que criptografa e descriptografa dados.

    A definição dessa senha é um pré-requisito para definir as chaves dinâmicas. Você pode modificar a senha depois de criar o ambiente usando a tarefa Sistema, Chaves secretas.

    Uma página resumindo as configurações do ambiente é exibida.

14. Examine as configurações do ambiente. Clique em Voltar para modificar ou clique em Concluir para criar o ambiente do CA Identity Manager com as configurações atuais.

    A tela Environment Configuration Output exibe o andamento da criação do ambiente.

15. Clique em Continue para sair do assistente de ambiente do CA Identity Manager.

16. Inicie o ambiente.

    Clique no nome do ambiente e em Iniciar.

17. Se você interrompeu os Servidores de políticas na Etapa 1, reinicie-os agora.

Como acessar um ambiente do CA Identity Manager

Depois de criar um ambiente do CA Identity Manager, você pode acessá-lo digitando um URL em um navegador.

Observação: ative o JavaScript no navegador que você usa para acessar o Management Console.

O formato do URL depende de como você configurou o ambiente e do tipo de tarefa que deseja acessar.

- Para acessar tarefas protegidas no Console de usuário, use o seguinte URL:

  `http://nome_do_host/iam/im/alias`

  hostname

  Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado, por exemplo, meu_servidor.minha_empresa.com

  alias

  Define o alias do alias do ambiente, por exemplo, funcionários.

  Efetue logon no Ambiente do CA Identity Manager com uma conta de administrador privilegiado, como a conta do Gerente do sistema criada para o Ambiente do CA Identity Manager.

  Observação: todas as tarefas do CA Identity Manager são protegidas, a menos que você configure tarefas públicas.

- Para acessar tarefas públicas, que não exigem que os usuários forneçam credenciais, use um URL com o seguinte formato:

  `http://nome_do_host/iam/im/alias/index.jsp?task.tag=tasktag`

  hostname

  Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado, por exemplo, meu_servidor.minha_empresa.com.

alias

Define o alias para tarefas públicas, por exemplo, autoatendimento.

task_tag

Define o qualificador para a tarefa a ser chamada.

Você pode especificar o qualificador de tarefa quando configura uma tarefa no Console de usuário.

Os qualificadores da tarefa para as tarefas padrão de autorregistro e redefinição de senha esquecida são SelfRegistration e ForgottenPasswordReset.

Observação: para obter mais informações, consulte o *Guia de Administração*.

Como configurar um ambiente de provisionamento

Você poderá configurar um ambiente para provisionamento depois que tiver ativado o acesso ao Servidor de provisionamento (na página 171).

Em seguida, você pode criar um usuário especial do CA Identity Manager, denominado administrador de entrada, criar uma conexão com o Servidor de provisionamento e configurar a sincronização de entrada no Gerenciador de provisionamento.

Observação: sempre que você modificar as propriedades de provisionamento de um ambiente, certifique-se de reiniciar o servidor de aplicativos para que as alterações entrem em vigor.

Configurar o administrador de entrada

Para que a sincronização de entrada funcione, crie um usuário especial do CA Identity Manager chamado *administrador de entrada*. Nas releases anteriores do CA Identity Manager, o administrador de entrada era chamado de *usuário corporativo*. Nenhum usuário efetua logon nessa conta de usuário. Em vez disso, o CA Identity Manager a usa internamente. No entanto, crie essa conta de usuário e forneça a ela as tarefas apropriadas.

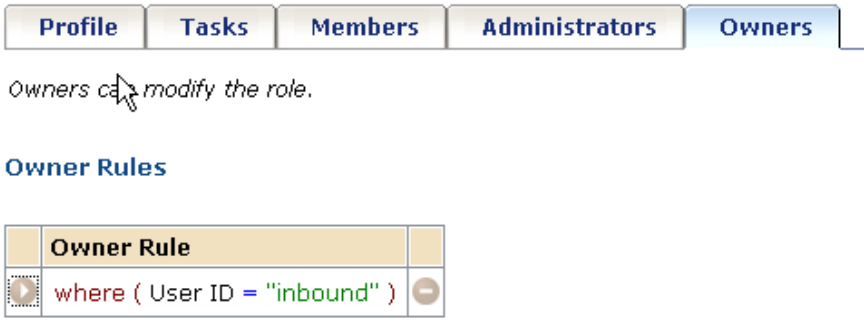
Siga estas etapas:

1. Efetue logon no ambiente do CA Identity Manager como o usuário com a função Gerente do sistema.
2. Crie um usuário. Você pode nomear a **entrada** do usuário como um lembrete de sua finalidade.

3. Escolha Funções administrativas, Modificar funções administrativas e selecione uma função que contenha as tarefas que usa para sincronização.
   - Criar usuário para provisionamento
   - Ativar/desativar usuário para provisionamento
   - Modificar usuário para provisionamento

   Observação: se você não tiver modificado as tarefas de sincronização padrão, use a função Gerenciador de sincronização de provisionamento.

4. Na guia Integrantes, adicione uma política de integrante, que inclua:
   - Uma regra de integrante que o novo usuário atenda.
   - Uma regra de escopo que forneça acesso a todos os usuários que são afetados pelas alterações no diretório de provisionamento que acionam a sincronização de entrada.

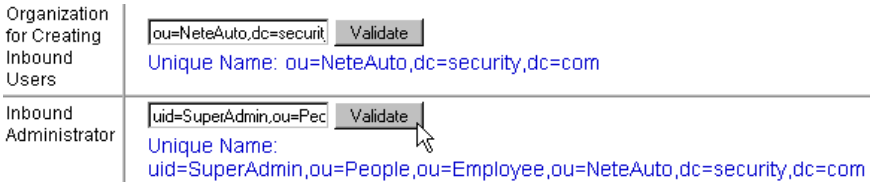


5. No Management Console:
   a. Selecione o ambiente.
   b. Selecione Advanced Settings, Provisioning.
   c. Preencha o campo Organization for Creating Inbound Users se o diretório do CA Identity Manager incluir uma organização.

      Essa organização é o local em que os usuários são criados quando a sincronização de entrada ocorre. Por exemplo, quando um usuário é adicionado ao diretório de provisionamento, o CA Identity Manager adiciona o usuário a essa organização.

d. Preencha o campo Inbound Administrator com a ID de usuário do usuário criado na Etapa 2.

e. Clique em Validate para verificar se a ID de usuário é aceita como mostrado no exemplo a seguir, onde a ID de usuário completa é exibida abaixo da ID de usuário digitada.



f. Modifique outros campos nessa tela. Nenhuma alteração é necessária.

Ao fazer modificações, entenda como os campos interagem. Para obter detalhes sobre cada campo, clique no link Help na tela.

Conectar um Ambiente ao Servidor de provisionamento

Siga estas etapas:

1. No Management Console, clique em Environments.

   Uma lista de ambientes existentes é exibida.

2. Clique no nome do ambiente que deseja associar ao Servidor de provisionamento.

3. Clique no ícone de seta para a direita no campo Provisioning Server.

   A tela Provisioning Properties é aberta.

4. Selecione o Servidor de provisionamento.

5. Clique em Save, na parte inferior da tela.

6. Configure a Sincronização no Gerenciador de provisionamento (na página 197).

Configurar a Sincronização no Gerenciador de provisionamento.

A sincronização de entrada mantém o CA Identity Manager atualizado com as alterações que ocorrem no diretório de provisionamento. As alterações incluem aquelas realizadas usando o Gerenciador de provisionamento e as alterações em terminais nos quais o Servidor de provisionamento tem um conector. Cada Servidor de provisionamento oferece suporte a um único ambiente. No entanto, é possível configurar ambientes de backup em sistemas diferentes em um cluster, caso o ambiente atual não esteja disponível.

Siga estas etapas:

1. Escolha Iniciar, CA Identity Manager, Gerenciador de provisionamento.
2. Clique em Sistema, Configuração do CA Identity Manager.
3. Preencha o campo Nome do host com o nome do sistema em que o Servidor do CA Identity Manager está instalado.
4. Preencha o campo Porta com o número da porta do servidor de aplicativos.
5. Preencha o campo Nome do ambiente com o alias do ambiente.
6. Selecione Conexão protegida se você desejar que o protocolo HTTPS se comunique com o servidor do CA Identity Manager, em vez usar HTTP e criptografar as notificações individuais.
7. Clique em Adicionar.
8. Repita as etapas de 3 a 6 para cada versão de backup do ambiente.

   Se o servidor de aplicativos para o ambiente atual estiver indisponível, o CA Identity Manager falhará em um ambiente de backup. Você pode reorganizar os ambientes atuais e de backup para definir a ordem de tolerância a falhas.
9. Se esse for o primeiro ambiente, preencha os campos Shared Secret usando a senha que foi inserida durante a instalação do CA Identity Manager para o usuário de componentes incorporados.

   Observação: esses campos não se aplicam se o FIPS estiver ativado nessa instalação.
10. Configure o Nível de log, como segue:
    - Nenhum log - nenhuma informação é gravada no arquivo de log.
    - Erro - apenas mensagens de erro serão registradas.
    - Informações - mensagens de erro e informativas são registradas (padrão).
    - Aviso - mensagens de erro, aviso e informativas são registradas.
    - Depuração - todas as informações são registradas.
11. Reinicie o servidor de aplicativos antes de efetuar logon no ambiente.

Observação: para um log de operações de sincronização de entrada e todos os problemas encontrados durante a sincronização, consulte o seguinte arquivo:

PSHOME\logs\etanotify<date>.log

Importar funções de provisionamento personalizadas

Ao criar o ambiente, você tem a opção de usar as funções padrão ou um arquivo de definição personalizado que você cria. Se você importar definições de funções personalizadas, *também* importará as definições de função Somente provisionamento. Depois de criar o ambiente, importe as definições de função do arquivo ProvisioningOnly-RoleDefinitions.xml, que está em uma destas pastas:
ferramentas_administrativas/ProvisioningOnlyRoleDefinitions/Organization
ferramentas_administrativas/ProvisioningOnlyRoleDefinitions/NoOrganization

O local padrão para *ferramentas_administrativas* é:

- **Windows**: <caminho_de_instalação>\tools
- **UNIX**: <caminho_de_instalação2>/tools

Sincronização de conta para a tarefa Redefinir senha de usuário

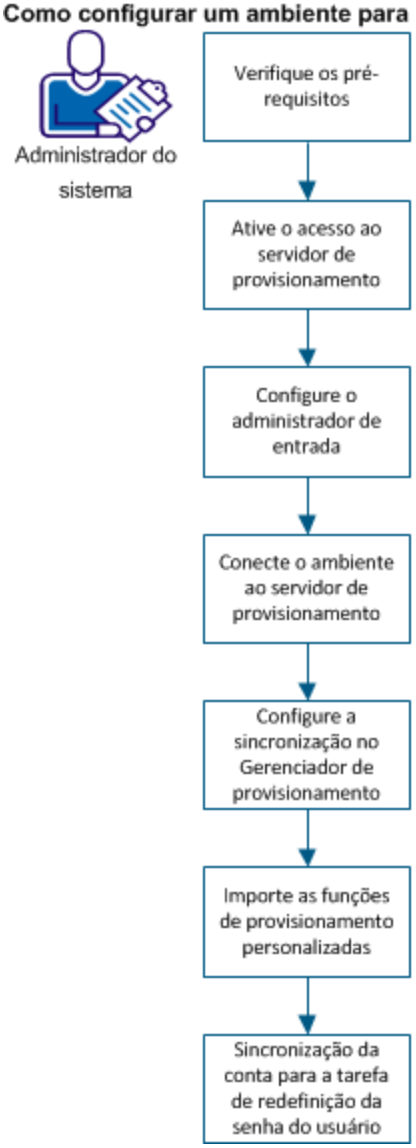
Antes de ativar o provisionamento para um ambiente do CA Identity Manager, a configuração de sincronização de conta para a tarefa Redefinir senha de usuário é definida como Ao concluir a tarefa. No entanto, quando você importa o arquivo de configuração ProvisioningOnly-RoleDefinitions.xml que cria as funções e tarefas para o provisionamento de usuários, a sincronização de conta é desativada.

Para usar Redefinir a senha de usuário para acionar a sincronização de conta, altere a sincronização de conta para essa tarefa de volta para Ao concluir a tarefa.

Como criar e implantar conectores usando o Connector Xpress

É possível configurar o provisionamento para um ambiente para fornecer contas em outros sistemas para os usuários gerenciados pelo CA Identity Manager. As contas fornecem aos usuários acesso a recursos adicionais, como uma conta de email. Forneça essas contas adicionais atribuindo funções de provisionamento, que são criadas por meio do CA Identity Manager.

Como configurar um ambiente para provisionamento



Como um administrador, execute as seguintes etapas:

1. Verificar os pré-requisitos (na página 201)
2. Ativar o acesso ao Servidor de provisionamento (na página 171)

3. Configurar o administrador de entrada (na página 195)
4. Conectar um Ambiente ao Servidor de provisionamento (na página 197)
5. Configurar a Sincronização no Gerenciador de provisionamento. (na página 197)
6. Importar funções de provisionamento personalizadas (na página 199)
7. Sincronização de conta para a tarefa Redefinir senha de usuário (na página 199)

Verificar os pré-requisitos

Antes de configurar o ambiente para o provisionamento, certifique-se de que o diretório de provisionamento esteja instalado no CA Directory. Para obter mais informações, consulte o *Guia de Instalação*.

Ativar o acesso ao Servidor de provisionamento

Você ativa o acesso ao Servidor de provisionamento usando o link Directories no Management Console.

Observação: um pré-requisito para este procedimento é instalar o Diretório de provisionamento no CA Directory. Para obter mais informações, consulte o *Guia de Instalação*.

Siga estas etapas:

1. Abra o Management Console digitando o seguinte URL em um navegador:

   `http://nome_do_host:porta/iam/immanage`

   nome do host

   Define o nome de host totalmente qualificado do sistema em que o servidor do CA Identity Manager está instalado.

   porta

   Define o número da porta do servidor de aplicativos.

2. Clique em Directories.

   A janela CA Identity Manager Directories é exibida.

3. Clique em Create from Wizard.

4. Digite o caminho e o nome do arquivo XML de diretório para configuração do Diretório de provisionamento. Ele é armazenado em directoryTemplates\ProvisioningServer na pasta Ferramentas administrativas. O local padrão dessa pasta é:

   - Windows: <caminho_de_instalação>\tools
   - UNIX: <caminho_de_instalação2>/tools

   Observação: você pode usar esse arquivo de configuração de diretório como foi instalado, sem modificação.

5. Clique em Avançar.

6. Forneça valores para os campos nessa janela, como se segue:

   Nome

   É um nome para o Diretório de provisionamento que está associado ao Servidor de provisionamento que você está configurando.

   - Se o CA Identity Manager não se integrar ao SiteMinder, especifique um nome significativo para o objeto que o CA Identity Manager usa para se conectar ao diretório de usuários.
   - Se o CA Identity Manager se integrar ao SiteMinder, você terá duas opções:

     Se desejar criar um objeto de conexão de diretório de usuários no SiteMinder, especifique um nome significativo. O CA Identity Manager cria esse objeto no SiteMinder com o nome especificado.

     Se desejar se conectar a um diretório de usuários existente do SiteMinder, especifique o nome do objeto de conexão de diretório de usuários do SiteMinder exatamente como ele aparece na interface de usuário do Servidor de políticas.

   Descrição

   (Opcional) Descreve o Diretório do CA Identity Manager.

   Host

   Especifica o nome do host ou endereço IP do sistema onde o diretório de usuários está instalado.

   Porta

   Especifica o número da porta do diretório de usuários.

Domínio

Especifica o nome do domínio de provisionamento que o CA Identity Manager gerencia.

Importante: ao criar um Diretório de provisionamento usando o Management Console com os caracteres de idioma estrangeiro como o nome de domínio, haverá falha na criação do Diretório de provisionamento.

O nome deve corresponder ao nome do domínio de provisionamento que você especificou durante a instalação.

Observação: o nome do domínio diferencia maiúsculas e minúsculas.

Nome de usuário

Especifica o usuário que pode efetuar logon no Gerenciador de provisionamento.

O usuário deve ter o perfil de Administrador de domínio ou um conjunto de privilégios equivalente para o Domínio de provisionamento.

Senha

Especifica a senha para o usuário global especificado no campo Username.

Confirmar senha

Digite novamente a senha que você digitou no campo Senha para confirmação.

Conexão segura

Indica se o CA Identity Manager usa uma conexão segura.

Certifique-se de selecionar essa opção para repositórios de usuários do Active Directory.

Parâmetros da pesquisa de diretório

maxrows define o número máximo de resultados que o CA Identity Manager pode retornar ao pesquisar um diretório de usuários. Esse valor substitui qualquer limite definido no diretório LDAP. Quando configurações conflitantes se aplicam, o servidor LDAP usa a configuração mais baixa.

Observação: o parâmetro maxrows não limita o número de resultados que são exibidos na tela de tarefas do CA Identity Manager. Para configurar as definições de exibição, modifique a definição da tela de lista no Console de usuário do CA Identity Manager. Para obter instruções, consulte o *Guia de Design do Console de Usuário*.

timeout determina o número máximo de segundos que o CA Identity Manager pesquisa um diretório antes de encerrar a pesquisa.

Failover Connections

O nome do host e o número da porta de um ou mais sistemas opcionais que são Servidores de provisionamento alternativos. Se vários servidores forem listados, o CA Identity Manager tentará estabelecer uma conexão com os sistemas na ordem em que estão listados.

Os Servidores de provisionamento alternativos serão usados se o Servidor de provisionamento principal falhar. Quando o Servidor de provisionamento principal se tornar disponível novamente, o alternativo continuará sendo usado. Se desejar voltar a usar o Servidor de provisionamento, reinicie os Servidores de provisionamento alternativo.

7. Clique em Avançar.
8. Selecione os objetos a serem gerenciados, como usuários ou grupos.
9. Após configurar os objetos de acordo com a necessidade, clique em Show summary deploy directory e verifique as configurações do Diretório de provisionamento.
10. Clique em uma destas ações:
    a. Clique em Back para modificar.
    b. Clique em Save para salvar as informações de diretório se quiser retornar mais tarde para fazer a implantação.
    c. Clique em Finish para concluir esse procedimento e começar a configurar um ambiente com provisionamento (na página 195).

Configurar o administrador de entrada

Para que a sincronização de entrada funcione, crie um usuário especial do CA Identity Manager chamado *administrador de entrada*. Nas releases anteriores do CA Identity Manager, o administrador de entrada era chamado de *usuário corporativo*. Nenhum usuário efetua logon nessa conta de usuário. Em vez disso, o CA Identity Manager a usa internamente. No entanto, crie essa conta de usuário e forneça a ela as tarefas apropriadas.

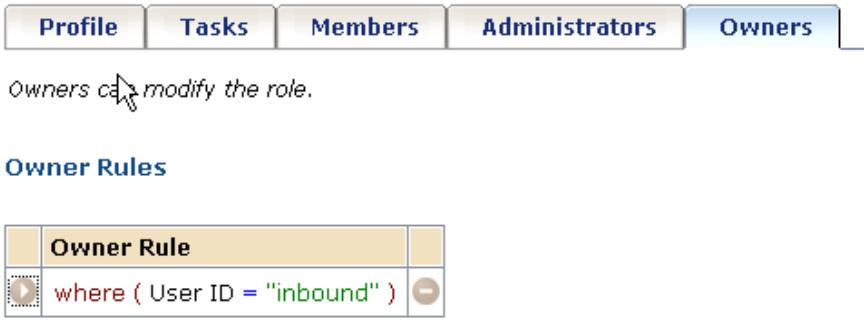
Siga estas etapas:

1. Efetue logon no ambiente do CA Identity Manager como o usuário com a função Gerente do sistema.
2. Crie um usuário. Você pode nomear a **entrada** do usuário como um lembrete de sua finalidade.

3. Escolha Funções administrativas, Modificar funções administrativas e selecione uma função que contenha as tarefas que usa para sincronização.
   - Criar usuário para provisionamento
   - Ativar/desativar usuário para provisionamento
   - Modificar usuário para provisionamento

   Observação: se você não tiver modificado as tarefas de sincronização padrão, use a função Gerenciador de sincronização de provisionamento.

4. Na guia Integrantes, adicione uma política de integrante, que inclua:
   - Uma regra de integrante que o novo usuário atenda.
   - Uma regra de escopo que forneça acesso a todos os usuários que são afetados pelas alterações no diretório de provisionamento que acionam a sincronização de entrada.

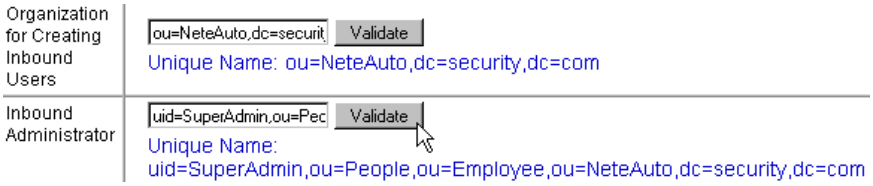


5. No Management Console:
   a. Selecione o ambiente.
   b. Selecione Advanced Settings, Provisioning.
   c. Preencha o campo Organization for Creating Inbound Users se o diretório do CA Identity Manager incluir uma organização.

      Essa organização é o local em que os usuários são criados quando a sincronização de entrada ocorre. Por exemplo, quando um usuário é adicionado ao diretório de provisionamento, o CA Identity Manager adiciona o usuário a essa organização.

d. Preencha o campo Inbound Administrator com a ID de usuário do usuário criado na Etapa 2.

e. Clique em Validate para verificar se a ID de usuário é aceita como mostrado no exemplo a seguir, onde a ID de usuário completa é exibida abaixo da ID de usuário digitada.



f. Modifique outros campos nessa tela. Nenhuma alteração é necessária.

Ao fazer modificações, entenda como os campos interagem. Para obter detalhes sobre cada campo, clique no link Help na tela.

Conectar um Ambiente ao Servidor de provisionamento

Siga estas etapas:

1. No Management Console, clique em Environments.

   Uma lista de ambientes existentes é exibida.

2. Clique no nome do ambiente que deseja associar ao Servidor de provisionamento.

3. Clique no ícone de seta para a direita no campo Provisioning Server.

   A tela Provisioning Properties é aberta.

4. Selecione o Servidor de provisionamento.

5. Clique em Save, na parte inferior da tela.

6. Configure a Sincronização no Gerenciador de provisionamento (na página 197).

Configurar a Sincronização no Gerenciador de provisionamento.

A sincronização de entrada mantém o CA Identity Manager atualizado com as alterações que ocorrem no diretório de provisionamento. As alterações incluem aquelas realizadas usando o Gerenciador de provisionamento e as alterações em terminais nos quais o Servidor de provisionamento tem um conector. Cada Servidor de provisionamento oferece suporte a um único ambiente. No entanto, é possível configurar ambientes de backup em sistemas diferentes em um cluster, caso o ambiente atual não esteja disponível.

Siga estas etapas:

1. Escolha Iniciar, CA Identity Manager, Gerenciador de provisionamento.
2. Clique em Sistema, Configuração do CA Identity Manager.
3. Preencha o campo Nome do host com o nome do sistema em que o Servidor do CA Identity Manager está instalado.
4. Preencha o campo Porta com o número da porta do servidor de aplicativos.
5. Preencha o campo Nome do ambiente com o alias do ambiente.
6. Selecione Conexão protegida se você desejar que o protocolo HTTPS se comunique com o servidor do CA Identity Manager, em vez usar HTTP e criptografar as notificações individuais.
7. Clique em Adicionar.
8. Repita as etapas de 3 a 6 para cada versão de backup do ambiente.

   Se o servidor de aplicativos para o ambiente atual estiver indisponível, o CA Identity Manager falhará em um ambiente de backup. Você pode reorganizar os ambientes atuais e de backup para definir a ordem de tolerância a falhas.
9. Se esse for o primeiro ambiente, preencha os campos Shared Secret usando a senha que foi inserida durante a instalação do CA Identity Manager para o usuário de componentes incorporados.

   Observação: esses campos não se aplicam se o FIPS estiver ativado nessa instalação.
10. Configure o Nível de log, como segue:
    - Nenhum log - nenhuma informação é gravada no arquivo de log.
    - Erro - apenas mensagens de erro serão registradas.
    - Informações - mensagens de erro e informativas são registradas (padrão).
    - Aviso - mensagens de erro, aviso e informativas são registradas.
    - Depuração - todas as informações são registradas.
11. Reinicie o servidor de aplicativos antes de efetuar logon no ambiente.

Observação: para um log de operações de sincronização de entrada e todos os problemas encontrados durante a sincronização, consulte o seguinte arquivo:

PSHOME\logs\etanotify<date>.log

Importar funções de provisionamento personalizadas

Ao criar o ambiente, você tem a opção de usar as funções padrão ou um arquivo de definição personalizado que você cria. Se você importar definições de funções personalizadas, *também* importará as definições de função Somente provisionamento. Depois de criar o ambiente, importe as definições de função do arquivo ProvisioningOnly-RoleDefinitions.xml, que está em uma destas pastas:

ferramentas_administrativas/ProvisioningOnlyRoleDefinitions/Organization
ferramentas_administrativas/ProvisioningOnlyRoleDefinitions/NoOrganization

O local padrão para *ferramentas_administrativas* é:

- **Windows**: <caminho_de_instalação>\tools
- **UNIX**: <caminho_de_instalação2>/tools

Sincronização de conta para a tarefa Redefinir senha de usuário

Antes de ativar o provisionamento para um ambiente do CA Identity Manager, a configuração de sincronização de conta para a tarefa Redefinir senha de usuário é definida como Ao concluir a tarefa. No entanto, quando você importa o arquivo de configuração ProvisioningOnly-RoleDefinitions.xml que cria as funções e tarefas para o provisionamento de usuários, a sincronização de conta é desativada.

Para usar Redefinir a senha de usuário para acionar a sincronização de conta, altere a sincronização de conta para essa tarefa de volta para Ao concluir a tarefa.

Gerenciar ambientes

Esta seção descreve como gerenciar um ambiente.

Modificar propriedades do ambiente do CA Identity Manager

A tela Environment Properties do CA Identity Manager no Management Console permite executar as seguintes tarefas:

- Exibir as configurações atuais do ambiente.
- Modificar a descrição, o URL base, bem como aliases protegidos e públicos.
- Importar um Ambiente existente do CA Identity Manager depois de uma atualização.

  Observação: para obter mais informações sobre como importar Ambientes existentes do CA Identity Manager, consulte a seção de atualização do *Guia de Instalação*.
- Iniciar e interromper o Ambiente

- Acessar páginas para configurar as tarefas a seguir:
  - **Configurações avançadas**

    Configura os recursos avançados, incluindo aqueles que são criados usando as APIs do CA Identity Manager.
  - **Configurações de função e tarefa**

    Importe um arquivo de definição de função que você exportou de outro Ambiente do CA Identity Manager.
  - **Gerente do sistema**

    Atribui funções de gerente do sistema.

Siga estas etapas:

1. Se o CA Identity Manager usar um cluster de Servidores de políticas do SiteMinder, interrompa todos, exceto um Servidor de políticas.
2. Se você tiver um cluster de nós do CA Identity Manager, interrompa todos, exceto um nó do CA Identity Manager.
3. Clique em Ambientes.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.
4. Clique no nome do Ambiente do CA Identity Manager a ser modificado.

   A tela Propriedades do CA Identity Manager é exibida e mostra as seguintes propriedades:

   OID

   Define um identificador exclusivo para o Ambiente. O CA Identity Manager gera esse identificador quando você cria um ambiente do CA Identity Manager.

   Use o OID ao configurar a remoção da tarefa de um banco de dados de persistência de tarefas. Consulte o *Guia de Instalação*.

   Nome

   Especifica o nome exclusivo do Ambiente do CA Identity Manager.

   Descrição

   Fornece uma descrição do Ambiente do CA Identity Manager.

   Diretório do CA Identity Manager

   Especifica o diretório do CA Identity Manager ao qual o Ambiente está associado.

Enable Verbose Log Output

Controla a quantidade de informações que o CA Identity Manager registra e exibe no log de Ambiente quando você importa um Ambiente. O log de Ambiente é exibido na janela de status no Management Console quando você importa um Ambiente ou outras definições de objeto de um arquivo.

Observação: a marcação dessa caixa de seleção pode ter um impacto significativo sobre o desempenho.

O log detalhado inclui mensagens de validação e implantação para cada objeto (tarefa, tela, função e política) e seus atributos no Ambiente.

Para ver o log detalhado, marque essa caixa de seleção e salve as propriedades do Ambiente. Quando você importa as funções ou outras configurações de um arquivo, as informações adicionais são exibidas no log.

Servidor de provisionamento

Especifica o diretório de provisionamento usado como repositório de usuários de provisionamento.

Clique no botão de seta para a direita para configurar o diretório de provisionamento na página Propriedades de provisionamento.

Versão

Define o número de versão do CA Identity Manager.

URL base

Especifica a parte do URL do CA Identity Manager que não inclui o alias protegido ou público para o ambiente.

O CA Identity Manager usa o URL base para formar o URL de redirecionamento que aponta para a tarefa Serviços de senha na política de senha padrão do ambiente.

Alias protegido

Define o nome do URL base para acessar tarefas protegidas no Console de usuário de um ambiente do CA Identity Manager.

Alias público

Define o nome do URL base para acessar tarefas públicas, como as tarefas de senha esquecida e autorregistro.

Usuário público

Define a conta de usuário que o CA Identity Manager usa no lugar das credenciais fornecidas pelo usuário para acessar tarefas públicas.

Tempo limite da tarefa

Determina a quantidade de tempo que o CA Identity Manager aguardará depois que uma tarefa é enviada para exibir uma mensagem de status.

Esse valor é definido na página Console de usuário em Configurações avançadas.

Status

Interrompe ou reinicia o Ambiente do CA Identity Manager.

Migrar dados de persistência de tarefas do CA Identity Manager 8.1

Migra dados de um banco de dados de persistência de tarefas do CA Identity Manager 8.1 para o banco de dados de persistência de tarefas do CA Identity Manager 12.6.5.

Para obter mais informações, consulte o *Guia de Instalação*.

Observação: o botão Migrate Task Persistence Data from CA Identity Manager 8.1 é visível apenas em ambientes que foram criados em versões anteriores do CA Identity Manager e migrados para o CA Identity Manager 12.6.5.

5. Modifique a descrição, o URL base, ou o alias protegido ou público, conforme necessário.
6. Se você modificou quaisquer propriedades do Ambiente, reinicie o Ambiente do CA Identity Manager.
7. Se você interrompeu os Servidores de políticas na Etapa 1, reinicie-os agora.

Configurações de ambiente

As informações específicas do Ambiente são armazenadas em três arquivos de configurações de ambiente:

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

Observação: o *alias* se refere ao alias do ambiente. Você especifica o alias ao criar o ambiente.

Você gera um arquivo ZIP contendo esses arquivos, que refletem a configuração atual ao exportar as configurações de ambiente.

Após exportar as configurações de ambiente, importe-as para realizar uma das tarefas a seguir:

- Gerenciar vários ambientes com configurações semelhantes. Nesse caso, você pode criar um ambiente com as configurações necessárias, importar essas configurações em outros ambientes e, em seguida, personalizar as configurações de cada ambiente, conforme a necessidade.
- Migrar um ambiente de um sistema de desenvolvimento para um sistema de produção.
- Atualizar um ambiente existente após a atualização para uma nova versão do CA Identity Manager.

Exportar um Ambiente do CA Identity Manager

Para implantar um ambiente do CA Identity Manager em um sistema de produção, exporte o ambiente de um sistema de desenvolvimento ou armazenamento temporário e importe-o no sistema de produção.

Observação: ao importar um ambiente anteriormente exportado, o CA Identity Manager exibe um log em uma janela de status no Management Console. Para ver as informações de validação e implantação para cada objeto gerenciado e seus atributos nesse log, selecione o campo Enable Verbose Log Output na página Environment Properties *antes* de exportar o ambiente. Certifique-se de que selecionar o campo Enable Verbose Log Output possa causar problemas de desempenho significativos durante a importação.

Siga estas etapas:

1. Clique em Environments no Management Console.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.

2. Selecione o ambiente que deseja exportar.
3. Clique no botão Export.

   A tela Download de arquivos é exibida.

4. Salve o arquivo ZIP em um local que possa ser acessado pelo sistema de produção.
5. Clique em Finalizar.

As informações do ambiente são exportadas para um arquivo ZIP que você pode importar em outro ambiente.

Importar um Ambiente do CA Identity Manager

Você pode importar as configurações de ambiente do CA Identity Manager para realizar uma das seguintes tarefas:

- Gerenciar vários ambientes com configurações semelhantes. Nesse caso, você pode criar um ambiente com as configurações necessárias, importar essas configurações em outros ambientes e, em seguida, personalizar as configurações de cada ambiente, conforme a necessidade.
- Migrar um ambiente de um sistema de desenvolvimento para um sistema de produção.
- Atualizar um ambiente existente após a atualização para uma nova versão do CA Identity Manager.

Siga estas etapas:

1. Clique em Environments no Management Console.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.

2. Clique no botão Import.

   A tela Import Environment é exibida.

3. Procure o arquivo ZIP exigido para importar um ambiente.
4. Clique em Finalizar.

O ambiente é importado no CA Identity Manager.

Reiniciar um Ambiente do CA Identity Manager

Siga estas etapas:

1. Clique em Environments no Management Console.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.

2. Clique no nome do ambiente do CA Identity Manager a ser iniciado.

   A tela Environment Properties do CA Identity Manager é exibida.

3. Selecione uma das seguintes opções:

   Restart Environment

   Interrompe e inicia um Ambiente.

   Parar

   Interrompe um Ambiente que está em execução no momento.

   Iniciar

   Inicia um Ambiente que não está em execução no momento.

Excluir um Ambiente do CA Identity Manager

Use este procedimento para remover um Ambiente do CA Identity Manager.

Observação: se o CA Identity Manager integra-se ao SiteMinder para autenticação avançada, ele também exclui o domínio de política do SiteMinder protegendo o ambiente e os esquemas de autenticação padrão que são criados para o ambiente.

Siga estas etapas:

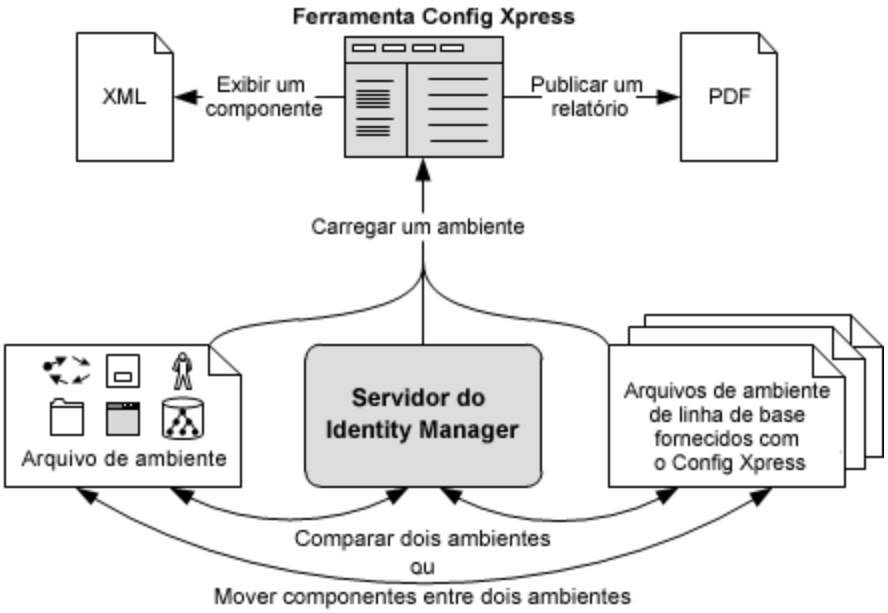
1. Na tela Ambientes, marque a caixa de seleção dos Ambientes do CA Identity Manager a serem excluídos.
2. Clique em Excluir.

   O CA Identity Manager exibirá uma mensagem de confirmação.
3. Clique em OK para confirmar a exclusão.

Gerenciar configurações

Config Xpress é uma ferramenta que está incluída no CA Identity Manager. Você pode usar essa ferramenta para analisar e trabalhar com as configurações de seus ambientes do CA Identity Manager.

E o mais importante, a ferramenta permite que você mova componentes entre ambientes. O Config Xpress detecta automaticamente todos os outros componentes necessários e solicita que você os mova também. Essa ajuda pode poupar trabalho e reduzir o risco de problemas.



Siga estas etapas:

1. Configure o Config Xpress (na página 216).
2. Para poder usar a ferramenta, carregue um ambiente do CA Identity Manager (na página 217) no Config Xpress para análise.
3. Use o Config Xpress para executar estas tarefas com o ambiente carregado:
   - Mover componentes entre ambientes (na página 219).
   - Publicar um relatório em PDF dos componentes do sistema (na página 220).
   - Exibir a configuração XML de um componente específico (na página 221).

Configurar o Config Xpress

Os arquivos de instalação do Config Xpress são incluídos na unidade de instalação, mas a ferramenta não é instalada.

O Config Xpress tem os seguintes requisitos de software:

- CA Identity Manager r12.0 e posterior
- Sistema operacional Windows
- Adobe Air Runtime
- Leitor de PDF para exibir relatórios

Siga estas etapas:

1. Faça download do Adobe Air Runtime em http://get.adobe.com/air e instale-o.
2. Certifique-se de que as Ferramentas de Administração estejam instaladas.
3. Examine o local a seguir para o arquivo de instalação do Config Xpress:

   ```
   C:\Arquivos de programas\CA\Identity Manager\IAM Suite\Identity Manager\tools\ConfigXpress
   ```
4. Execute Config Xpress.air para instalar o Config Xpress.
5. Quando a instalação estiver concluída, o Config Xpress será iniciado.

Carregar um Ambiente no Config Xpress

Para que você possa usar o Config Xpress, carregue um ou mais ambientes na ferramenta. Essa tarefa permite que você trabalhe com o ambiente no Config Xpress.

Você pode carregar um ambiente no Config Xpress diretamente de um servidor do CA Identity Manager em tempo real ou pode carregá-lo de um arquivo de ambiente. Ao usar um dos arquivos de ambiente de linha de base que são instalados com o Config Xpress, você poderá comparar seu ambiente com a configuração pronta para uso.

O processo de carregar um ambiente pode levar alguns minutos.

Siga estas etapas:

1. Abra o Config Xpress.
2. Para carregar um **ambiente em tempo real** diretamente de um servidor do CA Identity Manager:
   a. Clique na guia Servidor (Rede).
   b. Digite o nome e a porta do servidor do CA Identity Manager. Por exemplo:

      `nome_do_servidor.ca.com:8080`

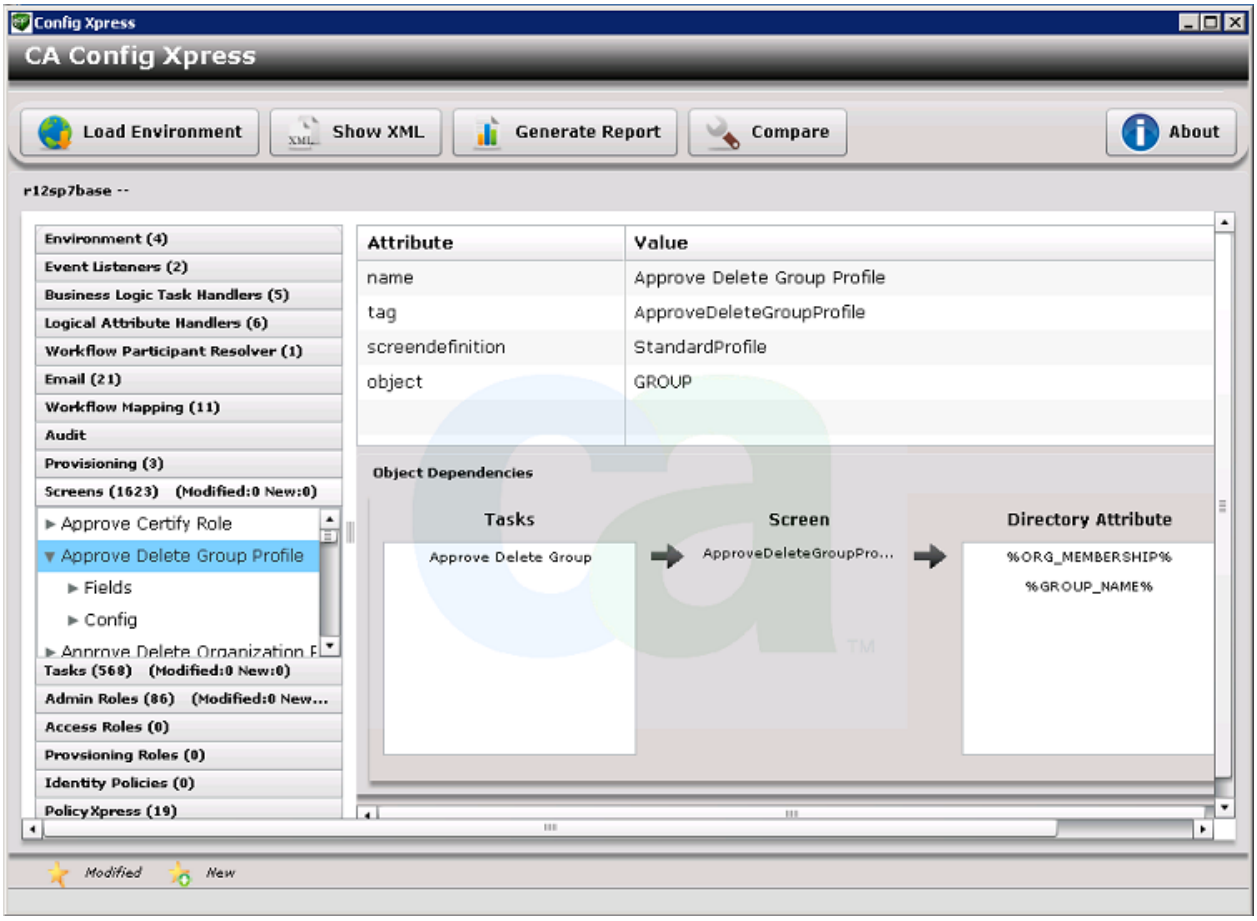
   c. Selecione Usar HTTPS se o servidor estiver configurado para permitir somente HTTPS.
   d. Selecione 12.5 SP7 se a versão do servidor for mais recente do que a release r12.5 SP6.
   e. Clique em Conectar.
   f. Escolha um ambiente na lista *Choose Environment to load* e clique em Carregar.
3. Para carregar um **arquivo de ambiente** que tenha sido exportado do ambiente do CA Identity Manager:
   a. Exporte um ambiente do CA Identity Manager.
   b. Em Config Xpress, clique na guia Sistema de arquivos.
   c. Selecione a versão, procure o arquivo de ambiente e clique em Carregar.
4. Para carregar um **arquivo de ambiente de linha de base** que foi instalado com o Config Xpress:
   a. Clique na guia Base Versions.
   b. Selecione a versão necessária e clique em Selecionar.

O Config Xpress analisa o ambiente e exibe os respectivos detalhes.

Agora, é possível publicar parte do ambiente, ou todo ele, como PDF (na página 220) ou XML (na página 221). Ao carregar um segundo ambiente, você pode comparar esses ambientes e mover componentes (na página 219) entre eles.

Exemplo: Config Xpress depois de carregar um arquivo de configuração de linha de base

Esta captura de tela mostra como o Config Xpress exibe objetos dependentes:



Mover um componente de um ambiente para outro

Sem o Config Xpress, a tarefa de mover componentes entre áreas de armazenamento temporário é complexa e apresenta probabilidade de falhas.

Quando você usa o Config Xpress para mover componentes, a ferramenta também move todos os objetos necessários. Por exemplo, se você mover uma tarefa que exija uma tela, o Config Xpress perguntará se você também deseja selecionar os componentes necessários. O Config Xpress compreende que a tarefa usa essa tela e que ela também deve ser movida para o ambiente de destino.

Se você quiser mover um componente para um ambiente em tempo real, o Config Xpress carrega-o imediatamente. Se você quiser mover o componente para um arquivo de ambiente, salve o componente como um arquivo XML e importe esse arquivo no ambiente.

Siga estas etapas:

1. Carregue o ambiente que contém o componente que você deseja mover.
2. Compare esse ambiente com um segundo:
   a. Clique em Comparar.
   b. Carregue o ambiente de destino.

      O Config Xpress exibe uma lista de diferenças entre os dois ambientes.
3. Na lista de diferenças, localize um componente que deseja mover. Você pode clicar na coluna Nome para classificar a lista.
4. Para cada componente, siga estas etapas:
   a. Selecione o item na coluna Ação.

      O Config Xpress analisa o componente; isso pode levar algum tempo.
   b. Se o componente tiver quaisquer componentes dependentes, a caixa Add Modified Dependant Screens é exibida. Clique em Sim ou Não para continuar.

   Quando tiver selecionado todos os componentes que deseja mover, você estará pronto para mover os componentes atualizados.
5. Se estiver movendo os componentes para um servidor em tempo real, clique em Carregar para.

   Os componentes são movidos imediatamente.
6. Se você movendo os componentes para um arquivo de ambiente:
   a. Clique em Salvar.
   b. Digite um nome de arquivo e clique em Salvar novamente.

      O Config Xpress salva todos os componentes selecionados em um arquivo XML. Agora, é possível importar esse arquivo XML no ambiente de destino.

Publicar um relatório em PDF

O Config Xpress pode gerar um relatório que documenta o estado atual de um ambiente do CA Identity Manager. É possível usar esse relatório para obter um instantâneo de um ambiente de produção. Ao gerar o relatório, você escolhe se deseja incluir a configuração completa ou apenas as alterações desde a instalação.

Esse relatório é útil para referência futura ou como parte de um plano de recuperação do sistema.

Siga estas etapas:

1. Carregue um ambiente no Config Xpress.
2. Clique em Generate Report.

   Na caixa de diálogo Generate PDF Report, você pode alterar o tamanho da fonte e pode inserir texto para as páginas de rosto ou título. Também é possível optar por incluir todos os itens de configuração ou apenas os itens novos ou modificados.

   Importante: se você não clicar na caixa *Only include details of new or modified tasks, screens, roles*, o relatório conterá o ambiente todo. O arquivo PDF terá aproximadamente 2.000 páginas e mais de 40 MB.
3. Clique em OK.
4. Digite um nome de arquivo e salve o relatório. Esse processo pode levar alguns minutos ou muito mais se você optar por publicar o ambiente todo.

   O relatório é aberto no leitor de PDF.

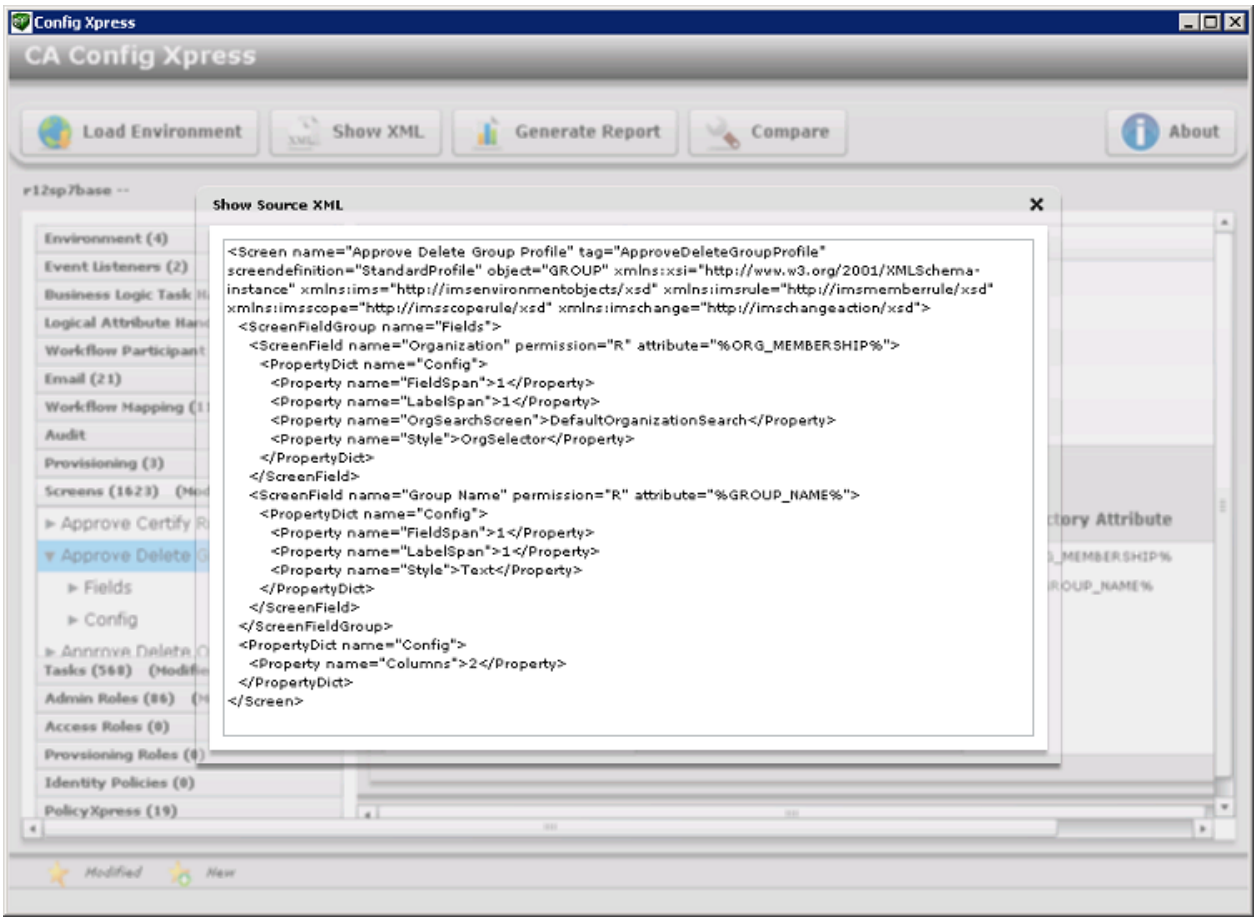
Exibir configuração XML

O Config Xpress pode exibir a configuração XML para um determinado componente. Você pode estudar esse arquivo XML para entender um sistema.

Siga estas etapas:

1. Carregue um ambiente no Config Xpress.
2. Clique em um componente na tela Config Xpress.
3. Clique em Show XML.

   A configuração XML é exibida:



Otimizar avaliação de regra de política

As regras de política, que dinamicamente identificam um conjunto de usuários, são usadas na avaliação de políticas de integrante, administrador e proprietário da função, bem como de políticas de identidade. A avaliação dessas regras pode demorar bastante em grandes implementações do CA Identity Manager.

Observação: para obter mais informações sobre as políticas de integrante, administrador, proprietário e identidade, consulte o *Guia de Administração*.

Para reduzir o tempo de avaliação para regras que incluem atributos de usuário, você pode ativar a opção de avaliação em memória. Quando a opção de avaliação na memória estiver ativada, o CA Identity Manager irá recuperar informações sobre um usuário a ser avaliado do repositório de usuários e armazenará uma representação desse usuário na memória. O CA Identity Manager usa a representação na memória para comparar valores de atributo em relação às regras da política. Isso limita o número de chamadas que o CA Identity Manager faz diretamente para o repositório de usuários.

Você ativa a opção de avaliação na memória para um ambiente no Management Console.

Siga estas etapas:

1. Abra o console de gerenciamento.
2. Selecione Environments, *nome do ambiente*, Advanced Settings, Miscellaneous.

   A página User Defined Properties é aberta.
3. Insira o texto a seguir no campo Property:

   UseInMemoryEvaluation
4. Insira *um* dos seguintes números no campo Value:

   0

   A avaliação na memória é desativada.

   1

   A avaliação na memória é ativada. Quando essa opção é especificada, a comparação de atributos diferencia letras maiúsculas de minúsculas.

   3

   A avaliação na memória é ativada. Quando essa opção é especificada, a comparação de atributos não diferencia letras maiúsculas de minúsculas.
5. Clique em Adicionar.

   O CA Identity Manager adiciona a nova propriedade à lista de propriedades existentes do ambiente.
6. Clique em Salvar.

Configurações de função e tarefa

Na tela Role and Task Settings no Management Console, você pode importar ou exportar configurações de tela, guia e tarefa em um arquivo XML, chamado de arquivo de Definições de função. O CA Identity Manager fornece os arquivos de Definições de função predefinidos que criam telas, guias, funções e tarefas para um conjunto de funcionalidades. Por exemplo, há um arquivo de Definições de função que oferece suporte ao Provisionamento inteligente e outros arquivos que oferecem suporte às telas de gerenciamento de terminal.

Além disso, você pode usar um arquivo de Definições de função para aplicar as configurações de um ambiente em vários ambientes. Execute as tarefas a seguir:

- Defina as configurações de tela, guia, tarefa e função em um ambiente.
- Exporte essas configurações para um arquivo XML.
- Importe o arquivo XML no ambiente necessário.

Exportar configurações de função e tarefa

Execute o procedimento a seguir para exportar as configurações de tarefa e função.

Siga estas etapas:

1. No Management Console, clique em Environments.

   Uma lista de ambientes do CA Identity Manager é exibida.

2. Clique no nome do ambiente adequado do CA Identity Manager.

   A janela Properties desse ambiente é exibida.

3. Clique em Role and Task Settings e em Export.

4. Clique em Open para exibir o arquivo em uma janela do navegador ou em Save para salvar as configurações em um arquivo XML.

Importar configurações de função e tarefa

As configurações de função e tarefa são definidas nos arquivos XML, denominados arquivos de Definições de função. Você pode importar arquivos de Definições de função predefinidos para oferecer suporte a conjuntos específicos de funcionalidades do CA Identity Manager (por exemplo, Provisionamento inteligente) ou importar arquivos de Definições de função de um ambiente para outro.

Observação: também é possível importar definições de função para conectores personalizados que são criados com o Connector Xpress. Você cria esses arquivos de definições de função com o Role Definitions Generator. Para obter mais informações, consulte o *Guia do Connector Xpress*.

Execute o procedimento a seguir para importar as configurações de tarefa e função.

Siga estas etapas:

1. No Management Console, clique em Environments.

   Uma lista de ambientes do CA Identity Manager é exibida.

2. Clique no nome do ambiente do CA Identity Manager onde você deseja importar as configurações de função e tarefa.

   A janela Properties desse ambiente é exibida.

3. Clique em Role and Task Settings e em Import.

4. Execute uma das seguintes ações:

   - Selecione um ou mais arquivos de Definições de função para criar funções e tarefas padrão para o ambiente.

     Para selecionar todos os arquivos de Definições de função, clique em Select/Deselect All.

   - Digite o caminho e o nome do arquivo de definições de função a ser importado ou procure o arquivo. Clique em Finish.

5. Clique em Finalizar.

   O status é exibido na janela Role Configuration Output.

6. Clique em Continuar para sair.

Como criar funções e tarefas para terminais dinâmicos

Usando o Connector Xpress, você pode configurar conectores dinâmicos para permitir o provisionamento e o gerenciamento de bancos de dados SQL e diretórios LDAP. Para cada conector dinâmico, é possível usar o Role Definitions Generator para criar definições de tarefa e tela para telas de gerenciamento de conta que aparecem no Console de usuário.

Depois de executar o Role Definitions Generator, importe o arquivo de Definições de função resultante (na página 224) no Management Console.

Observação: para obter mais informações sobre o Role Definitions Generator, consulte o *Guia do Connector Xpress*.

Modificar a conta do gerente do sistema

Um gerente do sistema é responsável por configurar e manter um ambiente do CA Identity Manager. Geralmente, as tarefas de um gerente do sistema incluem:

- Criação e gerenciamento do ambiente inicial
- Criação e modificação de funções administrativas
- Criação e modificação de outras contas de administrador

Você cria uma conta de gerente do sistema quando cria um ambiente do CA Identity Manager. Se essa conta for "bloqueada", por exemplo, se o gerente do sistema esquecer a senha, você poderá recriar a conta usando o assistente do Gerente do sistema.

O assistente do Gerente do sistema guia você pelas etapas de atribuição de uma função de gerenciamento do sistema a um usuário.

Observe os seguintes pontos antes de modificar a conta do Gerente do sistema:

- Suponha que você esteja usando um repositório de usuários LDAP e que configurou um recipiente de usuários como ou=People no arquivo de configuração de diretório (directory.xml) para o seu diretório do CA Identity Manager. Os usuários selecionados devem existir no mesmo recipiente em que você configura o gerente do sistema. A seleção de uma conta de usuário que não existe no recipiente de usuários pode causar falhas.
- Quando o ambiente do CA Identity Manager gerencia um diretório de usuários com um estrutura simples ou estrutura de usuários simples, o perfil do usuário selecionado também deverá incluir a organização. Para garantir que o perfil de um usuário seja configurado corretamente, adicione o nome da organização do usuário ao atributo físico correspondente ao atributo conhecido %ORG_MEMBERSHIP% no arquivo directory.xml (na página 86). Por exemplo, quando a descrição do atributo físico é mapeada para o atributo conhecido %ORG_MEMBERSHIP% no arquivo directory.xml e o usuário pertence à organização Funcionários, o perfil do usuário deve conter o par atributo/valor descrição=Funcionários.

Siga estas etapas:

1. Na tela de ambientes do CA Identity Manager, clique no nome do ambiente adequado do CA Identity Manager.

   A tela de propriedades desse ambiente específico é exibida.

2. Clique em Gerente do sistema.

   O assistente do Gerente do sistema é exibido.

3. Digite um nome exclusivo para o usuário com a função Gerente do sistema da seguinte maneira:

   - Para usuários do banco de dados relacional, digite o identificador exclusivo do usuário ou o valor que é mapeado para o atributo conhecido %USER_ID% no arquivo de configuração de diretório.
   - Para usuários LDAP, digite o DN relativo do usuário. Por exemplo, se o DN do usuário for uid=Admin1, ou=People, ou=Employees, ou=NeteAuto, digite Admin1.

   Observação: certifique-se de que o Gerente do sistema *não* é o mesmo usuário que o administrador do repositório de usuários.

4. Clique em Validar para exibir o identificador completo do usuário.

5. Clique em Avançar.

6. Na segunda página do assistente, selecione uma função para atribuir ao usuário da seguinte maneira:
   - Se você desejar atribuir a função Gerente do sistema, execute as seguintes tarefas:
     a. Selecione o botão de opção próximo à função Gerente do sistema.
     b. Clique em Finalizar.
   - Se você desejar atribuir uma função diferente da função Gerente do sistema, execute as seguintes tarefas:
     a. Selecione uma condição da primeira lista.
     b. Digite um nome de função completo ou parcial, ou um asterisco (*) na segunda caixa de listagem. Clique em Pesquisar.
     c. Selecione a função a ser atribuída na lista de resultados de pesquisa.
     d. Clique em Finalizar.

   A tela System Manager Configuration Output exibe as informações de status.
7. Clique em Continuar para fechar o assistente do Gerente do sistema.

Acessar o status de um ambiente do CA Identity Manager

O CA Identity Manager inclui uma página de status que pode ser usada para verificar os seguintes status:

- Se o diretório do CA Identity Manager foi carregado corretamente.
- Se o CA Identity Manager pode se conectar ao repositório de usuários.
- Se o Ambiente do CA Identity Manager é carregado corretamente.

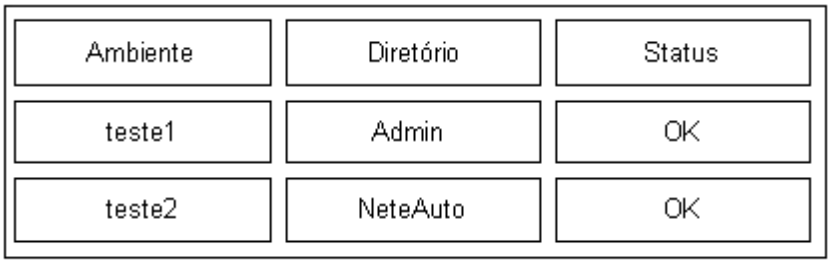
Para acessar a página de status, digite o seguinte URL em um navegador:

`http://`*`nome_do_host`*`/iam/im/status.jsp`

hostname

Determina o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado, por exemplo, meu_servidor.minha_empresa.com.

Se o Ambiente do CA Identity Manager for iniciado corretamente e todas as conexões estiverem sendo executadas com êxito, a página de status se parecerá com esta ilustração:



A página de status também indica se o ambiente é compatível com o FIPS 140-2.

Solucionando problemas dos ambientes do CA Identity Manager

A tabela a seguir descreve as possíveis mensagens de erro e o processo de solução de problemas:

Mensagem	Descrição	Solução de problemas
Não carregado	O Diretório do CA Identity Manager que é associado ao ambiente não foi carregado quando o CA Identity Manager foi iniciado.	1. Verifique se o repositório de usuários está em execução. Se o CA Identity Manager se integrar ao SiteMinder, verifique se o SiteMinder pode se conectar ao repositório de usuários.
Sem conexão	O CA Identity Manager não pode se conectar ao Diretório do CA Identity Manager.	Na interface de usuário do Servidor de políticas, você pode verificar a conexão abrindo a página de propriedades da conexão do Diretório de usuários do SiteMinder que está associado ao repositório de usuários e clicar no botão Exibir conteúdos. Se for possível exibir o conteúdo do repositório de usuários, o SiteMinder poderá se conectar com êxito. Para obter mais informações sobre o Servidor de políticas, consulte o *Guia de Configuração do Servidor de Políticas do CA SiteMinder Web Access Manager*. 2. Reinicie o CA Identity Manager e o Servidor de políticas.

Mensagem	Descrição	Solução de problemas
Não há conexão com o SM	O CA Identity Manager não pode se conectar ao Servidor de políticas do SiteMinder (para implementações que incluem o SiteMinder)	1. Verifique as seguintes condições: ■ O Servidor de políticas está em execução. ■ O Agente web está protegendo recursos. Você pode verificar se o agente web está sendo executado corretamente acessando a interface de usuário do Servidor de políticas. Se você for solicitado a fornecer as credenciais, o agente web está funcionando corretamente. 2. Reinicie o CA Identity Manager e o Servidor de políticas.
O IMS não está disponível agora	Ocorreu um erro no CA Identity Manager.	Verifique o log do servidor de aplicativos para obter detalhes do erro.
Mensagem de erro 500 do Windows	A página de status não é exibida quando é acessada na remoção da conectividade com o diretório de usuários LDAP.	Defina a opção do navegador da internet "Show friendly error message" para desativa a exibição da página de status.

Capítulo 7: Configurações avançadas

A janela Advanced Settings no Management Console permite que você faça a seguintes configurações:

- Acesse as telas para definir as configurações avançadas
- Importe e exporte configurações avançadas, conforme descrito em Importar/exportar configurações personalizadas (na página 245).

Esta seção contém os seguintes tópicos:

Auditoria

Os logs de auditoria mantêm registros das operações realizadas em um ambiente do CA Identity Manager. É possível usar os dados nos logs de auditoria para monitorar as atividades do sistema.

O CA Identity Manager faz a auditoria de *eventos*. Um evento é uma operação gerada por uma tarefa do CA Identity Manager. Uma tarefa pode gerar vários eventos. Por exemplo, a tarefa CreateUser pode gerar os eventos CreateUserEvent e AddToGroupEvent.

Por padrão, o CA Identity Manager exporta todas as informações de eventos para o banco de dados de auditoria. Para controlar o tipo e a quantidade de informações de eventos que o CA Identity Manager registra, é possível executar as seguintes tarefas:

- Ativar a auditoria das tarefas administrativas do CA Identity Manager.
- Ativar a auditoria de alguns ou todos os eventos do CA Identity Manager gerados pela tarefas administrativas.
- Registrar informações sobre eventos em determinados estados, por exemplo, quando um evento é concluído ou cancelado.
- Registrar em log informações sobre os atributos envolvidos em um evento. Por exemplo, você pode registrar em log os atributos que mudam durante um ModifyUserEvent.
- Defina o nível de auditoria para os eventos e atributos.

Manipuladores de tarefas de lógica de negócios

Um Manipulador de tarefas de lógica de negócios executa a lógica de negócios personalizada antes que uma tarefa do CA Identity Manager seja enviada para processamento. Normalmente, a lógica de negócios personalizada valida os dados. Por exemplo, um manipulador de tarefas de lógica de negócios pode verificar o limite de associação de um grupo antes que o CA Identity Manager adicione um integrante ao grupo. Quando o limite de associação ao grupo for atingido, o manipulador de tarefas de lógica de negócios exibirá uma mensagem informando o administrador do grupo que o novo integrante não pôde ser adicionado.

Você pode usar os manipuladores de tarefas de lógica de negócios predefinidos ou criar os manipuladores personalizados usando a API do Manipulador de tarefas de lógica de negócios.

Observação: para obter informações sobre a criação de lógica de negócios personalizada, consulte o *Guia de Programação do Java*.

A tela Manipuladores de tarefas de lógica de negócios contém uma lista de manipuladores de tarefas de lógica de negócios globais existentes. A lista inclui os manipuladores predefinidos fornecidos com o CA Identity Manager e todos os manipuladores personalizados definidos em seu site. O CA Identity Manager executa os manipuladores na ordem em que aparecem na lista.

Os manipuladores de tarefas de lógica de negócios globais pode ser implementados somente em Java.

Limpar campos de senha automaticamente na tarefa Redefinir senha de usuário

É possível configurar o CA Identity Manager para limpar automaticamente os campos de senha quando um valor previamente inserido viola uma política de senha ou quando os valores nos campos Senha e Confirmar senha não correspondem.

Siga estas etapas:

1. Abra o Management Console.
2. Selecione o ambiente que deseja gerenciar e clique em Advanced Settings.

   A página Advanced Settings é exibida.
3. Clique em Business Logic Task Handlers, BlthPasswordServices.

   A página Business Logic Handler Properties é exibida.
4. Crie as propriedades a seguir:

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. Verifique se as configurações ConfirmPasswordHandler são as seguintes:
   - Object type – Usuário
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   Agora, os usuários podem limpas os campos de senha na tarefa Redefinir senha de usuário.

Lista de eventos

As tarefas administrativas incluem *eventos*, ações que o CA Identity Manager executa para concluir a tarefa. Uma tarefa pode incluir vários eventos. Por exemplo, a tarefa Criar usuário pode incluir eventos de criação do perfil de um usuário, adicionar o usuário a um grupo e atribuir funções.

O CA Identity Manager audita eventos, aplica regras de negócios específicas de cliente que estão associadas a eventos e, quando os eventos são mapeados para os processos de fluxo de trabalho, exige aprovação para eventos.

Use essa página para exibir uma lista dos eventos que estão disponíveis no CA Identity Manager.

Notificações por email

O CA Identity Manager pode enviar notificações por email quando uma tarefa ou um evento é concluído, ou quando um evento no controle de fluxo de trabalho atinge um estado específico. Por exemplo, um email pode informar um aprovador que um evento exige aprovação.

Para especificar o conteúdo das notificações por email, é possível usar modelos de email predefinidos ou personalizar os modelos para atender às suas necessidades.

Usando o Management Console, você pode executar as seguintes tarefas:

- Ativar notificações por email para um ambiente do CA Identity Manager.
- Especificar os conjuntos de modelos para criar mensagens de email.
- Indicar os eventos e as tarefas para os quais as notificações por email são enviadas.

Ouvinte de eventos

Uma tarefa do CA Identity Manager é composta por uma ou mais ações, eventos nomeados que o CA Identity Manager executa durante a execução da tarefa. Por exemplo, a tarefa Criar usuário pode incluir os seguintes eventos:

- CreateUserEvent — cria um perfil de usuário em uma organização
- AddToGroupEvent — (opcional) adiciona o usuário como um integrante de um grupo
- AssignAccessRole — (opcional) atribui uma função de acesso ao usuário

Um *ouvinte de eventos* "escuta" um evento específico e, em seguida, executa a lógica de negócios personalizada em um ponto específico do ciclo de vida de um evento. Por exemplo, depois que um novo usuário é criado no CA Identity Manager, um ouvinte de eventos pode adicionar as informações de um usuário a um banco de dados de outro aplicativo.

Observação: para obter mais informações sobre como configurar ouvintes de eventos, consulte o *Guia de Programação do Java*.

Políticas de identidade

Uma política de identidade aplica-se a um conjunto de mudanças nos negócios para os usuários que atendem a determinadas regras ou condições. Você pode usar as políticas de identidade para executar as seguintes tarefas:

- Automatizar determinadas tarefas de gerenciamento de identidade, como a atribuição de funções e associação ao grupo, alocação de recursos ou modificação dos atributos de perfil do usuário.
- Aplicar a segregação de tarefas. Por exemplo, você pode criar uma política de identidade que proíba os integrantes da função Verificar atribuidor de ter a função Verificar aprovador.
- Aplicar conformidade. Por exemplo, você pode fazer a auditoria de usuários que tenham um determinado cargo e que podem ganhar mais de US$ 100.000.

É possível criar e gerenciar conjuntos de políticas de identidade no Console de usuário. Para obter mais informações sobre políticas de identidade, consulte o *Guia de Administração*.

Antes de usar políticas de identidade, use o Management Console para executar as seguintes tarefas:

- Ativar políticas de identidade para um ambiente do CA Identity Manager.
- Definir o nível máximo de recursão (opcional).

Manipuladores de atributos lógicos

Os atributos lógicos do CA Identity Manager permitem exibir atributos do repositório de usuários (chamados de *atributos físicos*) em um formato amigável ao usuário nas telas de tarefas. Os administradores do CA Identity Manager usam as telas de tarefas para executar funções no CA Identity Manager.

Os atributos lógicos não existem em um repositório de usuários. Em geral, eles representam um ou mais atributos físicos para simplificar a apresentação. Por exemplo, a *data* do atributo lógico pode representar os atributos físicos *dia*, *mês* e *ano*.

Os atributos lógicos são processados pelo atributo Logical que são objetos Java que são escritos utilizando a API do atributo Logical. Por exemplo, quando uma tela de tarefas é exibida, um manipulador de atributos lógicos pode converter dados de atributo físico do repositório de usuários em dados de atributo lógico.

Você pode usar os atributos lógicos predefinidos e os manipuladores de atributo lógico incluídos com o CA Identity Manager ou pode criar outros usando a API do atributo Logical.

Observação: para obter mais informações, consulte o *Guia de Programação do Java*.

Diversos

As propriedades definidas pelo usuário que estão definidas nessa tela se aplicam a todo o ambiente do CA Identity Manager. Elas são passadas como pares de nome/valor para o método init() de cada objeto Java personalizado que você cria com as APIs do CA Identity Manager. Um objeto personalizado pode usar esses dados de qualquer forma exigida pela lógica de negócios do objeto.

As propriedades definidas pelo usuário também são definidas para um determinado objeto personalizado. Por exemplo, suponha que as propriedades definidas pelo usuário sejam definidas na tela Propriedades de um ouvinte de eventos denominado MyListener. As propriedades definidas pelo usuário específicas de objeto e as propriedades de todo o ambiente definidas nas telas Diversos são transmitidas em uma chamada única para MyListener.init().

Para adicionar uma propriedade definida pelo usuário, especifique um nome e valor de propriedade e clique em Adicionar.

Para excluir uma ou mais propriedades definidas pelo usuário, marque a caixa de seleção ao lado de cada par de nome/valor a ser excluído e clique em Excluir.

Depois que as alterações forem efetuadas, clique em Salvar. Reinicie o servidor de aplicativos para que as alterações entrem em vigor.

Observação: todas as diversas propriedades diferenciam maiúsculas de minúsculas. Portanto, se você definir uma propriedade denominada SelfRegistrationLogoutUrl e outra propriedade denominada selfregistrationlogouturl, ambas serão adicionadas.

Regras de notificação

Uma regra de notificação determina os usuários que receberão uma notificação por email. Quando uma tarefa for concluída ou um evento em uma tarefa atingir um determinado estado, como aprovação pendente, aprovado ou rejeitado, os usuários receberão uma notificação por email de acordo com a regra de notificação.

Observação: para obter mais informações sobre o recurso de notificação por email, consulte o *Guia de Administração*.

O CA Identity Manager inclui as seguintes regras de notificação predefinidas:

ADMIN_ADAPTER

Envia uma mensagem de email ao administrador que inicia a tarefa

USER_ADAPTER

Envia uma mensagem de email ao usuário afetado pela tarefa

USER_MANAGER

Envia um email ao gerente do usuário no contexto atual

Para criar regras de notificação personalizadas, use a API de regra de notificação.

Observação: para obter mais informações sobre as regras de notificação, consulte o *Guia de Programação do Java*.

Seletores de organização

Um setor de organização é um manipulador de atributos lógicos personalizado que determina onde o CA Identity Manager cria o perfil de um usuário autorregistrado, que se baseia em informações que o usuário fornece durante o registro. Por exemplo, o perfil dos usuários que fornecem um código promocional quando eles se registram pode ser adicionado a uma organização de Usuários promocionais.

Provisionamento

Use essa tela quando estiver usando o CA Identity Manager com provisionamento.

Observação: um procedimento mais detalhado, configurando o provisionamento de um ambiente do CA Identity Manager (na página 195), fornece instruções passo a passo.

As opções de Propriedades de provisionamento são as seguintes:

Ativado

Especifica o uso de dois repositórios de usuários, um para o CA Identity Manager e outro separado (chamado de Diretório de provisionamento) para contas de provisionamento. Se essa opção for desativada, apenas o repositório de usuários do CA Identity Manager será usado.

Usar pool de sessão

Ativa o uso de um pool de sessão.

Sessões iniciais do pool de sessão

Define o número mínimo de sessões disponíveis no pool na inicialização.

Padrão: 8

Máximo de sessões do pool de sessão

Define o número máximo de sessões no pool.

Padrão: 32

Ativar alterações de senha de contas de terminal

Define a configuração para Ativar agente de sincronização de senhas de cada usuário no Servidor de provisionamento. Essa opção permite a sincronização de senhas entre os usuários do CA Identity Manager e contas de termina associadas.

Ativar acumulação de eventos de associação da função de provisionamento

Se ativada, essa caixa de seleção garante que o CA Identity Manager execute os eventos relacionados à associação da função de provisionamento em uma ordem específica. Todas as ações de adição são combinadas em uma única operação e enviadas ao Servidor de provisionamento para processamento. Após a conclusão do processamento das ações de adição, o CA Identity Manager reúne as ações de remoção em uma única operação e envia essa operação ao servidor de provisionamento. Um único evento, denominado AccumulatedProvisioningRoleEvent, é gerado para executar os eventos nessa ordem.

Observação: para obter mais informações sobre o AccumulatedProvisioningRoleEvent, consulte o *Guia de Administração*.

Organização para criação de usuários de entrada

Define o caminho totalmente qualificado para o repositório de usuários que o CA Identity Manager usa. Esse campo é exibido apenas quando o repositório de usuários inclui uma organização.

Administrador de entrada

Define uma conta de administrador do CA Identity Manager que pode executar tarefas que são mapeadas para mapeamentos de entrada. Essas tarefas estão incluídas na função Gerenciador de sincronização de provisionamento função. O administrador deve ser capaz de executar cada tarefa em qualquer usuário do CA Identity Manager.

Diretório de provisionamento

O Diretório de provisionamento é um repositório de informações de provisionamento, incluindo domínio, usuários globais, tipos de terminal, terminais, contas e modelos de conta. Ao selecioná-lo, outras opções são exibidas para mapeamento do repositório de usuários do CA Identity Manager para o Diretório de provisionamento.

Ativar pool de sessão

Para melhorar o desempenho, o CA Identity Manager pode pré-alocar várias sessões para pool ao se comunicar com o Servidor de provisionamento.

Se a opção Pools de sessão for desativada, o CA Identity Manager irá criar e destruir sessões conforme a necessidade.

Em um novo ambiente, os pools de sessão são ativados por padrão. Em ambientes existentes, você pode ativar os pools de sessão.

Siga estas etapas:

1. No Management Console, escolha Advanced Settings, Provisioning.
2. Selecione Use Session Pool.
3. Defina o número mínimo de sessões no pool na inicialização.
4. Defina o número máximo de sessões no pool.
5. Clique em Salvar.
6. Reinicie o servidor de aplicativos.

   O Pool de sessão é ativada pelas configurações definidas.

Ativar sincronização de senhas

O Servidor de provisionamento permite a sincronização de senhas entre usuários do CA Identity Manager e as contas de usuário do terminal associadas. Em outras palavras, quando um usuário que tem funções de provisionamento é criado ou modificado no CA Identity Manager, o usuário do provisionamento é definido para permitir alterações de senha nas contas de terminal.

Observação: ao ativar esse recurso no Management Console, *todos* os usuários no ambiente são definidos para permitir alterações de senha nas contas de terminal.

Siga estas etapas:

1. No Management Console, escolha Advanced Settings, Provisioning.
2. Marque Enable Password Changes from Endpoint Accounts.
3. Clique em Salvar.
4. Reinicie o servidor de aplicativos.

Mapeamentos de atributo

Os mapeamentos de atributo associam os atributos de usuário em tarefas administrativas relacionadas ao provisionamento, como Provision Create User, aos atributos correspondentes no Servidor de provisionamento. Um único atributo de provisionamento pode ser mapeados para vários atributos no repositório de usuários do CA Identity Manager.

Os mapeamentos padrão para os atributos estão nas tarefas padrão, que são listadas na seção Mapeamentos de entrada. Se você modificar uma dessas tarefas administrativas de maneira a usar atributos diferentes, atualize os mapeamentos de atributo conforme a necessidade.

Mapeamentos de entrada

Os mapeamentos de entrada são eventos de mapa gerados pelo Servidor de provisionamento para uma tarefa administrativa. Esses mapeamentos são predefinidos e não podem ser modificados.

Mapeamentos de saída

Os mapeamentos de saída associam eventos, que são gerados por tarefas administrativas, a eventos que são aplicados ao Diretório de provisionamento. Os mapeamentos padrão existem para os eventos que afetam os atributos de usuário.

Console de usuário

Você acessa um ambiente do CA Identity Manager usando o Console de usuário, um aplicativo web que permite que usuários executar tarefas administrativas. Você define determinadas propriedades do Console de usuário que os administradores usam para acessar um Ambiente na página Console de usuário no Management Console.

A página Console de usuário inclui os seguintes campos:

Propriedades gerais

Defina propriedades que se aplicam a um ambiente.

Show Recently Completed Tasks

Determina se o CA Identity Manager exibe uma mensagem de status quando uma tarefa é concluída.

Quando essa opção é selecionada, os usuários devem clicar em OK para limpar a mensagem de status que o CA Identity Manager exibe.

Para desativar a mensagem e impedir que os usuários tenham que clicar em OK quando cada mensagem de status é exibida, desmarque essa opção.

Show About Link

Determina se um link Sobre aparecerá no canto inferior direito do Console de usuário. Quando essa opção é selecionada, os usuários do CA Identity Manager podem clicar no link Sobre para exibir as informações de versão dos componentes do CA Identity Manager.

Enable Language Switching

Determina se o CA Identity Manager incluirá uma lista suspensa Escolher o idioma na tela de logon e no Console de usuário. Quando esse campo é selecionado, os usuários do CA Identity Manager podem alterar o idioma no Console de usuário selecionando um novo idioma na lista.

Observação: para exibir o campo Escolher o idioma, verifique se você selecionou o campo Enable Language Switching *e* configure o CA Identity Manager para oferecer suporte a vários idiomas.

Consulte o *Guia de Design do Console de Usuário* para obter mais informações.

Job Timeout

Determina a quantidade de tempo que o CA Identity Manager aguardará depois que uma tarefa é enviada para exibir uma mensagem de status.

Quando a tarefa é concluída dentro do período de tempo especificado, o CA Identity Manager exibe a seguinte mensagem:

"Tarefa concluída"

Se a tarefa levar mais tempo para ser concluída ou estiver sob controle do fluxo de trabalho, CA Identity Manager exibirá a seguinte mensagem:

"A tarefa foi enviada para processamento na *data atual*"

Observação: as alterações talvez não tenham efeito imediatamente.

Theme Properties

Permite que você personalize o ícone e o título do Console de usuário em um Ambiente. Por exemplo, você pode adicionar o logotipo da empresa e o nome da empresa às telas do Console de usuário.

As propriedades do tema incluem as seguintes configurações:

Icon (URI)

Define o ícone usando um URI para uma imagem disponível ao servidor de aplicativos.

Exemplo: http://myserver.mycompany.com/images/front/logo.gif

Icon Link (URI)

Define o link de navegação para a imagem usando um URI.

Icon Title

Define a dica de ferramenta que aparece como um texto ao passar o mouse no ícone.

Cargo

Especifica o texto personalizado, que é exibido ao lado do ícone na parte superior do Console de usuário.

Observação: se você tiver definido uma capa personalizada, é possível especificar um ícone ou título que faça referência a um arquivo de propriedades da capa. Por exemplo, se a entrada da imagem do ícone no arquivo de propriedades de uma capa personalizada for imagem/logo.gif, você poderá inserir essa mesma sequência de caracteres no campo Ícone.

Login Properties

Especifique o método de autenticação e o local da página de logon para a qual os usuários serão direcionados quando acessarem um Ambiente.

Authentication Provider module class name

Especifica o nome da classe do módulo do provedor de autenticação.

Página de logon

Especifica a página a qual os usuários são direcionados ao acessar um Ambiente.

Serviços web

O TEWS (TaskExecution Web Service - serviço web de execução de tarefa) do CA Identity Manager permite que aplicativos cliente de terceiros enviem tarefas do CA Identity Manager ao CA Identity Manager para execução remota.

A tela Propriedades de serviços web permite configurar o TEWS para um ambiente. Nessa tela, é possível executar as seguintes tarefas:

- Ativar o TEWS para um ambiente do CA Identity Manager.
- Gerar documentos WSDL (Web Services Definition Language - idioma de definição dos serviços web) específicos de tarefa.
- Permitir a personificação.
- Especificar que a senha do administrador é obrigatório para autenticação.
- Configurar a autenticação do SiteMinder.
- Configurar o SiteMinder para proteger o URL de serviços web, se o CA Identity Manager integrar-se ao SiteMinder
- Especificar a autenticação de token do Nome de usuário de serviços de segurança na web.
- Especificar pelo menos um dos três possíveis tipos de autenticação.

Para obter informações sobre como emitir solicitações remotas para o CA Identity Manager por meio do TEWS, consulte o *Guia de Programação do Java*.

Propriedades do fluxo de trabalho

Se ativadas, o recurso de fluxo de trabalho controlará a execução de uma tarefa do CA Identity Manager que está associada a um processo de fluxo de trabalho.

Um processo de fluxo de trabalho é um conjunto de etapas a serem executadas para atingir um objetivo de negócios, como a criação de uma conta de usuário. Geralmente, uma dessas etapas envolve aprovação ou rejeição de tarefas.

Uma tarefa administrativa é associada a um ou mais eventos, que podem disparar um ou mais processos de fluxo de trabalho. Depois que os processos de fluxo de trabalho são concluídos, o CA Identity Manager executa ou rejeita a tarefa com base nos resultados dos processos de fluxo de trabalho.

A ilustração a seguir mostra a relação entre a tarefa do CA Identity Manager, um evento associado e um processo de fluxo de trabalho:

Propriedades do fluxo de trabalho

Use a caixa de seleção para ativar ou desativar o fluxo de trabalho para o Ambiente do CA Identity Manager.

Delegação do item de trabalho

Se ativada, a delegação do item de trabalho permite que um participante (o delegante) especifique que outro usuário (o representante) obtenha permissões para aprovar tarefas na lista de tarefas do delegante. Um participante pode atribuir itens de trabalho a outro aprovador durante os períodos em que o delegante "estiver fora do escritório". Os delegantes retêm acesso completo aos seus itens de trabalho durante o período de delegação.

A delegação usa o seguinte atributo conhecido:

%DELEGATORS%

Esse atributo conhecido armazena os nomes de usuários que estão sendo delegados ao usuário com o atributo, assim como o horário em que a delegação foi criada.

Observação: para obter mais informações sobre delegação de item de trabalho, consulte o *Guia de Administração*.

Resolvedores participantes do fluxo de trabalho

As atividades de um processo de fluxo de trabalho, como aprovar ou rejeitar uma tarefa, são executadas pelos *participantes*.

Use a tela Resolvedores participantes do fluxo de trabalho para mapear um resolvedor participante personalizado para uma classe Java do resolvedor participante totalmente qualificado.

Um *resolvedor participante* personalizado é um objeto Java que determina os participantes da atividade de um fluxo de trabalho e retorna uma lista ao CA Identity Manager. O CA Identity Manager passa a lista para o mecanismo de fluxo de trabalho.

Normalmente, você cria um resolvedor participante personalizado somente se nenhum resolvedor participante padrão puder fornecer a lista de participantes que uma atividade exige.

Observação: para obter informações sobre como desenvolver resolvedores participantes personalizados, consulte o *Guia de Programação do Java*. Para obter informações sobre os resolvedores participantes padrão, consulte o *Guia de Administração*.

Importar/exportar configurações personalizadas

Na tela Advanced Settings do Management Console, você pode aplicar as configurações avançadas a vários ambientes, como se segue:

- Defina as configurações avançadas em um ambiente.
- Exporte as configurações avançadas para um arquivo XML.
- Importe o arquivo XML para os ambientes necessários.

Erros de memória insuficiente da máquina virtual Java

Sintoma:

Recebo erros de memória insuficiente da JVM durante períodos de carga alta ou de tensão que afetam a funcionalidade do Servidor do CA Identity Manager.

Solução:

Aconselhamos a configuração das opções de depuração da JVM para que você seja alertado sobre condições de memória insuficiente.

Observação: para obter mais informações sobre como configurar as opções de depuração da JVM, consulte Debugging Options em Java HotSpot VM Options, no site http://www.oracle.com.

Capítulo 8: Auditoria

Esta seção contém os seguintes tópicos:

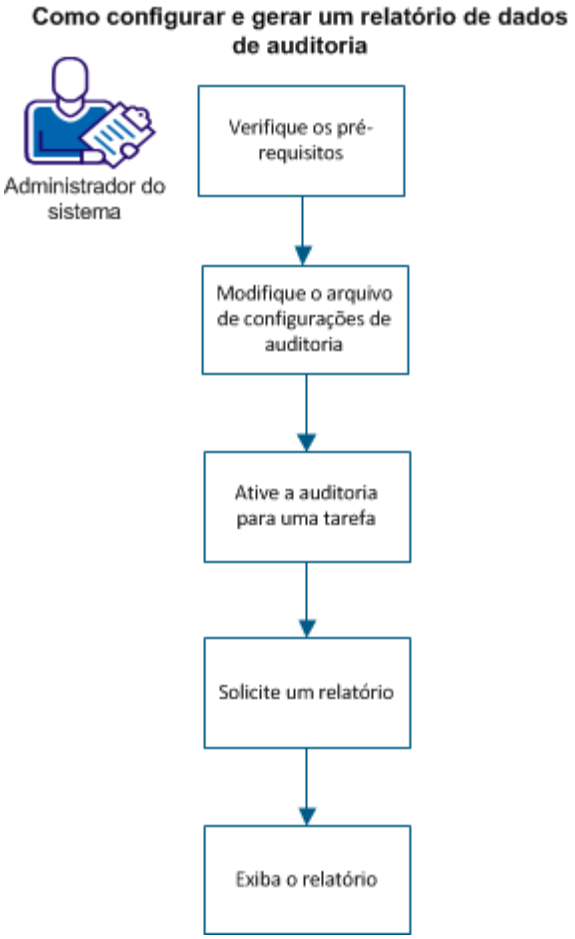
Como configurar e gerar relatórios de dados de auditoria

Os dados de auditoria fornecem um registro histórico de operações que ocorrem em um ambiente. Ao configurar e ativar a auditoria, o sistema registra informações sobre as tarefas em um banco de dados de auditoria. As informações de auditoria podem ser usadas para gerar relatórios. Alguns exemplos de dados de auditoria incluem os seguintes pontos:

- Atividade do sistema por um período específico de tempo.
- Eventos de logon e logoff do usuário ao acessar um ambiente específico.
- As tarefas que um usuário específico executa
- Uma lista de objetos que foram modificados durante um período específico.
- As funções atribuídas ao usuário
- As operações que foram executadas para uma determinada conta de usuário.

Os dados de auditoria são gerados para *eventos* do CA Identity Manager. Um evento é uma operação gerada por uma tarefa do CA Identity Manager. Por exemplo, a tarefa Criar usuário pode incluir um evento AssignAccessRoleEvent.

O diagrama a seguir descreve como um administrador do sistema configura a auditoria e gera um relatório sobre dados de auditoria:



Como um administrador, execute as seguintes etapas:

1. Verificar os pré-requisitos (na página 249)
2. Modificar um arquivo de configurações de auditoria (na página 249)
3. Ativar a auditoria para uma tarefa (na página 254)
4. Solicitar um relatório (na página 255)
5. Exibir o relatório (na página 257)

Verificar os pré-requisitos

Verifique se os seguintes pré-requisitos foram atendidos antes de definir as configurações de auditoria:

- Uma instância de banco de dados separada é criada para armazenar dados que estão relacionados à auditoria. Por padrão, o arquivo de esquema de banco de dados do CA Identity Manager está no seguinte local:
  - **Windows**: C:\Arquivos de programas\CA\Identity Manager\IAM Suite\Identity Manager\Identity Manager\ferramentas\banco de dados
- Configure a conexão do servidor de relatórios para solicitar e exibir o relatório de auditoria.
- Adicione um objeto de conexão para o relatório de auditoria. Execute as seguintes etapas:
  a. Efetue logon no console de usuário com privilégios administrativos.
  b. Vá para Funções e tarefas, Tarefas administrativas e pesquise um relatório de auditoria a ser modificado.
  c. Digite o seguinte nome de conexão no campo Objeto de conexão para o relatório:
  `rptParamConn`

Modificar um arquivo de configurações de auditoria

Defina as configurações de auditoria no arquivo de configurações de auditoria para definir o tipo de informação que o CA Identity Manager deverá auditar. É possível configurar um arquivo de configurações de auditoria para executar as seguintes tarefas:

- Auditar alguns ou todos os eventos gerados de tarefas administrativas.
- Registrar informações sobre eventos em determinados estados, por exemplo, quando um evento é concluído ou cancelado.
- Registrar informações sobre os atributos que estão envolvidos em um evento. Por exemplo, você pode registrar em log os atributos que mudam durante um evento ModifyUserEvent.

- Definir o nível de auditoria do log de atributos.

O arquivo de configurações de auditoria é um arquivo XML criado pela exportação de configurações de auditoria. O arquivo tem o seguinte esquema:

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

Para obter mais informações sobre o esquema e elementos de auditoria, consulte os comentários no arquivo de configurações de auditoria.

Os elementos AuditProfileAttribute indicam os atributos que o CA Identity Manager audita. Os atributos se aplicam ao objeto especificado no elemento AuditProfile.

Observação: se não houver atributos de perfil de auditoria especificados, todos os atributos do objeto que estiverem especificados no elemento AuditProfile serão registrados.

A tabela a seguir mostra os atributos válidos para os tipos de objeto do CA Identity Manager:

Atributos válidos para tipos de objeto do CA Identity Manager

Tipo de objeto	Atributos válidos
ACCESS ROLE	■ name — nome da função visível ao usuário ■ description — um comentário opcional sobre a finalidade da função. ■ members — os usuários que podem usar a função. ■ administrators — os usuários que podem atribuir integrante da função ou administradores. ■ owners — os usuários que podem modificar a função. ■ enabled — indica se a função está ativada ou não. ■ assignable — indica se a função pode ser atribuída por um administrador ou não. ■ tasks — as tarefas de acesso que estão associadas à função.

Atributos válidos para tipos de objeto do CA Identity Manager	
Tipo de objeto	**Atributos válidos**
ACCESS TASK	■ name — nome da tarefa visível ao usuário ■ description — um comentário opcional sobre a finalidade da tarefa ■ application — o aplicativo que é associado à tarefa. ■ tag — o identificador exclusivo da tarefa ■ reserved1, reserved2, reserved3, reserved4 — os valores dos campos reservados para a tarefa
ADMINISTRATIVE ROLE	■ name — nome da função visível ao usuário ■ description — um comentário opcional sobre a finalidade da função ■ members — os usuários que podem usar a função. ■ administrators — os usuários que podem atribuir integrante da função ou administradores. ■ owners — os usuários que podem modificar a função. ■ enabled — indica se a função está ativada ou não. ■ assignable — indica se a função pode ser atribuída por um administrador ou não. ■ tasks — as tarefas que estão associadas à função.

Atributos válidos para tipos de objeto do CA Identity Manager

Tipo de objeto	Atributos válidos
ADMINISTRATIVE TASK	■ name — nome da tarefa visível ao usuário ■ description — um comentário opcional sobre a finalidade da tarefa ■ tag — o identificador exclusivo da tarefa ■ category — a categoria na interface de usuário do CA Identity Manager em que a tarefa é exibida ■ primary_object — o objeto em que a tarefa opera ■ action — a operação que é executada no objeto. ■ hidden — indica se a tarefa *não* aparecerá nos menus. ■ public — indica se a tarefa estará disponível aos usuários que não efetuaram logon no CA Identity Manager. ■ auditing — indica se a tarefa permite o registro das informações de auditoria. ■ external — indica se a tarefa é uma tarefa externa. ■ url — o URL para onde o CA Identity Manager redireciona o usuário quando uma tarefa externa é executada. ■ workflow — indica se os eventos do CA Identity Manager associados à tarefa disparam o fluxo de trabalho ■ webservice — indica se a tarefa é uma para a qual a saída WSDL pode ser gerada do Management Console do CA Identity Manager.
GROUP	Qualquer atributo válido que seja definido para o objeto GROUP no arquivo de configuração de diretório (directory.xml).
ORGANIZATION	Qualquer atributo válido que seja definido para o objeto Organization no arquivo de configuração de diretório (directory.xml).
PARENTORG	

Atributos válidos para tipos de objeto do CA Identity Manager	
Tipo de objeto	**Atributos válidos**
RELATIONSHIP	■ %CONTAINER% — identificador exclusivo do objeto pai. Por exemplo, se o objeto RELATIONSHIP descrever a associação à função, o recipiente será a função. ■ %CONTAINER_NAME% — nome do grupo pai visível ao usuário ■ %ITEM% — identificador exclusivo do objeto contido no objeto pai. Por exemplo, se o objeto RELATIONSHIP descrever a associação à função, os itens serão os integrantes da função. ■ %ITEM_NAME% — nome do grupo aninhado visível ao usuário
USER	Qualquer atributo válido que seja definido para o objeto USER no arquivo de configuração de diretório (directory.xml).
NENHUM	Nenhum atributo

Observação: os pontos a seguir se aplicam à tabela anterior:

- Ativado, atribuível, auditável, fluxo de trabalho, oculto, serviço web e público são registrados como true ou false.
- Ao auditar tarefas para funções, o nome visível ao usuário é registrado.
- O banco de dados armazena políticas de integrante, administrador e proprietário no formato XML compilado. Esse formato é diferente da interface de usuário em que cada política é exibida como uma expressão.

Siga estas etapas:

1. Efetue logon no console de gerenciamento, selecione o ambiente, Configurações avançadas e clique em Auditoria.
2. Clique em Exportar.

   O sistema exporta as configurações de auditoria atuais para um arquivo XML de configurações de auditoria.

3. Modifique as configurações de auditoria no arquivo XML exportado na etapa anterior. Execute as tarefas a seguir:
   a. Defina o valor de Audit enabled ="true" e forneça o valor de Nome do JNDI de "iam_im_<auditdb>.xml" para o elemento de origem de dados.
   b. Especifique o seguinte nome JDNI:
      `java:/auditDbDataSource`

      Observação: a origem de dados está no seguinte local:
      `iam/im/jdbc/auditDbDataSource`
   c. Adicione, modifique ou exclua elementos no arquivo.
   d. Modifique o nível de informações que são registradas para cada evento.
4. Repita as etapas 1 e 2. Clique em Importar e faça upload do arquivo XML de configurações de auditoria modificado.
5. Reinicie o ambiente.

O arquivo de configurações de auditoria agora está atualizado.

Ativar a auditoria para uma tarefa

Ative a auditoria das tarefas para as quais você configurou a auditoria no arquivo de configurações de auditoria.

Siga estas etapas:

1. Efetue logon no console de usuário com privilégios de administrador do sistema.
2. Crie ou modifique a tarefa para a qual você deseja ativar a auditoria.
3. Na guia Perfil, certifique-se de que a caixa de seleção Ativar a auditoria está marcada.
4. Clique em Submit.

A auditoria agora está ativada para a tarefa.

Solicitar um relatório

Para exibir o relatório, solicite um relatório de um usuário com privilégios de administração de relatórios. Selecione o relatório apropriado que rastreia os dados de auditoria. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Antes de programar um relatório, execute as etapas seguintes:

1. Efetue logon no console de usuário com privilégios administrativos.
2. Vá para Funções e tarefas, Modificar tarefa administrativa e selecione um relatório de auditoria a ser modificado.
3. Selecione a guia Guias e clique em IAM ReportServerScheduler para editar.
4. Marque a caixa de seleção Ativar opção de recorrência.
5. Clique em OK e em Enviar.

Siga estas etapas:

1. Efetue logon no console de usuário com privilégios de usuário de tarefas de geração de relatório.
2. Selecione Relatórios, Tarefas de geração de relatórios, Solicitar um relatório.

   Uma lista de relatórios será exibida.
3. Selecione um relatório com base em auditoria.

   Uma tela de parâmetros é exibida.
4. Clique em Programar relatório e selecione uma programação para o relatório.

   Agora

   Especifica que o relatório é executado imediatamente.

   Uma vez

   Especifica que o relatório é executado uma vez, durante um período específico. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

   (Apenas relatório de auditoria) Por hora

   Especifica que o relatório é gerado na hora de início e, em seguida, a cada 'n' horas; 'n' denota o intervalo entre relatórios sucessivos. Selecione a data de início, a data de término, a hora de início, a hora de término e o intervalo entre os relatórios sucessivos.

   (Apenas relatório de auditoria) Diariamente

   Especifica que o relatório é gerado na hora de início e, em seguida, a cada 'n' dias; 'n' denota o intervalo entre relatórios sucessivos. Selecione a data de início, a data de término, a hora de início, a hora de término e o intervalo entre os relatórios sucessivos.

(Apenas relatório de auditoria) Semanalmente

Especifica que o relatório é gerado a cada semana no dia selecionado a partir da data de início. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

(Apenas relatório de auditoria) Mensal

Especifica que o relatório é gerado mensalmente a partir da data de início e, em seguida, a cada 'n' meses. 'n' denota o intervalo entre os relatórios sucessivos. Selecione a data de início, a data de término, a hora de início, a hora de término e o intervalo entre os relatórios sucessivos.

(Apenas relatório de auditoria) Execute o relatório no Xº dia do mês

Especifica que o relatório é gerado no dia específico do mês mencionado. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

(Apenas relatório de auditoria) Primeira segunda-feira

Especifica que o relatório é gerado sempre na primeira segunda-feira do mês. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

(Apenas relatório de auditoria) Último dia do mês

Especifica que o relatório é gerado no último dia do mês. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório.

(Apenas relatório de auditoria) No Xº dia da semana X de cada mês

Especifica que o relatório é gerado em um determinado dia de uma determinada semana de cada mês. Selecione a data de início, a data de término, a hora de início e a hora de término quando desejar gerar o relatório. Por exemplo, é possível gerar um relatório em uma sexta-feira na terceira semana de cada mês.

5. Clique em Submit.

A solicitação de relatório é enviada. Dependendo da configuração do ambiente, a solicitação será executada imediatamente, ou após a aprovação de um administrador.

Normalmente, um administrador do sistema ou outro usuário com privilégios de administração de relatório deve aprovar uma solicitação de relatório antes que ela seja executada pelo sistema. A aprovação é obrigatória, pois alguns relatórios podem exigir muito tempo ou recursos significativos do sistema para que sejam executados. Se a solicitação de relatório exigir uma aprovação, o sistema enviará um alerta de email.

Observação: ative o fluxo de trabalho para o ambiente, se a aprovação for necessária.

Exibir o relatório

Dependendo da configuração do ambiente, um relatório ficará disponível para exibição quando um administrador aprovar a solicitação para aquele relatório. Se a solicitação de relatório tiver uma aprovação pendente, o sistema enviará um alerta de email. O relatório que você deseja exibir não aparecerá na lista de pesquisa até que seja aprovado.

Observação: para exibir relatórios no CA Identity Manager usando a tarefa Exibir meus relatórios, ative os cookies de sessão de terceiros no navegador.

Siga estas etapas:

1. No console de usuário, vá para Relatórios, Tarefas de geração de relatórios, e clique em Exibir meus relatórios.
2. Procure o relatório gerado que deseja exibir.

   As instâncias de relatórios de recorrência gerados e de relatórios sob demanda são exibidas.

   Observação: se o status do relatório for Pendente/recorrente, o relatório não será gerado e poderá levar algum tempo para ser concluído.
3. Selecione o relatório que deseja exibir.
4. (Opcional) Clique em Exportar esse relatório (canto superior esquerdo) para exportar o relatório para os seguintes formatos:
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) – somente dados
   - Microsoft Excel (97-2003) – editável
   - RTF (Rich Text Format – Formato Rich Text)
   - CSV (Comma Separated Values – Valores Separados por Vírgulas)
   - XML

Limpar o banco de dados de auditoria

Com o tempo, o banco de dados de auditoria pode acumular registros que não são mais necessários. Para remover esses registros, execute o seguinte procedimento de banco de dados no diretório db\auditing:

`garbageCollectAuditing12` *environment-ID MM/DD/YYYY*

environment-ID

Define a ID do ambiente do CA Identity Manager

MM/DD/AAAA

Define a data antes da qual os registros de auditoria devem ser removidos.

Capítulo 9: Ambientes de produção

Esta seção fornece descrições funcionais passo a passo para migrar partes específicas da funcionalidade. Certifique-se de que ela seja usada somente quando alterações limitadas forem feitas no ambiente de desenvolvimento e que essas alterações sejam totalmente entendidas.

Esta seção contém os seguintes tópicos:

Para migrar definições de tarefas e funções administrativas

É possível personalizar as funções e tarefas do CA Identity Manager para atender às necessidades específicas da sua empresa. A personalização envolve a criação ou modificação de funções e tarefas administrativas, ou o uso de uma tarefa Criar ou Modificar para uma função ou tarefa administrativa.

Um método alternativo, embora *não seja recomendado*, é modificar funções e tarefas no arquivo roledefinition.xml. Use esse método para alterações muito limitadas devido ao risco de erros na edição.

Esse processo migrará apenas definições de tarefa e função administrativas. Se as funções foram associadas às organizações, pense na possibilidade de migrar todo o ambiente do CA Identity Manager.

Importante: se você alterou as definições de tarefa ou função no ambiente de produção, essas alterações serão perdidas quando você importar as definições de tarefa ou função de um ambiente de desenvolvimento. A importação de definições de tarefa e função substitui as definições de tarefa e função existentes com os mesmos nomes.

Para exportar definições de tarefa e função administrativas

Se as alterações foram realizadas diretamente no arquivo roledefinition.xml, esse arquivo poderá ser diretamente importado no ambiente de produção. Caso contrário, para exportar as definições de tarefa e função:

1. Se você possuir um cluster de Servidores de políticas, verifique se apenas um Servidor de políticas está em execução.
2. Pare todos, exceto um nó do CA Identity Manager.
3. Efetue logon no Management Console.
4. Clique nos ambientes do CA Identity Manager.
5. Selecione o ambiente do CA Identity Manager, do qual deseja exportar as definições de tarefa e função.
6. Clique em Roles, em Export e forneça um nome para o arquivo.
7. Siga as instruções no próximo procedimento para importar esse arquivo.

Para importar definições de tarefa e função administrativas

Siga estas etapas:

1. Copie o arquivo criado no procedimento anterior no ambiente de produção.
2. Efetue logon no Management Console no ambiente de produção.
3. Clique nos ambientes do CA Identity Manager.
4. Selecione o ambiente do CA Identity Manager apropriado.
5. Clique em Roles.
6. Clique em Import e especifique o nome do arquivo XML gerado pela exportação.
7. Se essas etapas forem bem-sucedidas, inicie todos os Servidores de políticas extras e os nós do CA Identity Manager que foram interrompidos.

   Observação: se ainda houver qualquer alteração a ser feita em um ambiente do CA Identity Manager, repita a etapa 6.

Para verificar a importação de tarefas e funções

Para verificar se as funções e tarefas foram importadas com êxito, efetue logon no CA Identity Manager como uma conta de administrador que pode usar as seguintes tarefas:

- Modificar função administrativa
- Modificar tarefa administrativa

Execute essas tarefas e verifique se as funções e tarefas refletem as definições de função recentemente importadas.

Para migrar capas do CA Identity Manager

As capas do CA Identity Manager podem ser personalizadas para fornecer uma aparência específica ao aplicativo. Se você tiver modificado ou criado novas capas para um conjunto de usuários, use as seguintes etapas para migrar capas do ambiente de desenvolvimento para o de produção.

Se estiver modificando uma capa, copie os arquivos modificados.

Siga estas etapas:

1. Copie arquivos novos e modificados do servidor de desenvolvimento para o de produção, como arquivos de imagem, folhas de estilo, arquivos de propriedades e a página do console (index.jsp).
2. Se vários capas estiverem sendo usados, configure a resposta do SiteMinder.

   Observação: para obter mais informações sobre como usar várias capas, consulte o *Guia de Configuração*.

Para verificar a migração de capas, efetue logon no Console de usuário e verifique se a capa é exibida corretamente.

Atualizar o CA Identity Manager em um ambiente de produção

Depois de migrar o CA Identity Manager do desenvolvimento para a produção, talvez seja preciso executar atualizações incrementais. Para migrar nova funcionalidade do CA Identity Manager do ambiente de desenvolvimento para o ambiente de produção, execute as etapas a seguir:

1. Migre ambientes do CA Identity Manager.
2. Copie o iam_im.ear.
3. Migre definições do processo de fluxo de trabalho.

Para migrar um ambiente do CA Identity Manager

Um Ambiente do CA Identity Manager é criado no Management Console. O ambiente do CA Identity Manager inclui um conjunto de definições de tarefa e função, definições de fluxo de trabalho, recursos personalizados que são criados com as APIs do CA Identity Manager e um Diretório do CA Identity Manager.

Siga estas etapas:

1. Se o CA Identity Manager integrar-se ao SiteMinder e você tiver um cluster de Servidores de políticas, verifique se apenas uma Política está em execução.
2. Pare todos, exceto um nó do CA Identity Manager.
3. Exporte os Ambientes do CA Identity Manager no Management Console no ambiente de desenvolvimento.
4. Importe os ambientes exportados no Management Console no ambiente de produção.
5. Se o CA Identity Manager integrar-se ao SiteMinder, proteja novamente os realms do CA Identity Manager na Interface de usuário do servidor de políticas.

   O domínio da política não é exportado do repositório de políticas quando você exporta um Ambiente do CA Identity Manager.
6. Reinicie o Servidor de política e os nós do CA Identity Manager que foram interrompidos.

Ao migrar um Ambiente do CA Identity Manager, as seguintes atividades ocorrem:

- Se o mesmo objeto existir nos dois locais, as alterações feitas no servidor de desenvolvimento substituirão as alterações no servidor de produção.
- Se novos objetos forem criados no ambiente de desenvolvimento, eles são adicionados ao servidor de produção.
- Se novos objetos forem criados no servidor de produção, eles são mantidos.

Para exportar um ambiente do CA Identity Manager

Para implantar um ambiente do CA Identity Manager em um sistema de produção, exporte o ambiente de um sistema de desenvolvimento ou armazenamento temporário e importe-o no sistema de produção.

Observação: ao importar um ambiente anteriormente exportado, o CA Identity Manager exibe um log em uma janela de status no Management Console. Para ver as informações de validação e implantação para cada objeto gerenciado e seus atributos nesse log, selecione o campo Enable Verbose Log Output na página Environment Properties *antes* de exportar o ambiente. Certifique-se de que selecionar o campo Enable Verbose Log Output possa causar problemas de desempenho significativos durante a importação.

Siga estas etapas:

1. Clique em Environments no Management Console.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.

2. Selecione o ambiente que deseja exportar.
3. Clique no botão Export.

   A tela Download de arquivos é exibida.

4. Salve o arquivo ZIP em um local que possa ser acessado pelo sistema de produção.
5. Clique em Finalizar.

   As informações do ambiente são exportadas para um arquivo ZIP que você pode importar em outro ambiente.

Para importar um ambiente do CA Identity Manager

Após a exportação de um ambiente do CA Identity Manager de um sistema de desenvolvimento, você poderá importá-lo em um sistema de produção.

Siga estas etapas:

1. Clique em Environments no Management Console.

   A tela de ambientes do CA Identity Manager aparece com uma lista de ambientes do CA Identity Manager.

2. Clique no botão Import.

   A tela Import Environment é exibida.

3. Procure o arquivo ZIP exigido para importar um ambiente.
4. Clique em Finalizar.

O ambiente é importado no CA Identity Manager.

Para verificar a migração do ambiente do CA Identity Manager

Para verificar a migração adequada do ambiente do CA Identity Manager, confirme se o Ambiente do CA Identity Manager é exibido na Interface de usuário do servidor de políticas para o Servidor de políticas no ambiente de produção.

No Interface de usuário do servidor de políticas, verifique os seguintes pontos:

- Se as configurações do diretório de usuários do CA Identity Manager são precisas.
- Se o novo domínio do CA Identity Manager existe
- Se os esquemas de autenticação corretos protegem os realms do CA Identity Manager.

Além disso, ao efetuar logon no Management Console, verifique se o Ambiente do CA Identity Manager é exibido quando você seleciona os Ambientes.

Migrar o iam_im.ear para o JBoss

Reimplante o iam_im.ear toda vez que a funcionalidade for migrada do ambiente de desenvolvimento para o ambiente de produção. Ao migrar todo o EAR, certifique-se de que o ambiente de produção seja idêntico ao ambiente de desenvolvimento.

Siga estas etapas:

1. Copie o iam_im.ear do ambiente de desenvolvimento em um local acessível para o ambiente de produção.
2. Na cópia do iam_im.ear, edite as informações da conexão com o Servidor de políticas, de modo a refletir o ambiente de produção.

   Para fazer essa alteração, copie o *base_do_jboss*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml de seu ambiente de produção no iam_im.ear.

3. Substitua o iam_im.ear instalado pela cópia do iam_im.ear de seu ambiente de desenvolvimento na Etapa como se segue:
   a. No servidor de produção, exclua o iam_im.ear:

      base_do_jboss_do_nó_do_cluster\server\default\deploy\iam_im.ear

   b. Substitua os arquivos excluídos pela cópia editada do iam_im.ear do ambiente de desenvolvimento.
4. Repita essas etapas para cada nó no cluster.

Migrar o iam_im.ear para o WebLogic

Reimplante o iam_im.ear toda vez que a funcionalidade for migrada do ambiente de desenvolvimento para o ambiente de produção. Ao migrar todo o EAR, certifique-se de que o ambiente de produção seja idêntico ao ambiente de desenvolvimento.

Siga estas etapas:

1. Preserve as informações da conexão com o Servidor de políticas.

   As informações de conexão com o Servidor de políticas são armazenadas no arquivo ra.xml no diretório policyserver_rar/WEB-INF. Copie esse arquivo em outro local para que ele possa ser substituído no iam_im.ear antes de reimplantá-lo.
2. Copie o iam_im.ear em um local disponível no Servidor de administração do WebLogic.
3. Substitua as informações da conexão com o Servidor de políticas.

   No iam_im.ear, substitua o arquivo policyserver_rar/WEB-INF/ra.xml pelo arquivo preservado na Etapa 1.
4. Reimplante o iam_im.ear
   a. Efetue logon no console do WebLogic.
   b. Vá para Implantações, Aplicativo, Identity Manager.

Na guia Deploy, selecione Deploy (Re-Deploy) Application.

Migrar o iam_im.ear para o WebSphere

Siga estas etapas:

1. Copie o script *imsInstall.jacl* de *dir_ferramentas_im_was**ferramentas-WebSphere* no diretório *dir_gerencidor_implantação**bin* em que:
   - *dir_ferramentas_im_was* é o diretório no sistema de desenvolvimento em que as Ferramentas do CA Identity Manager para o WebSphere estão instaladas.
   - *dir_gerenciador_implantação* é o local em que o Gerenciador de implantação está instalado.
2. No sistema de desenvolvimento onde você configurou o aplicativo CA Identity Manager, copie *dir_ferramentas_im_was**ferramentas-WebSphere**imsExport.bat* ou *imsExport.sh* em *base_do_was**bin.*
3. Na linha de comando, navegue para *base_do_was**bin*.
4. Certifique-se de que o servidor de aplicativos do WebSphere esteja em execução.
5. Exporte o aplicativo CA Identity Manager implantado da seguinte forma:

   Para Windows, insira este comando:

   `imsExport.bat "caminho-para-ear-exportado"`

   onde *caminho-para-ear-exportado* é o caminho completo e o nome do arquivo criados pelo utilitário imsExport.

   Nos sistemas Windows, use as barras diagonais (/) em vez de barras invertidas (\) ao especificar o caminho para was_im.ear. Por exemplo:

   ```
   imsExport.bat "c:/programas de arquivos/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   Para UNIX, insira este comando:

   `./wsadmin -f imsExport.jacl -conntype RMI -port 2809 caminho para o ear exportado`

   onde *caminho-para-ear-exportado* é o caminho completo, incluindo o nome do arquivo EAR exportado.
6. Copie o arquivo EAR exportado do local no sistema de desenvolvimento onde você o exportou para um local no sistema onde o Gerenciador de implantação está instalado.
7. Substitua *dir_ferramentas_im_was*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml pelo correspondente do ambiente de produção.

   O arquivo ra.xml contém as informações de conexão com o Servidor de políticas.

8. No sistema onde o Gerenciador de implantação está instalado, implante o Identity Manager EAR:

   a. Na linha de comando, navegue para:

      dir_gerenciador_de_implantação\bin.

   b. Certifique-se de que o servidor de aplicativos do WebSphere esteja em execução.

   c. Execute o script imsInstall.jacl como se segue:

   Observação: o script imsInstall.jacl pode levar alguns minutos para ser executado.

   Windows:

      wsadmin -f imsInstall.jacl *"caminho-para-ear-copiado" nome_do_cluster*

      onde *caminho-para-ear-copiado* é o caminho completo, incluindo o nome de arquivo do Identity Manager EAR que você copiou no sistema do Gerenciador de implantação.

      Por exemplo:

      wsadmin -f imsInstall.jacl "c:\Arquivos de Programa\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

   UNIX:

      ./wsadmin -f imsInstall.jacl *caminho-para-ear-copiado nome_do_cluster*

      onde *caminho-para-ear-copiado* é o caminho completo, incluindo o nome de arquivo do Identity Manager EAR que você copiou no sistema do Gerenciador de implantação.

      Por exemplo:

      ./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. Se o CA Identity Manager integrar-se ao SiteMinder, verifique os seguintes pontos:

   - Se os agentes do SiteMinder podem se conectar com seu repositório de políticas.
   - Se o Servidor de políticas pode se conectar com o repositório de usuários.
   - Se os domínios do CA Identity Manager foram criados.

Migrar definições do processo de fluxo de trabalho

Se você usou o fluxo de trabalho no ambiente de desenvolvimento, exporte as definições do fluxo de trabalho e importe-as no ambiente de produção. Em seguida, configure o fluxo de trabalho em cada um dos nós do servidor.

Exportar definições do processo

No sistema do ambiente de desenvolvimento, é possível exportar as definições do processo de fluxo de trabalho.

Siga estas etapas:

1. Certifique-se de que o servidor de aplicativos esteja em execução.
2. Vá para *ferramentas_administrativas*\Workpoint\bin\ e execute Archive.bat (para Windows) ou Archive.sh (para UNIX) da seguinte forma:
   a. Na caixa de diálogo Importar, selecione o objeto raiz.
   b. Clique em Adicionar.
   c. Especifique o nome do arquivo a ser gerado.
   d. Clique em Exportar.
   e. Clique em Ir.

   ferramentas_administrativas se refere às Ferramentas administrativas que são instaladas por padrão em um dos seguintes locais:
   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools
3. Siga as instruções na próxima seção, Para importar definições do processo (na página 268).

Importar definições do processo

No sistema do ambiente de produção, importe as definições do processo de fluxo de trabalho.

Siga estas etapas:

1. Reinicie o servidor de aplicativos.
2. Se preferir, crie uma cópia de backup das suas definições atuais exportando as definições usando o procedimento anterior.

3. Vá para *ferramentas_administrativas*\Workpoint\bin\ e execute o script Archive como se segue:

   a. Na caixa de diálogo Importar, selecione todos os itens a serem importados.

   b. Quando for solicitado que você informe sobre o uso do formato novo ou antigo, mantenha o formato antigo.

      O novo formato não oferece suporte ao CA Identity Manager.

   c. Forneça o nome do arquivo gerado pela exportação.

   d. Clique em Ir.

   ferramentas_administrativas se refere às Ferramentas administrativas que são instaladas por padrão em um dos seguintes locais:

   - **Windows:** <caminho_de_instalação>\tools
   - **UNIX:** <caminho_de_instalação2>/tools

Capítulo 10: Logs do CA Identity Manager

Esta seção contém os seguintes tópicos:

Como acompanhar problemas no CA Identity Manager

O CA Identity Manager inclui os seguintes métodos para registrar status e rastrear problemas:

Tarefa Exibir tarefas enviadas

Exibe o status de todos os eventos e tarefas em um ambiente do CA Identity Manager. Os administradores usam essa tarefa no Console de usuário.

Exibir tarefas enviadas oferece os seguintes tipos de informação:

- A lista de eventos e tarefas que ocorrem no ambiente.
- A lista de atributos que são associados a um evento.
- Eventos bem-sucedidos e com falha
- Eventos que estão em um estado pendente ou passado.
- Eventos rejeitados, incluindo o motivo da rejeição
- Status da sincronização da conta
- Status da sincronização da política de identidade
- Informações de provisionamento (quando o provisionamento é ativado).

logs do servidor de aplicativos

Exibe informações sobre todos os componentes em uma instalação do CA Identity Manager, além de fornecer detalhes sobre todas as operações no CA Identity Manager.

O local e o tipo de arquivo de log depende dos seguintes tipos de servidores de aplicativos que você está usando:

- WebLogic — as informações do CA Identity Manager são gravadas fora do padrão. Por padrão, fora do padrão é a janela do console na qual a instância do servidor está em execução.
- JBoss — as informações do CA Identity Manager são gravadas na janela do console onde a instância do servidor está em execução e em *base_do_jboss*\server\log\server.log
- WebSphere — as informações do CA Identity Manager são gravadas na janela do console onde a instância do servidor está em execução e em *base_do_was*\AppServer\logs*nome_do_servidor*\SystemOut

Consulte a documentação do seu servidor de aplicativos para obter mais informações.

Arquivo de logo do Servidor de diretórios

Contém informações sobre a atividade que ocorre no diretório de usuários.

O tipo de informação que é registrado e o local do arquivo de log dependem do tipo do servidor de diretórios que você está usando. Consulte a documentação do diretório do servidor para obter mais informações.

Arquivo de log do Servidor de políticas

Exibe as seguintes informações quando o CA Identity Manager integra-se ao SiteMinder:

- Problemas de conexão do SiteMinder
- Problemas de autenticação do SiteMinder
- Informações sobre os objetos gerenciados do CA Identity Manager no repositório de políticas do SiteMinder.
- Avaliação da política de senha

Para obter informações sobre como configurar logs do SiteMinder, consulte o *Guia de Administração do Servidor de Políticas do CA SiteMinder Web Access Manager*.

Policy Server Profiler

Se o CA Identity Manager integrar-se ao SiteMinder, você poderá rastrear as funções internas de diagnóstico e processamento do Servidor de políticas, incluindo as funções relacionadas ao CA Identity Manager.

Para obter mais informações, consulte Como rastrear campos de dados e componentes (na página 273).

Arquivos de log do agente web

Se o CA Identity Manager integrar-se ao SiteMinder, os agentes web gravarão informações nos dois logs a seguir:

- Arquivo de log de erros — contém os erros em nível operacional e de programa, por exemplo, o agente web não está podendo se comunicar com o Servidor de políticas.
- Arquivo de log de rastreamento — contém mensagens de aviso e informativas, como mensagens de rastreamento e sobre o estado do fluxo. Ele também inclui dados, como detalhes do cabeçalho ou variáveis de cookie.

Observação: para obter mais informações sobre os arquivos de log do agente web, consulte o *Guia de Configuração do Agente Web do SiteMinder Web Access Manager*.

Como rastrear campos de dados e componentes

Quando o CA Identity Manager integra-se ao SiteMinder, você pode usar o Policy Server Profiler do SiteMinder para rastrear campos de dados e componentes nas extensões do CA Identity Manager do Servidor de políticas. O Profiler permite configurar filtros para a saída de rastreamento, de modo que somente valores específicos de um campo de dados ou componente são capturados.

Observação: para obter instruções sobre como usar o Policy Server Profiler, consulte o *Guia de Administração do Servidor de Políticas do SiteMinder Web Access Manager*.

Você pode ativar o rastreamento para os seguintes componentes:

Function_Begin_End

Fornece instruções de rastreamento de nível baixo quando determinados métodos nas extensões do CA Identity Manager do Servidor de políticas são executados.

IM_Error

Rastreia erros de tempo de execução nas extensões do CA Identity Manager do Servidor de políticas do SiteMinder.

IM_Info

Fornece as informações gerais de rastreamento das extensões do CA Identity Manager.

IM_Internal

Rastreia informações gerais sobre operações internas do CA Identity Manager.

IM_MetaData

Fornece as informações de rastreamento quando o CA Identity Manager processa os metadados de diretório.

IM_RDB_Sql

Fornece as informações de rastreamento de bancos de dados relacionais.

IM_LDAP_Provider

Fornece informações de rastreamento de diretórios LDAP.

IM_RuleParser

Rastreia o processo de análise e avaliação de políticas administrativas, de integrante e proprietário, que são definidas em um arquivo XML que é interpretado no tempo de execução.

IM_RuleEvaluation

Rastreia a avaliação das regras de integrante, administrativas, de proprietário e de escopo.

IM_MemberPolicy

Rastreia a avaliação de políticas de integrante, incluindo associação e escopo.

IM_AdminPolicy

Rastreia a avaliação de políticas administrativas.

IM_OwnerPolicy

Rastreia a avaliação de políticas de proprietário.

IM_RoleMembership

Rastreia as informações relacionadas à associação da função, como a lista de funções que um usuário tem e a lista de integrantes em uma determinada função.

IM_RoleAdmins

Rastreia as informações relacionadas à administração da função, como a lista de funções que um usuário pode administrar e a lista de administradores de uma determinada função.

IM_RoleOwners

Rastreia as informações relacionadas à associação da função, como a lista de funções que um usuário possui e a lista de proprietários de uma determinada função.

IM_PolicyServerRules

Rastreia a avaliação das regras de integrante, como RoleMember, RoleAdmin, RoleOwner que o Servidor de políticas resolveu, e as regras de escopo, como as regras All e AccessTaskFilter de AccessTasks

IM_LLSDK_Command

Rastreia a comunicação entre o SDK interno do CA Identity Manager e o servidor de políticas. O Suporte técnico usa esse componente de rastreamento.

IM_LLSDK_Message

Rastreia mensagens que são explicitamente enviadas do SDK interno do CA Identity Manager pelo código Java ao Servidor de políticas. O Suporte técnico usa esse componente de rastreamento.

IM_IdentityPolicy

Rastreia a avaliação e aplicação de Políticas de identidade.

IM_PasswordPolicy

Rastreia a avaliação de políticas de senha.

IM_Version

Fornece informações sobre a versão do CA Identity Manager.

IM_CertificationPolicy

Rastreia a avaliação de políticas de certificação.

IM_InMemoryEval

Rastreia o processamento das políticas do CA Identity Manager, incluindo políticas administrativas, de integrante, proprietário e identidade. O Suporte técnico usa esse componente de rastreamento.

IM_InMemoryEvalDetail

Fornece detalhes adicionais sobre o processamento de políticas do CA Identity Manager, incluindo políticas administrativas, de integrante, proprietário e identidade. O Suporte técnico usa esse componente de rastreamento.

Os campos de dados para os quais você pode configurar o rastreamento são listados no *Guia de Administração do Servidor de Políticas do SiteMinder Web Access Manager*.

Capítulo 11: Proteção do CA Identity Manager

Esta seção contém os seguintes tópicos:

Segurança do Console de usuário

O Console de usuário é a interface de usuário que permite aos administradores gerenciar objetos, como usuários, grupos e organizações em um ambiente do CA Identity Manager. Esses objetos recebem um conjunto de funções e tarefas associadas. Quando um administrador efetua logon no Console de usuário, as tarefas que estão relacionadas ao administrador são exibidas nesse ambiente.

Por padrão, o CA Identity Manager protege o acesso ao Console de usuário com autenticação nativa. Os administradores do CA Identity Manager inserem um nome de usuário e uma senha válidos para efetuar logon em um ambiente do CA Identity Manager. O CA Identity Manager autentica o nome e a senha no repositório de usuários que o CA Identity Manager gerencia.

Se o CA Identity Manager integrar-se ao SiteMinder, o CA Identity Manager usará *automaticamente* a autenticação básica do SiteMinder para proteger o ambiente. Não é necessária nenhuma configuração adicional para usar a autenticação básica. Você pode configurar métodos de autenticação avançados usando a Interface de usuário administrativa do SiteMinder.

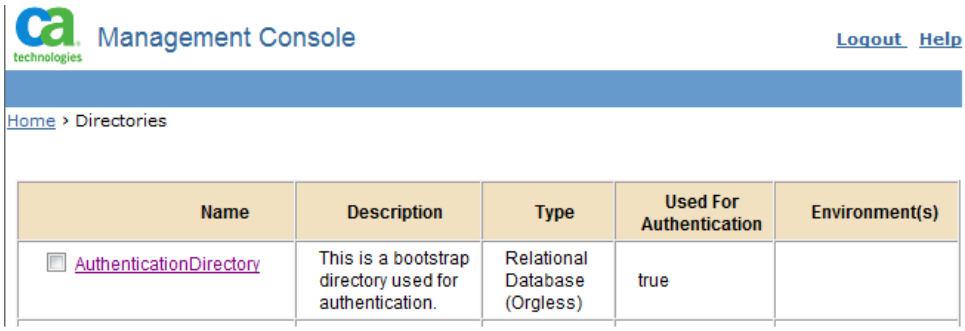
Observação: para obter mais informações, consulte o *Guia de Configuração do Servidor de Políticas do CA SiteMinder Web Access Manager*.

Segurança do Management Console

O Management Console permite aos administradores criar e gerenciar diretórios e ambientes do CA Identity Manager. Os administradores também podem usar o Management Console para configurar a funcionalidade personalizada para um ambiente.

A instalação do CA Identity Manager inclui uma opção para proteger o Management Console. Essa opção é selecionada por padrão. Durante a instalação, especifique as credenciais que o CA Identity Manager usa para autenticar um administrador que poderá acessar o Management Console. O CA Identity Manager cria um usuário com as credenciais que você fornece em um diretório de inicialização chamado AuthenticationDirectory. Você pode exibir esse diretório no Management Console.

Observação: não é possível usar a segurança nativa para proteger o Management Console quando o CA Identity Manager integra-se ao CA SiteMinder.



Adicionar outros administradores do Management Console

Por padrão, um Management Console que é protegido pela segurança nativa do CA Identity Manager tem uma conta de administrador, que é criada em um novo diretório do CA Identity Manager durante a instalação.

Para adicionar outros administradores, especifique um diretório do CA Identity Manager que contenha os usuários que precisam de acesso ao Management Console. O uso de um diretório existente permite conceder acesso do Management Console aos usuários em suas organizações, sem precisar criar novas contas.

Você pode especificar somente um diretório para autenticação. Não é possível excluir um diretório enquanto ele estiver configurado para autenticação.

Siga estas etapas:

1. Efetue logon no Management Console com as credenciais de usuário que você forneceu durante a instalação.
2. Abra Directories e clique no diretório que contém os usuários que exigem acesso para ao Management Console.
3. Clique em Update Authentication.
4. Selecione a opção Used for Authentication.
5. Insira o nome de logon do primeiro usuário e clique em Add.
6. Continue adicionando os usuários que exigem acesso ao Management Console até que todos eles tenham sido adicionados. Em seguida, clique em Save.

   Os usuários que você especificou agora podem usar o respectivo nome de usuário e senha para acessar o Management Console.

Desativar a segurança nativa para o Management Console

Se você ativou a segurança nativa para o Management Console e agora deseja usar outro aplicativo para protegê-lo, desative a segurança nativa antes de implementar outro método de segurança.

Siga estas etapas:

1. Desative a segurança nativa para o Management Console no arquivo web.xml da seguinte maneira:
   a. Abra *installation_do_CA Identity Manager*\iam_im.ear\management_console.war\WEB-INF\web.xml em um editor de texto.
   b. Defina o valor do parâmetro Enable de ManagementConsoleAuthFilter para false da seguinte maneira:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>false</param-value>
   </init-param>
   </filter>
   ```
   c. Salve o arquivo web.xml.
2. Reinicie o servidor do CA Identity Manager.

   O Management Console não está mais protegido pela segurança nativa.

Usar o SiteMinder para proteger o Management Console

Para proteger inicialmente o Management Console, você pode criar uma política do SiteMinder.

Uma política do SiteMinder identifica um recurso que você deseja proteger, como o Management Console, e concede um conjunto de acessos de usuários a esse recurso.

Siga estas etapas:

1. Desative a segurança nativa (na página 280) para o Management Console.
2. Efetue logon em uma das interfaces a seguir como um administrador com privilégios de domínio:
   - No CA SiteMinder r12 ou superior, efetue logon na Interface de usuário administrativa.
   - No CA SiteMinder 6.0 SP*x*, efetue logon na Interface de usuário do servidor de políticas.

   Observação: para obter informações sobre como usar essas interfaces, consulte a documentação da versão do SiteMinder que você está usando.
3. Localize o domínio da política para o Ambiente do CA Identity Manager apropriado.

   Esse domínio é criado automaticamente quando o CA Identity Manager integra-se ao SiteMinder. O nome do domínio tem o seguinte formato:

   *ambiente-do-Identity Manager*Domain

   Nesse formato, *ambiente-do-Identity Manager* especifica o nome do ambiente que você está modificando. Por exemplo, quando o nome for *funcionários*, o nome do domínio será *funcionários*Domain.
4. Crie um realm com o filtro de recursos a seguir:

   /iam/immanage/
5. Crie uma regra para o realm. Especifique um asterisco (*) como o filtro para proteger todas as páginas no Management Console.
6. Crie uma nova política e a associe à regra criada na etapa anterior.

   Certifique-se de associar os usuários que podem acessar o Management Console à política.
7. Reinicie o servidor de aplicativos.

Proteger um ambiente existente após atualização

Após a atualização para o CA Identity Manager 12.6 ou superior, você pode proteger o Management Console usando a segurança nativa.

Observação: não é possível usar a segurança nativa do CA Identity Manager para proteger o Management Console quando o CA Identity Manager integra-se ao CA SiteMinder.

Siga estas etapas:

1. Ative a segurança nativa para o Management Console no arquivo web.xml da seguinte maneira:
   a. Abra *installation_do_CA Identity Manager*\iam_im.ear\management_console.war\WEB-INF\web.xml em um editor de texto.
   b. Defina o valor do parâmetro Enable de ManagementConsoleAuthFilter para true da seguinte maneira:
   ```
   <filter>
   <filter-name>ManagementConsoleAuthFilter</filter-name>
   <filter-
   class>com.netegrity.ims.manage.filter.ManagementConsoleAuth
   Filter</filter-class>
   <init-param>
   <param-name>Enable</param-name>
   <param-value>true</param-value>
   </init-param>
   </filter>
   ```
   c. Salve o arquivo web.xml.
2. Crie a tabela IM_AUTH_USER no repositório de objetos do CA Identity Manager.

   A tabela IM_AUTH_USER armazena informações sobre os administradores do Management Console.
   a. Navegue até CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore
   b. Execute um dos seguintes scripts no repositório de objetos:
      - sql_objectstore.sql
      - oracle_objectstore.sql

   Observação: para obter informações sobre como executar um script em um banco de dados existente, consulte a documentação do fornecedor do banco de dados.

3. Use a ferramenta de senha para criptografar a senha do usuário.

   A ferramenta de senha é instalada com as ferramentas do CA Identity Manager no seguinte local:

Windows: C:\Arquivos de Programas\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   Execute a ferramenta de senha usando o seguinte comando:
   `pwdtools -JSAFE -p anypassword`

   A opção JSAFE criptografa um valor de texto sem formatação usando o algoritmo PBE.

1. Insira as informações do usuário de inicialização na tabela IM_AUTH_USER. Especifique os valores para todas as colunas na tabela IM_AUTH_USER.

   Por exemplo:

   USER_NAME: admin1

   PASSWORD: *qualquer_senha*

   DISABLED: 0

   ID:1

2. Reinicie o servidor do CA Identity Manager.

   O Management Console está protegido pela segurança nativa.

Proteção contra ataques CSRF

O CA Identity Manager foi aperfeiçoado para melhorar a resistência contra ataques CSRF (Cross-Site Request Forgery - solicitação intersite forçada). Por padrão, o aprimoramento é desativado no CA Identity Manager.

Para ativar o aprimoramento:

1. Abra o arquivo web.xml localizado no seguinte local:

   servidor-de-aplicativos/iam_im.ear/user_console.war/WEB-INF

2. Encontre o elemento <context-param> com <param-name> csrf-prevention-on.
3. Defina o <param-value> como true.
4. Reinicie o servidor de aplicativos.

Capítulo 12: Integração com o Service Desk

A integração NIM SM (Normalized Integration Management Service Management) permite integrar o CA Identity Manager a diversos produtos de central de atendimento por meio de uma única API RESTful normalizada. O NIM fornece um serviço web totalmente integrado que expõe essa API RESTful e converte internamente todas as solicitações no formato nativo da central de atendimento com base em um conjunto de mapeamentos configuráveis.

Com o Policy Xpress e suas ações dos serviços web, é possível criar automaticamente tickets de central de atendimento com base no estado das tarefas e dos eventos dentro do CA Identity Manager.

Para obter uma lista completa de produtos de central de atendimento suportados, consulte a Matriz de suporte de produtos.

Os exemplos abaixo demonstram casos de uso para integração com a central de atendimento.

Caso de uso de exemplo: ticket de terminal não disponível

É possível criar uma política do Policy Xpress que é executada com base em falha de uma tarefa ou um evento, por exemplo, quando o CA Identity Manager não consegue se conectar a um terminal. Essa política do Policy Xpress poderá chamar a API RESTful do NIM e criar um ticket na central de atendimento. O ticket contém detalhes suficientes da falha, incluindo mensagens de erro, para ativar a investigação e a resolução de falhas; o fluxo de trabalho é acompanhado pelo ticket da central de atendimento.

Caso de uso de exemplo: ticket de solicitação de provisionamento manual

É possível usar a funcionalidade de serviços para implementar uma solicitação de provisionamento manual e permitir que as contas sejam manualmente provisionadas e desprovisionadas em sistemas que não são gerenciados pelo CA Identity Manager. É possível configurar um serviço com ações de processamento e descumprimento que criam um ticket na central de atendimento por meio da API RESTful do NIM. Um usuário pode, assim, solicitar acesso a esses sistemas e ter a solicitação atribuída, acompanhada e preenchida na forma de um ticket da central de atendimento.

Observação: atualmente o NIM SM oferece suporte à conexão com apenas uma central de atendimento configurada por instância, com uma instância por servidor.

Esta seção contém os seguintes tópicos:

Atualizar credenciais do NIM

O CA NIM SM (Normalized Integration Management Service Management) permite integrar o CA Identity Manager a diversas soluções de central de atendimento.

Durante uma nova instalação, o NIM é configurado para usar o nome de usuário e a senha que você especificar para componentes incorporados da CA.

Ao fazer a atualização para o CA Identity Manager 12.6.5 a partir de uma versão anterior, o nome do usuário e a senha de componentes incorporados da CA não estarão disponíveis. Em vez disso, o nome de usuário e a senha do NIM são revertidos para o valor padrão de "nimadmin". É recomendável atualizar as credenciais do NIM alterando os valores de nome de usuário e senha nos seguintes arquivos:

- iam_im.ear/config/ca_nim.properties
- iam_im.ear/ca-nim-sm.war/WEB-INF/config/NIM-Users.xml

Siga estas etapas:

1. Use a ferramenta de senha para criptografar sua senha.

   Observação: antes de usar a ferramenta de senha, defina a variável de ambiente %JAVE_HOME% no arquivo pwdtools.bat. Para obter mais informações, consulte a Ferramenta de senha.

   a. No computador onde o servidor do CA Identity Manager está instalado, abra uma janela de prompt de comando e vá para o diretório da ferramenta de senha.

   Exemplo:

   C:\Arquivos de programas (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool.

   b. Digite *um* dos seguintes comandos, dependendo dos requisitos de criptografia:

   - Para criptografia compatível com não FIPS, digite o seguinte comando:

   ```
   pwdtools -JSAFE -p password
   ```

   Exemplo de saída:

   Plain text: password

   Encrypted value: {PBES}:WQf3wza4JfbqICD/4D8xog==

   - Para criptografia compatível com FIPS, digite o seguinte comando:

   ```
   pwdtools –FIPS –k [FIPS Key Path] -p password
   ```

   Exemplo de saída:

   Key File location=C:/FIPSkey.dat

   Plain text: password

Encrypted value: {AES}:3BqepUi09EfB3IKmvBBBWg==

2. Vá até iam_im.ear/config/ e abra o arquivo ca_nim.properties em um editor de texto.

   Exemplo: C:\Arquivos de programas\jboss-eap-6.2\standalone\deployments\iam_im.ear\config\ca_nim.properties

3. Localize as seguintes linhas:

   ```
   nimadminUser=nimadmin
   nimadminPassword={PBES}:Q82YUY22ku8X04T1DyBvww==
   ```

4. Substitua os valores por seu nome de usuário e senha criptografada:

   Exemplo:

   ```
   nimadminUser=myusername
   nimadminPassword=myencryptedpassword
   ```

5. Salve o arquivo ca_nim.properties.

6. Use a ferramenta de senha para criptografar a senha no formato esperado pelo NIM. Digite o seguinte comando:

   ```
   pwdtools -CANIMSM -p password
   ```

   Exemplo de saída:

   Texto sem formatação: senha

   Valor criptografado: AAAAEM7HElhthx74qHBkjDD7L/nIthHpxl8z3piCMFyw5ctL

7. Navegue até iam_im.ear/ca-nim-sm.war/WEB-INF/config/ e abra o arquivo NIM-Users.xml em um editor de texto.

8. Localize as seguintes linhas de código:

   ```
   <User>
   <property name="username" value="nimadmin"/>
   <property name="password"
   value="AAAAEDFsjJUDxVV9PK+2putOEiUsoPzGAcDjnMGFie4NC01Z"/>
   </User>
   ```

9. Substitua os valores por seu nome de usuário e senha criptografada.

   Exemplo:

   ```
   <User>
   <property name="username" value="myusername"/>
   <property name="password" value="myencryptedpassword"/>
   </User>
   ```

10. Reinicialize o servidor de aplicativos.

Você atualizou suas credenciais do NIM.

Importar definições de função para integração com a central de atendimento

Para integrar o ambiente do CA Identity Manager à solução do Service Desk, importe as definições de função do Gerenciamento de serviços do CA NIM. Essas definições de função adicionam as seguintes tarefas à função do gerenciador do sistema:

- Configurar a integração com o Service Desk
- Personalizar mapeamentos de campos do Service Desk
- Exibir a documentação da API REST da integração com o Service Desk

Siga estas etapas:

1. No Console de gerenciamento, vá para Environments e clique no ambiente que deseja integrar com a solução do Service Desk.
   A tela Environment Properties é exibida.
2. Clique em Roles and Tasks, Import, selecione NIM Service Management e clique em Import.
3. Reinicie o ambiente.

Você importou as definições de função da integração com o Service Desk.

Configurar a integração com o Service Desk

Para permitir que o CA Identity Manager se comunique com a solução do Service Desk, configure a integração com o Service Desk.

Siga estas etapas:

1. No Console do usuário do CA Identity Manager, vá para Sistema, Integração NIM SM e clique em Configurar a integração com o Service Desk.
2. Selecione a solução de central de atendimento na lista suspensa.
3. Insira as configurações de conexão de sua solução de central de atendimento e clique em Enviar.

Observação: para obter mais informações, consulte a seção de configurações de conexões da sua solução de central de atendimento específica.

Mais informações:

Configurações de conexão do CA Cloud Service Management (na página 295)
Configurações de conexão do CA Service Desk Manager (na página 291)
Configurações de conexão do HP Service Manager (na página 292)
Configurações de conexão do BMC Remedy ITSM (na página 293)
Configurações de conexão do ServiceNow (na página 296)

Configurações de conexão do CA Service Desk Manager

Para realizar a integração com o CA Service Desk Manager, forneça os seguintes parâmetros:

- Protocol_SOAP
  Especifica o protocolo usado para se conectar aos serviços web SOAP do CA Service Desk Manager.
  Valores válidos: http, https
  Padrão: http
- Host_SOAP
  Especifica o host usado para se conectar aos serviços web SOAP do CA Service Desk Manager.
  Exemplo: CA-SERDESK-S1
- Port_SOAP
  Especifica o número de porta usado para se conectar aos serviços web SOAP do CA Service Desk Manager.
  Padrão: 8080
- Protocol _REST
  Especifica o protocolo usado para se conectar aos serviços web REST do CA Service Desk Manager.
  Exemplo: http
- Host_REST
  Especifica o host usado para se conectar aos serviços web REST do CA Service Desk Manager.
  Exemplo: CA-SERDESK-S1
- Port_REST
  Especifica o número de porta usado para se conectar aos serviços web REST do CA Service Desk Manager.
  Padrão: 8050
  Porta SSL: 8413
- Nome de usuário
  Especifica a ID de usuário usada para se conectar aos serviços web do CA Service Desk Manager.
  Padrão: ServiceDesk
- Senha
  Define a senha do usuário do CA Service Desk Manager.
- DefaultAttachmentRepositoryName
  Define o repositório padrão usado para armazenar anexos do CA Service Desk Manager.
  Padrão: Service Desk

Para obter mais informações sobre o CA Service Desk Manager, consulte a documentação do CA Service Desk Manager.

Configurações de conexão do HP Service Manager

Para realizar a integração com o HP Service Manager, forneça os seguintes parâmetros:

- Host
  Especifica o host usado para estabelecer conexão com o HP Service Manager.
- Porta
  Especifica o número de porta usado para estabelecer conexão com o HP Service Manager.
  Exemplo: 13080
- Nome de usuário
  Especifica o nome de usuário usado para estabelecer uma conexão com o HP Service Manager.
- Senha
  Especifica a senha usada para estabelecer conexão com o HP Service Manager.
- HPSMClientURL
  Especifica o HPSMClientURL usado para estabelecer conexão com o HP Service Manager.
  Padrão: http://hpsm-host-name:port-number/webtier-9.32
- ProxyServer do Service Desk (opcional)
  Especifica qualquer servidor proxy no ambiente usado para estabelecer conexão com o HP Service Manager.
  Exemplo: proxy.xxx.com
- ProxyPort do Service Desk (opcional)
  Especifica a porta de proxy configurada e usada para estabelecer conexão com o HP Service Manager.
  Exemplo: 80
- ProxyUser do Service Desk (opcional)
  Especifica o usuário do proxy usado para estabelecer conexão com o HP Service Manager.
- ProxyPassword do Service Desk (opcional)
  Especifica a senha do proxy usada para estabelecer conexão com o HP Service Manager.
- EnabledProtocol
  Especifica o protocolo em uso.
  Padrão: http

(WebLogic) Configurar IDM_OPTS

Um problema conhecido com a implementação padrão do WebLogic SAAJ pode gerar a seguinte mensagem de erro:

java.lang.UnsupportedOperationException: essa classe não oferece suporte a SAAJ 1.3

Adicione a seguinte propriedade à variável IDM_OPTS configurada em WebLogic Install Dir/user_projects/domains/base_domain/bin/setDomainEnv.cmd e reinicie o WebLogic:

```
-Djavax.xml.soap.MessageFactory=weblogic.xml.saaj.MessageFactoryImpl
```

Para obter mais informações sobre o HP Service Desk Manager, consulte a documentação do HP Service Desk Manager.

Configurações de conexão do BMC Remedy ITSM

Pré-requisitos

Antes de definir as configurações do BMC Remedy ITSM, copie os arquivos jar do SDK do sistema BMC Remedy para o servidor. Esses arquivos permitem a comunicação entre o CA Identity Manager e o BMC Remedy.

Siga estas etapas:

Válido no Windows e no Linux

1. No sistema BMC Remedy, vá até o seguinte arquivo:
   \\bmc\Software\ARSystem\Arserver\api\lib
2. Copie os seguintes arquivos jar do SDK:
   - arapi8*.jar
   - arutil81*.jar
3. Salve os arquivos jar copiados no seguinte local do sistema do CA Identity Manager:
   iam_im.ear/ca-nim-sm.war/WEB-INF/lib
4. Reinicialize o servidor de aplicativos.

Parâmetros

Para realizar a integração com o BMC Remedy ITSM, forneça os seguintes parâmetros:

- Host
  Define o host usado para estabelecer conexão com o BMC Remedy ITSM.
  Padrão: bmc_host_name
- Porta
  Define o número da porta usada para estabelecer conexão com o BMC Remedy ITSM.
  Padrão: 0
- Nome de usuário
  Define o nome de usuário usado para estabelecer conexão com o BMC Remedy ITSM.
  Padrão: admin
- Senha
  Define a senha usada para se conectar ao BMC Remedy ITSM.
- BMCRemedyClientURL
  Define o BMCRemedyClientURL usado para estabelecer conexão com o BMC Remedy ITSM.
  Exemplo: http://bmc_client_host_name:8080/arsys

Configurações de conexão do CA Cloud Service Management

(WebSphere) Recuperar certificados de servidor

Para permitir a comunicação entre o CA Cloud Service Management e o CA Identity Manager, recupere os certificados do servidor e adicione-os ao NodeDefaultTrustStore.

Siga estas etapas:

1. No console administrativo do WebSphere, expanda Segurança e clique em Certificado SSL e Gerenciamento de chaves.
2. Em Definições de configuração, clique nas configurações de segurança Gerenciar terminais.
3. Selecione a configuração de saída apropriada para atingir o escopo de gerenciamento (cell): <server-name>Node01Cell:(node):<server-name>Node01.
4. Em Itens relacionados, clique em Repositório de chaves e certificados e clique no repositório de chaves NodeDefaultTrustStore.
5. Em Propriedades adicionais, clique em Certificados signatários e Recuperar da porta.
6. Digite os seguintes parâmetros no campo Host:

   nome do host: sm2t.saas.ca.com

   porta: 443

   alias: sm2t.saas.ca.com_cert
7. Clique em Recuperar informações do signatário.
8. Verifique se as informações do certificado são de um certificado confiável.
9. Clique em Aplicar e salvar.
10. Reinicie o WebSphere.

Você recuperou os certificados do servidor.

Parâmetros

Para realizar a integração com o CA Cloud Service Desk Management, forneça os seguintes parâmetros:

- URL
  Especifica o URL usado para estabelecer conexão com o CA Cloud Service Management.
  Exemplo: https://xxx.saas.ca.com/
  Padrão: https://cacsmwebservice_host_name/

- Nome de usuário
  Especifica o nome de usuário usado para estabelecer conexão com o CA Cloud Service Management.
  Exemplo: webuser@org.com
- Senha
  Especifica a senha usada para estabelecer conexão com o CA Cloud Service Management.
- CACSMClient URL
  Especifica o CACSMClient URL que é usado para LaunchIncontext URL. LaunchIncontext redireciona o usuário final para a ID de incidente do CA Cloud Service Management Service Desk específico.
  Exemplo: https://xxx.saas.ca.com/
  Padrão: https://cacsmclient_host_name/
- ProxyServer do Service Desk (opcional)
  Especifica qualquer servidor proxy no ambiente que é usado para estabelecer conexão com o CA Cloud Service Management.
  Exemplo: proxy.xxx.com
- ProxyPort do Service Desk (opcional)
  Especifica a porta de proxy que está configurada e é utilizada para estabelecer conexão com o CA Cloud Service Management.
  Exemplo: 80
- ProxyUser do Service Desk (opcional)
  Especifica o nome de usuário que está sendo usado com o servidor proxy.
- ProxyPassword do Service Desk (opcional)
  Define a senha do nome de usuário do proxy.

Para obter mais informações sobre o CA Cloud Service Management, consulte a documentação do produto.

Configurações de conexão do ServiceNow

Para autorizar o acesso da API REST a um usuário que não seja um administrador, é possível atribuir a função rest_service a um usuário em sua instância.

Parâmetros

Para realizar a integração com o ServiceNow, forneça os seguintes parâmetros:

- URL
  Especifica o URL usado para estabelecer conexão com o ServiceNow.
  Exemplo: https://xxx.service-now.com/
  Padrão: https://servicenow-webservice-host-name
- Nome de usuário
  Especifica o nome de usuário usado para estabelecer conexão com o ServiceNow.

- Senha
  Especifica a senha usada para estabelecer conexão com o ServiceNow.
- ServiceNowClientURL
  Especifica o ServiceNowClientURL usado para estabelecer conexão com o ServiceNow.
  Padrão: https://servicenow-host-name
- useCustomEndpoint
  Especifica se deve realizar a conexão por meio do Terminal personalizado.
  Padrão: Falso

  Observação: se essa opção não estiver ativada em sua solução do Service Desk, toda validação será realizada com a configuração useCustomEndpoint.
- ProxyServer do Service Desk (opcional)
  Especifica o servidor proxy no ambiente usado para estabelecer conexão com o ServiceNow.
  Exemplo: proxy.xxx.com
- ProxyPort do Service Desk (opcional)
  Especifica a porta do proxy configurada e usada para estabelecer conexão com o ServiceNow.
  Exemplo: 80
- ProxyUser do Service Desk (opcional)
  Especifica o usuário proxy usado para estabelecer conexão com o ServiceNow.
- ProxyPassword do Service Desk (opcional)
  Especifica a senha do proxy usada para estabelecer conexão com o ServiceNow.

(WebSphere) Recuperar certificados de servidor

Para permitir a comunicação entre o ServiceNow e o CA Identity Manager, recupere os certificados do servidor e adicione-os ao NodeDefaultTrustStore.

Siga estas etapas:

1. No console administrativo do WebSphere, expanda Segurança e clique em Certificado SSL e Gerenciamento de chaves.
2. Em Definições de configuração, clique nas configurações de segurança Gerenciar terminais.
3. Selecione a configuração de saída apropriada para atingir a (célula): <server-name>Node01Cell:(node):<server-name>Node01 management scope.
4. Em Itens relacionados, clique em Repositório de chaves e certificados e clique no repositório de chaves NodeDefaultTrustStore.
5. Em Propriedades adicionais, clique em Certificados signatários e Recuperar da porta.

6. Digite os seguintes parâmetros no campo Host:

   nome do host: service-now.com

   porta: 443

   alias: service-now.com_cert

7. Clique em Recuperar informações do signatário.
8. Verifique se as informações do certificado são de um certificado confiável.
9. Clique em Aplicar e salvar.
10. Reinicie o WebSphere.

Você recuperou os certificados do servidor.

(WebLogic) Configurar o verificador de nome do host

O verificador de nome do host padrão do WebLogic tem um problema com os nomes de host que contêm caracteres curinga; configure o servidor WebLogic para usar SSLWLSWildcardHostnameVerifier.

Siga estas etapas:

1. No console WLS, vá para Ambiente, Servidores, AdminServer.
2. Selecione a guia SSL e clique em Avançado.
3. Altere a entrada de verificação de nome do host para Verificador de nome do host personalizado.
4. No tipo de verificador de nome do host personalizado, digite o seguinte texto: weblogic.security.utils.SSLWLSWildcardHostnameVerifier
5. Selecione usar SSL JSSE
6. Clique em Salvar e reiniciar o WebLogic

Você configurou o verificador de nome do host.

Personalizar mapeamentos de campos do Service Desk

Quando você configura a integração com o Service Desk, por padrão, vários campos do NIM são mapeados em campos na sua solução do Service Desk. Você pode personalizar esses mapeamentos de campos, adicionar mapeamentos extra e criar mapeamentos de campos personalizados. Por exemplo, é possível criar outros níveis de gravidade ou urgência.

Definir um novo mapeamento de campo

Siga estas etapas:

1. Vá para Sistema, Integração NIM SM e clique em Personalizar mapeamentos de campos do Service Desk.
2. Selecione o campo do CA NIM que deseja mapear.
3. Selecione o campo do Service Desk que deseja mapear para o NIM.
4. (Opcional) Adicione um valor padrão.
5. (Opcional) Adicione valores possíveis.
6. Clique em Adicionar.

Você definiu um novo mapeamento de campo.

Observação: para personalizar os mapeamentos de campos existentes, primeiro exclua o mapeamento que deseja personalizar e readicione-o da mesma forma que você define um novo mapeamento de campo.

Definir mapeamentos de campos personalizados

Se sua solução do Service Desk contiver campos personalizados que não são detectados automaticamente pelo NIM, defina os mapeamentos de campos personalizados.

Siga estas etapas:

1. Vá para Sistema, Integração NIM SM e clique em Personalizar mapeamentos de campos do Service Desk.
2. Selecione Ativar campo NIM personalizado.
3. Em Campo NIM personalizado, defina um nome para o campo.
4. Selecione o tipo de dados.
   Valores: DateTime, String
5. Selecione o campo do Service Desk para o qual deseja que o campo personalizado seja mapeado.
6. (Opcional) Adicione um valor padrão.
7. (Opcional) Adicione valores possíveis.
8. Clique em Adicionar.

Você definiu um mapeamento de campo personalizado.

Observação: em uma chamada do REST, os campos personalizados são usados de maneira diferente dos Campos CA NIM padrão. O exemplo a seguir mostra como usar os campos personalizados em uma chamada REST:

Corpo da solicitação XML

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<incident>
   <description>incidente de teste</description>
   <impact>alto</impact>
   <label>alterar_rótulo</label>
   <priority>crítica</priority>
   <severity>alta</severity>
   <status>novo</status>
   <urgency>alta</urgency>
   <customproperties>
      <property>
        <name>customField1</name>
        <value>10</value>
      </property>
   </customproperties>
</incident>
```

Corpo da solicitação JSON

```
{
   "description": "test incident",
   "category": "inquiry",
   "customproperties": {
     "property": [
     {
       "name": "customField1",
       "value": "10"
     }
  ]
  },
  "impact": "high",
  "label": "label_change",
  "priority": "critical",
  "severity": "high",
  "status": "new",
  "urgency": "high"
}
```

Documentação da API REST da integração com o Service Desk

A documentação da API REST do NIM está disponível no console do usuário do CA Identity Manager.

Vá para Sistema, Integração NIM SM e clique em Exibir a documentação da API REST da integração com o Service Desk. No quadro que se abre, é possível exibir o modelo de cada tipo de objeto e testar as chamadas de API usando o botão Try it out!

Observe o seguinte:

- Para acessar a documentação da API REST, certifique-se de procurar usando todo o domínio no URL do servidor CA Identity Manager. Exemplo: use http://myserver.domain.com:8080/iam/im/env, não http://myserver:8080/iam/im/env
- Para usar o recurso "Experimente", é necessário digitar suas informações de autenticação de acesso básico no campo de cabeçalho Autorização básica HTTP. Esse é apenas um cabeçalho de autenticação básica padrão.

  Exemplo: no cabeçalho de autenticação básica "Basic bmltYWRtaW46bmltYWRtaW4=", bmltYWRtaW46bmltYWRtaW4= é simplesmente “username:password” codificado em Base64.

Detalhes do NIM SM Web Service

Para chamar o NIM Web Service, use estes URLs:

- URL base:
  http://myserver.domain.com:[Server Port Number]/iam/imnimsm/api/v1
- URL base (implantação de cluster):
  http://localhost:[Server Port Number]/iam/imnimsm/api/v1 como o URL base.
- Para acessar APIs específicas, adicione o nome no fim do URL.
  Exemplo: para acessar a API do incidente, use este URL:
  http://myserver.domain.com:[Server Port Number]/iam/imnimsm/api/v1/incident

O NIM Web Service usa a Autenticação básica de HTTP e as credenciais são o nome de usuário e a senha fornecidos para componentes CA incorporados durante uma instalação nova ou as credenciais atualizadas que você configura após a atualização.

Amostras PolicyXpress do NIM

O CA Identity Manager 12.6.5 inclui um Policy Xpress de amostra que pode ser útil quando você precisa criar suas próprias políticas.

É possível importar as políticas de amostra contidas em NimIntegrationSample.xml em seu ambiente. Esse arquivo está localizado no diretório de instalação do CA Identity Manager em samples\PolicyXpress\NimIntegration.

Exemplo: C:\Arquivos de programas (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\PolicyXpress\NimIntegration

Para obter mais informações, consulte o arquivo leiame.txt encontrado no diretório em que a política de exemplo está localizada.

Capítulo 13: Integração do CA SiteMinder

Esta seção contém os seguintes tópicos:

SiteMinder e CA Identity Manager

Quando o CA Identity Manager integra-se ao CA SiteMinder, o CA SiteMinder pode adicionar as seguintes funcionalidades a um ambiente do CA Identity Manager:

Autenticação avançada

O CA Identity Manager inclui autenticação nativa para Ambientes do CA Identity Manager por padrão. Os administradores do CA Identity Manager inserem um nome de usuário e uma senha válidos para efetuar logon em um Ambiente do CA Identity Manager. O CA Identity Manager autentica o nome e a senha no repositório de usuários que o CA Identity Manager gerencia.

Quando o CA Identity Manager integra-se ao CA SiteMinder, o CA Identity Manager usa a autenticação básica do CA SiteMinder para proteger o Ambiente. Quando você cria um Ambiente do CA Identity Manager, um domínio da política e um esquema de autenticação são criados no CA SiteMinder para proteger o Ambiente.

Quando o CA Identity Manager integra-se ao CA SiteMinder, também é possível usar a autenticação do SiteMinder para proteger o Management Console.

Funções e tarefas de acesso

As funções de acesso permitem que os administradores do CA Identity Manager atribuam privilégios em aplicativos que o CA SiteMinder protege. As funções de acesso representam uma única ação que um usuário pode executar em um aplicativo de negócios, como a geração de uma ordem de compra em um aplicativo financeiro.

Mapeamento de diretório

Um administrador pode precisar gerenciar usuários cujos perfis existem em um repositório de usuários diferente daquele que é usado para autenticar o administrador. Ao efetuar logon no Ambiente do CA Identity Manager, o administrador é autenticado usando um diretório e outro diretório para autorizar o administrador a gerenciar usuários.

Quando o CA Identity Manager integra-se ao CA SiteMinder, é possível configurar um Ambiente do CA Identity Manager para usar diretórios diferentes para autenticação e autorização.

Capas de diferentes conjuntos de usuários

A capa muda a aparência do Console de usuário. Quando o CA Identity Manager integra-se ao CA SiteMinder, é possível ativar diferentes conjuntos de usuários para ver diferentes capas. Para fazer essa alteração, use uma resposta do SiteMinder para associar uma capa a um conjunto de usuários. A resposta é emparelhada com uma regra em uma política, que está associada a um conjunto de usuários. Quando a regra é acionada, ela dispara a resposta para passar informações sobre a capa ao CA Identity Manager para criação do Console de usuário.

Observação: para obter mais informações, consulte o *Guia de Design do Console de Usuário*.

Preferências de localidade para um ambiente localizado

Quando o CA Identity Manager integra-se ao CA SiteMinder, é possível definir a preferência de localidade para um usuário usando um cabeçalho HTTP imlanguage. No Servidor de políticas do SiteMinder, você deverá definir esse cabeçalho dentro de uma resposta do SiteMinder e especificar um atributo de usuário como o valor do cabeçalho. Esse cabeçalho imlanguage atua como a preferência de localidade de prioridade mais alta para um usuário.

Observação: para obter mais informações, consulte o *Guia de Design do Console de Usuário*.

Mais informações:

Coletar credenciais do usuário usando um esquema de autenticação personalizado (na página 357)

Como os recursos são protegidos

A autenticação avançada exige que você use um Servidor de políticas do SiteMinder em sua implementação. O servidor de aplicativos que hospeda o Servidor do CA Identity Manager está em um ambiente operacional diferente do servidor web. Para fornecer serviços de encaminhamento, o servidor web exige:

- Um fornecedor de servidor de aplicativos que forneceu o plugin.
- Um agente do SiteMinder para proteger os recursos do CA Identity Manager, como o Console de usuário, o Autorregistro e o recurso de Senha esquecida.

O Agente web controla o acesso de usuários que solicitam recursos do CA Identity Manager. Depois que os usuários forem autenticados e autorizados, o Agente web permitirá que o servidor web processe as solicitações.

Quando o servidor web receber a solicitação, o plugin do servidor de aplicativos a encaminhará ao servidor de aplicativos que hospeda o Servidor do CA Identity Manager.

O Agente web protege os recursos do CA Identity Manager que são expostos aos usuários e administradores.

Visão geral da integração do SiteMinder e CA Identity Manager

Quando o administrador de políticas e o administrador de identidades trabalham juntos para integrar o SiteMinder a uma instalação existente do CA Identity Manager, a arquitetura do CA Identity Manager é expandida para incluir os seguintes componentes:

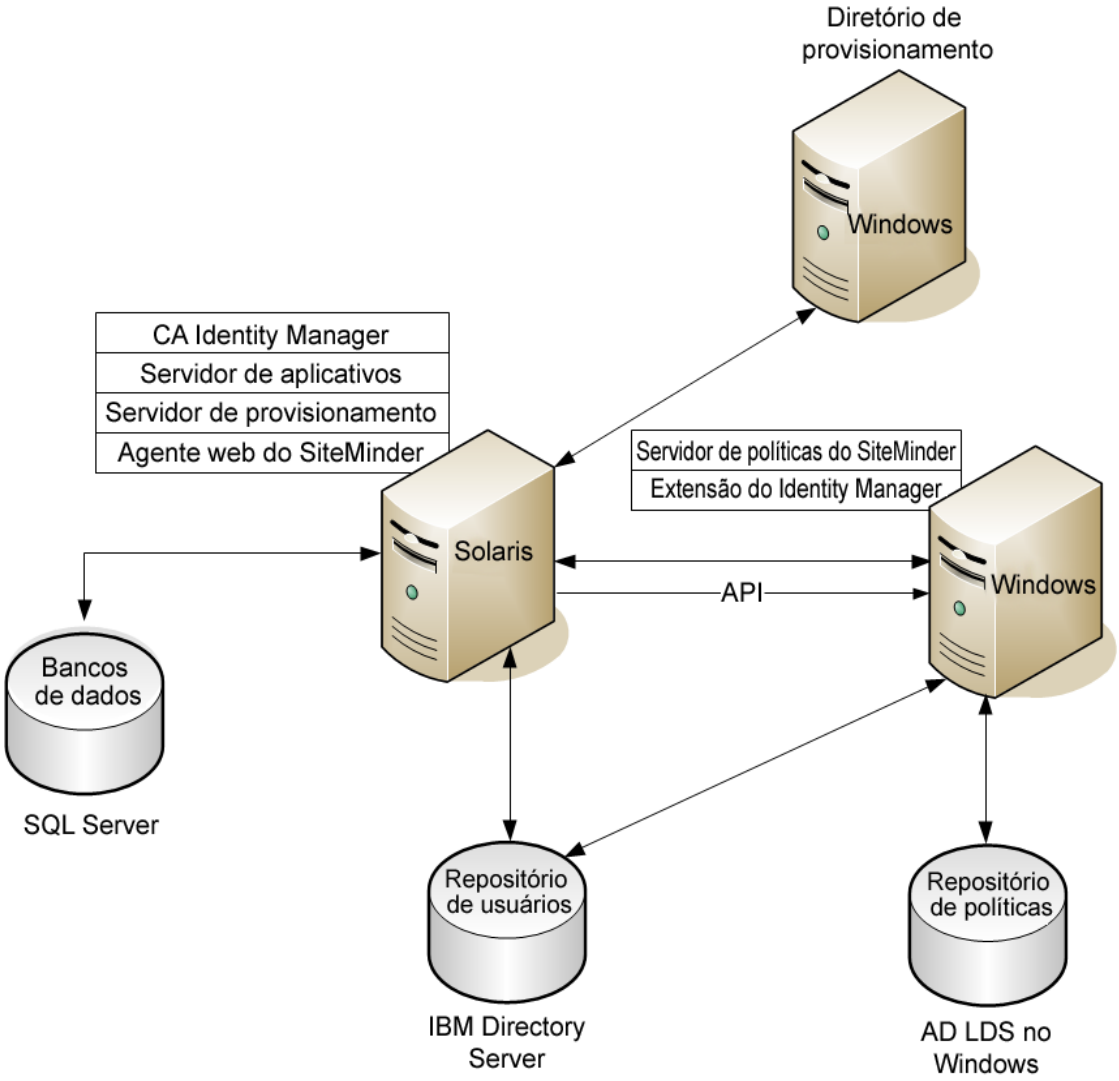
Agente web do SiteMinder

Protege o Servidor do CA Identity Manager. O Agente web está instalado no sistema com o Servidor do CA Identity Manager.

Servidor de políticas do SiteMinder

Fornece autenticação avançada e autorização para o CA Identity Manager.

A figura a seguir é um exemplo de uma instalação do CA Identity Manager com um Servidor de políticas e Agente web do SiteMinder:

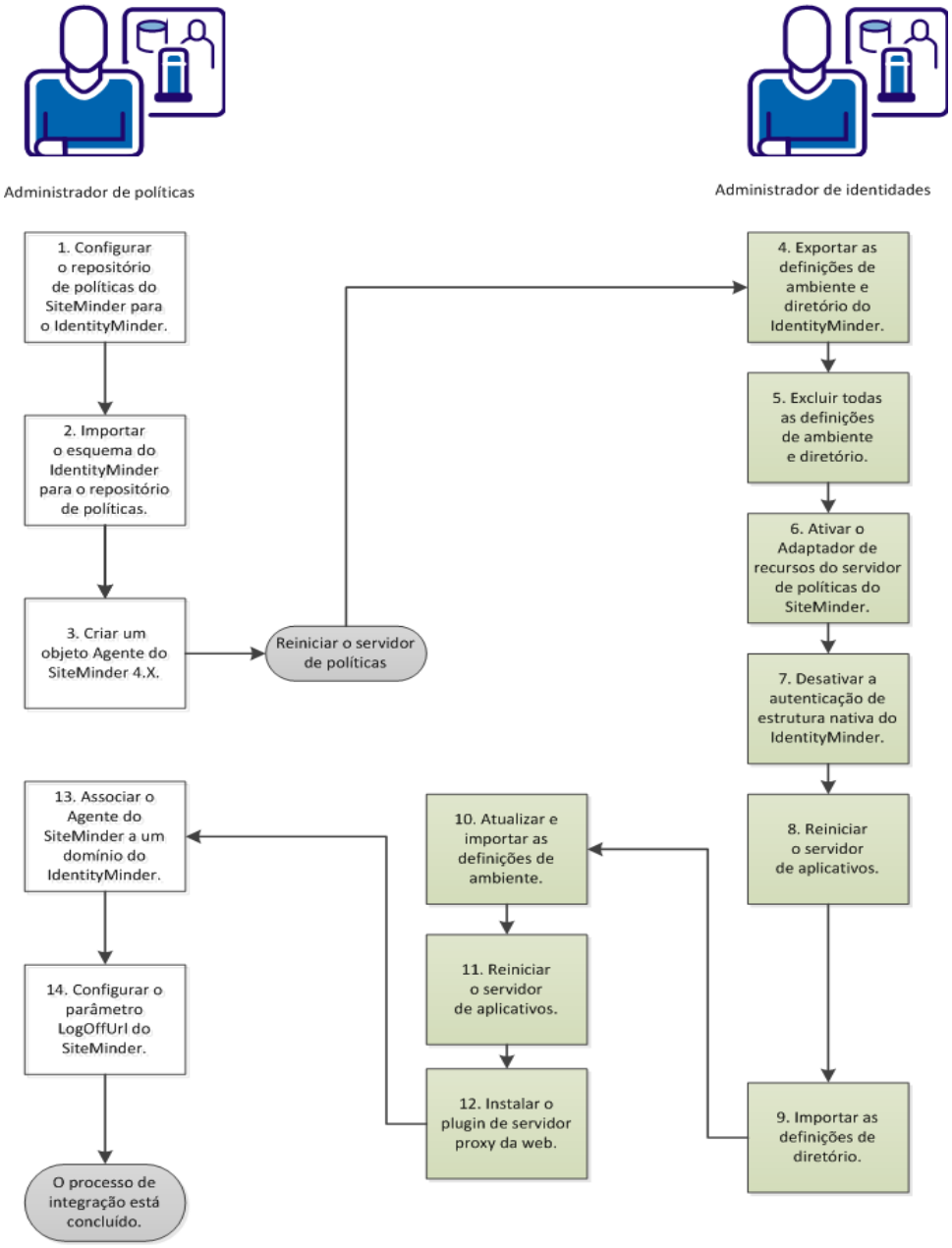


Observação: os componentes são instalados em diferentes plataformas, como nos exemplos. No entanto, você pode escolher outras plataformas. Os bancos de dados do CA Identity Manager estão no Microsoft SQL Server e o repositório de usuários está no IBM Directory Server. O Servidor de políticas do SiteMinder está no AD LDS do Windows.

A conclusão desse processo exige duas funções: o administrador de identidades do CA Identity Manager e o administrador de políticas do SiteMinder. Em algumas organizações, uma pessoa preenche ambas as funções. Quando duas pessoas são envolvidas, a colaboração próxima é necessária para concluir os procedimentos nesse cenário. O administrador de políticas começa e termina esse processo; o administrador de identidades realiza todas as etapas intermediárias.

Importante: para instalações do CA Identity Manager que começam com Release12.5 SP7, os arquivos Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files (bibliotecas JCE) são necessários. Faça download desses bibliotecas no site da Oracle. Carregue-as na seguinte pasta: <caminho_Java>\<versão_jdk>\jre\lib\security\.

O diagrama a seguir ilustra o processo completo da integração do SiteMinder ao CA Identity Manager:



Siga estas etapas:

1. Configure o repositório de políticas do SiteMinder para o CA Identity Manager. (na página 310)
2. Importe o esquema do CA Identity Manager no repositório de políticas. (na página 316)
3. Crie um objeto de agente do SiteMinder 4.X. (na página 316)
4. Exporte os diretórios e ambientes do CA Identity Manager. (na página 318)
5. Exclua todas as definições de diretório e ambiente. (na página 318)
6. Ative o adaptador de recursos do Servidor de políticas do SiteMinder. (na página 319)
7. Desative o Filtro de autenticação de estrutura nativo do CA Identity Manager. (na página 320)
8. Reinicialize o servidor de aplicativos. (na página 321)
9. Configure uma origem de dados para o SiteMinder. (na página 321)
10. Importe as definições de diretório. (na página 322)
11. Atualize e importe as definições de ambiente. (na página 323)
12. Reinicialize o servidor de aplicativos. (na página 321)
13. Instale o plugin do servidor proxy web. (na página 323)
14. Associe o Agente do SiteMinder a um domínio do CA Identity Manager. (na página 342)
15. Configure o parâmetro LogOffUrl do SiteMinder. (na página 343)

Configurar o repositório de políticas do SiteMinder para o CA Identity Manager

Como um administrador de políticas, você usa as Ferramentas administrativas do CA Identity Manager para acessar os scripts SQL ou o texto de esquema LDAP para adicionar o esquema IMS ao repositório de políticas. O administrador de identidades terá instalado essas ferramentas na pasta Ferramentas administrativas. Siga *um* dos procedimentos a seguir para configurar o repositório de políticas:

Configurar um banco de dados relacional (na página 310)

Configurar o Servidor de diretórios do Sun Java Systems ou do IBM Directory Server (na página 311)

Configurar o Microsoft Active Directory (na página 311)

Configurar o Microsoft ADAM (na página 312)

Configurar o CA Directory Server (na página 313)

Configurar o Novell eDirectory Server (na página 314)

Configurar o Oracle Internet Directory (OID) (na página 315)

Configurar um banco de dados relacional

Após a configuração, você poderá usar o banco de dados relacional como um repositório de políticas do SiteMinder.

Siga estas etapas:

1. Configure o banco de dados como um repositório de políticas do SiteMinder suportado.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do SiteMinder*.

2. Execute o script apropriado para o banco de dados:

   - **SQL:** <caminho_de_instalação>\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** <caminhos_de_instalação2>/tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   Os caminhos anteriores são locais de instalação padrão. O local para a sua instalação pode ser diferente.

Configurar o Servidor de diretórios do Sun Java Systems ou do IBM Directory Server

Para configurar um servidor de diretórios do Java ou IBM, aplique o arquivo de esquema.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

2. Adicione o arquivo de esquema LDIF apropriado para o diretório. O local padrão do Windows para os arquivos LDIF é <caminho_de_instalação>\tools\policystore-schemas.

   Adicione os seguintes arquivos de esquema para seu diretório:

   - **IBM Directory Server:**

     IBMDirectoryServer\V3.identityminder8

   - **Servidor de diretórios do Sun Java Systems (iPlanet):**

     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Configurar o Microsoft Active Directory

Para configurar um repositório de políticas do Microsoft Active Directory, aplique o script activedirectory_ims8.ldif.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

2. Modifique o arquivo de esquema activedirectory_ims8.ldif da seguinte maneira:

   a. Em um editor de texto, abra o arquivo activedirectory_ims8.ldif. O local padrão do Windows é:

      <caminho_de_instalação>\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Substitua todas as instâncias de {root} pela organização raiz do diretório.

      A organização raiz deve corresponder à organização raiz que você especificou quando configurou o repositório de políticas no Management Console do Servidor de políticas.

Por exemplo, se a raiz for dc=myorg,dc=com, substitua
dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root} pelo dn:
CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com

c. Salve o arquivo.

3. Adicione o arquivo de esquema conforme descrito na documentação do seu diretório.

Configurar o Microsoft ADAM

Para configurar um repositório de políticas do Microsoft ADAM, aplique o script adam_ims8.ldif.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

   Anote o valor do CN (o guid).

2. Modifique o arquivo de esquema adam_ims8.ldif da seguinte maneira:

   a. Abra o arquivo adam_ims8.ldif\.ldif em um editor de texto. O local padrão do Windows é:

      <caminho_de_instalação>\tools\policystore-schemas\MicrosoftActiveDirectory

   b. Substitua cada referência a cn={guid} pela sequência de caracteres encontrada quando você configurou o repositório de políticas do SiteMinder na Etapa 1 desse procedimento.

      Por exemplo, se a sequência de caracteres do GUID for CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}, substitua cada referência a cn={guid} por CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}.

   c. Salve o arquivo.

3. Adicione o arquivo de esquema conforme descrito na documentação do seu diretório.

Configurar o CA Directory Server

Para configurar um CA Directory Server, você cria um arquivo de esquema personalizado. Nas etapas a seguir, *base_de_dxserver* é o diretório onde o CA Directory está instalado. O local de origem padrão para esse arquivo no Windows é <caminho_de_instalação>\tools\\policystore-schemas eTrustDirectory.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

2. Copie etrust_ims8.dxc em *base_de_dxserver*\config\esquema.

3. Crie um arquivo de configuração de esquema personalizado da seguinte maneira:

   a. Copie o *base_de_dxserver*\config\schema\default.dxg em *base_de_dxserver*\config\schema*nome_da_empresa*-schema.dxg.

   b. Edite o arquivo *base_de_dxserver*\config\schema*nome_da_empresa*-schema.dxg adicionando as linhas a seguir ao fim do arquivo:

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. Edite o arquivo *base_de_dxserver*\bin\schema.txt adicionando o conteúdo do etrust_ims_schema.txt ao fim do arquivo. O local de origem padrão para esse arquivo no Windows é <caminho_de_instalação>\tools\\policystore-schemas eTrustDirectory.

5. Crie um arquivo de configuração de limites personalizado da seguinte maneira:

   a. Copie o *base_de_dxserver*\config\limits\default.dxc em *base_de_dxserver*\config\limits*nome_da_empresa*-limits.dxc.

   b. Aumente o limite de tamanho padrão para 5000 no arquivo *base_de_dxserver*\config\limits*nome_da_empresa*-limits.dxc como se segue:

   ```
   set max-op-size=5000
   ```

   Observação: a atualização do CA Directory substitui o arquivo limits.dxc. Portanto, não se esqueça de redefinir max-op-size para 5000 depois que a atualização for concluída.

6. Edite o *base_de_dxserver*\config\servers*nome_dsa*.dxi como se segue:

   ```
   # schema
   source "nome_da_empresa-schema.dxg";

   #service limits
   source "nome_da_empresa-limits.dxc";
   ```

   onde *nome_dsa* é o nome do DSA que usam os arquivos de configuração personalizados.

7. Execute o utilitário dxsyntax.
8. Pare e reinicie o DSA como o usuário do dsa para que as alterações do esquema entrem em vigor, como a seguir:
   `dxserver stop nome_dsa`
   `dxserver start nome_dsa`

Configurar o Novell eDirectory Server

Para configurar um repositório de políticas do Novell eDirectory Server, aplique o script novell_ims8.ldif.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

2. Localize o DN (Distinguished Name - nome distinto) do NCPServer para seu Novell eDirectory Server inserindo as informações a seguir em uma janela de comando no sistema, onde o Servidor de políticas está instalado:
   `ldapsearch -h nome_do_host -p porta -b recipiente -s sub -D logon_admin -w senha objectClass=ncpServer dn`

   Por exemplo:
   `ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn`

3. Abra o arquivo novell_ims8.ldif.
4. Substitua cada variável de NCPServer pelo valor encontrado na Etapa 2.

   O local padrão para novell_ims8.ldif no Windows é:

   <caminho_de_instalação>\tools\policystore-schemas\NovelleDirectory

   Por exemplo, se o valor DN for cn=servername,o=servercontainer, você substituirá cada instância do *NCPServer* por cn=servername,o=servercontainer.

5. Atualize o eDirectory Server com o arquivo novell_ims8.ldif.

   Consulte a documentação do Novell eDirectory para obter instruções.

Configurar o Oracle Internet Directory (OID)

Para configurar um Oracle Internet Directory, atualize o arquivo ldif oracleoid.

Siga estas etapas:

1. Configure o diretório como um repositório de políticas suportado do SiteMinder.

   Observação: para obter instruções de configuração, consulte o *Guia de Instalação do Servidor de políticas do CA SiteMinder*.

2. Atualize o Servidor do Oracle Internet Directory com o arquivo oracleoid_ims8.ldif. O local de instalação padrão para esse arquivo no Windows é:

   caminho_de_instalação\policystore-schemas\OracleOID\

   Consulte a documentação do Oracle Internet Directory para obter instruções.

Verificar o repositório de políticas

Para verificar o repositório de políticas, confirme os pontos a seguir:

- O log do Servidor de políticas não contém uma seção de avisos que comece com o seguinte código:
  `*** IMS NO SCHEMA BEGIN`

  Esse aviso será exibido apenas se você tiver instalado as Extensões para o Servidor de políticas do SiteMinder, mas você não estendeu o esquema do repositório de políticas.

- Os objetos do CA Identity Manager existem no banco de dados ou no diretório do repositório de políticas. Os objetos do CA Identity Manager começam com um prefixo ims.

Importar o esquema do CA Identity Manager no repositório de políticas

O administrador de políticas importa o esquema do CA Identity Manager no repositório de políticas. Essa tarefa permite que o CA Identity Manager crie, atualize e exclua objetos de política. Os exemplos incluem objetos de diretórios, domínios, realms, regras, políticas e os objetos de política que permitem funções e tarefas de acesso.

Siga estas etapas:

1. No Servidor de políticas do SiteMinder, encerre o serviço do Servidor de políticas.
2. Execute o instalador do CA Identity Manager para a versão que você está usando.
3. Quando for perguntado quais componentes serão instalados, selecione as Extensões do SiteMinder (se SiteMinder estiver instalado localmente).
4. Verifique se o serviço do Servidor de políticas é reiniciado antes de continuar.

Criar um objeto de agente do SiteMinder 4.X

O administrador de políticas cria um Agente web do SiteMinder 4.x. Essa tarefa permite a comunicação entre o SiteMinder e o CA Identity Manager. O administrador de identidades faz referência a esse agente durante a configuração do CA Identity Manager.

Siga estas etapas:

1. Efetue logon na Interface de usuário administrativa do SiteMinder.

   As guias relevantes para seus privilégios de administrador são exibidas.
2. Clique em Infraestrutura, Agentes, Agente, Criar agente.

   A caixa de diálogo Criar agente é exibida.
3. Selecione Criar um objeto do tipo Agente e clique em OK.

   A caixa de diálogo Criar agente é exibida.
4. Insira um nome e uma descrição opcional.

   Observação: use um nome que você possa associar facilmente ao Assistente para Conexão do SharePoint correspondente.

5. Selecione SiteMinder.
6. Selecione Agente web na lista suspensa.
7. Ative a funcionalidade 4.x com as seguintes etapas:
   a. Marque a caixa de seleção Oferece suporte a agentes 4.x.

      Os campos de configurações confiáveis são exibidos.

   b. Adicione as configurações confiáveis preenchendo os seguintes campos:

      Endereço IP

      Especifica o endereço IP do Servidor de políticas.

      Shared Secret

      Especifica uma senha que é associada ao objeto de agente 4.x. O Assistente para Conexão do SharePoint também exige essa senha.

      Confirmar segredo

      Confirma uma senha que é associada ao objeto de agente 4.x. O Assistente para Conexão do SharePoint também exige a confirmação dessa senha.
8. Clique em Submit.

   A tarefa Criar objeto de agente é enviada para processamento e a mensagem de confirmação é exibida.

Exportar os diretórios e ambientes do CA Identity Manager

O processo de integração remove todas as definições atuais de ambiente e diretório. Para ajudar a garantir que as informações sejam mantidas, o administrador de identidades exporta os ambientes usando o Management Console do CA Identity Manager. Depois de concluir a integração, essas definições restauram os diretórios e ambientes.

Siga estas etapas:

1. Abra o Management Console do CA Identity Manager.
2. Clique em Diretórios.
3. Clique no primeiro diretório da lista e clique em Export.
4. Salve e arquive o arquivo xml de diretório.
5. Repita esse processo para os demais diretórios.
6. Clique em Home e em Environments.
7. Selecione o primeiro ambiente.
8. Clique em Exportar.
9. Repita esse processo para os demais ambientes.

   Observação: esse processo pode levar alguns minutos para cada ambiente.

Excluir todas as definições de diretório e ambiente

De modo a preparar o SiteMinder para proteger o CA Identity Manager, o administrador de identidades exclui as definições de diretório e a ambiente usando o Management Console do CA Identity Manager.

Siga estas etapas:

1. Abra o Management Console do CA Identity Manager.
2. Clique em Ambientes.
3. Selecione o primeiro ambiente
4. Clique em Excluir.
5. Repita esse processo para cada um dos ambientes restantes.

   Observação: exclua os ambientes antes de excluir os diretórios, pois os ambientes fazem referência a diretórios.
6. Navegue de volta para a seção Directories.
7. Selecione todos os diretórios listados.
8. Clique em Excluir.

Ativar o adaptador de recursos do Servidor de políticas do SiteMinder

O administrador de identidades ativa o adaptador de recursos do Servidor de políticas do SiteMinder. A finalidade do adaptador é validar o cookie SMSESSION. Após a validação, o SiteMinder cria o contexto de usuário.

Siga estas etapas:

1. Navegue até a pasta \policysever.rar\META-INF localizada dentro de iam_im.ear no servidor de aplicativos que está executando o CA Identity Manager.
2. Abra o arquivo ra.xml em um editor.
3. Procure Enabled config-property e altere o config-property-value para true, conforme mostrado no exemplo a seguir:

```
        <config-property-name>validateSmHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. Localize a propriedade ConnectionURL e forneça o nome do host do Servidor de política do SiteMinder. Usar um FQDN (Fully Qualified Domain Name - nome de domínio totalmente qualificado).
5. Localize a propriedade UserName e especifique a conta que deverá ser usada para comunicação com o SiteMinder. O SiteMinder é o valor padrão para essa conta.
6. Localize a propriedade AdminSecret. Forneça a senha criptografada. Copie a senha do arquivo directory.xml que você exportou e cole-a no ra.xml. Se você não tiver certeza se tem uma senha comum, criptografe sua senha usando a Ferramenta de senha do CA Identity Manager.
7. Cole a senha criptografada no arquivo ra.xml.
8. Especifique o nome do agente 4.x que o administrador de políticas criou durante a configuração do SiteMinder.
9. Especifique a senha criptografada. Use a Ferramenta de senha para criptografar a senha, se necessário.
10. Salve as alterações no arquivo ra.xml.

O adaptador de recursos do Servidor de políticas do SiteMinder é ativado.

Mais informações:

Modificar uma senha ou um shared secret do SiteMinder (na página 376)

Desativar o Filtro de autenticação de estrutura nativo do CA Identity Manager

Com o adaptador do SiteMinder definido, o Filtro de autenticação de estrutura não é mais necessário. O administrador de identidades pode desativar o filtro.

Siga estas etapas:

1. Localize e edite o arquivo web.xml na pasta \user_console.war\WEB-INF no iam_im.ear.
2. Localize o FrameworkAuthFilter e altere o valor de Enable init-param para false.

   Se você estiver usando o CA Identity Manager r12.5 SP7 ou posterior, verifique se os arquivos Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files (JCE) são baixados em \<caminho_Java>\<versão_jdk>\jre\lib\security no ambiente do CA Identity Manager. Esses arquivos permitem que o CA Identity Manager se conecte ao SiteMinder.

   Se as bibliotecas JCE forem instaladas, você verá as seguintes mensagens durante a inicialização do aplicativo CA Identity Manager:

   ```
   2012-07-06 11:23:56.079 WARN  [ims.default] (main) * Startup Step 2 :
   Attempting to start PolicyServerService
   2012-07-06 11:23:56.081 WARN  [ims.default] (main) Unlimited Strength Java
   Crypto Extensions enabled: TRUE
   ```

   Caso contrário, o valor será false para a entrada "Unlimited Strength Java Crypto Extensions enabled". O CA Identity Manager falha ao se conectar ao Servidor de políticas.

Reiniciar o servidor de aplicativos

O reinício atualiza o servidor de aplicativos com as alterações. O administrador de identidades confirma que a alternância foi bem-sucedida e que há uma conexão adequada com o Servidor de políticas do SiteMinder.

Siga estas etapas:

1. Use o painel de serviços para reiniciar o CA Identity Manager quando o servidor de aplicativos estiver sendo executado como um serviço.
2. Consulte server.log para validar a conexão

Configurar uma origem de dados para o SiteMinder

Se o ambiente do CA Identity Manager usa um banco de dados relacional para seu repositório de identidades, o administrador de identidades precisará concluir um processo adicional no Servidor de políticas do SiteMinder. O SiteMinder exige uma origem de dados local para se comunicar com o banco de dados.

Siga estas etapas:

1. Em servidores Windows, abra o console do Administrador de Fonte de Dados ODBC, que é encontrado em Ferramentas Administrativas.
2. Clique na guia DSN de sistema.
3. Clique em Adicionar e selecione o driver do SiteMinder correspondente para seu banco de dados.
4. Forneça as informações necessárias para fazer referência ao repositório de usuários do banco de dados relacional.
5. Teste a conectividade antes de continuar.

Importar as definições de diretório

Para se preparar para a importação de ambientes, o administrador de identidades importa os diretórios aos quais os ambientes fazem referência. Importar a definição de diretório no CA Identity Manager também adiciona as informações de diretório ao repositório de políticas do SiteMinder.

Siga estas etapas:

1. Certifique-se de que o CA Identity Manager esteja em execução e conectado ao SiteMinder.
2. Navegue até o Management Console do CA Identity Manager.
3. Clique em Directories e em Create or Update from XML.
4. Selecione seu arquivo de configuração de diretório (directory.xml). Esse é o arquivo que você exportou em Exportar os diretórios e ambientes do CA Identity Manager (na página 318).
5. Clique em Avançar.
6. Clique em Finish e analise a saída do carregamento. Verifique se o diretório está presente no CA Identity Manager e no SiteMinder.
7. Repita essas etapas para o Repositório de provisionamento e todos os demais diretórios.
8. Efetue logon na Interface de usuário administrativa do SiteMinder para validar a criação de diretórios de usuário.

Atualizar e importar as definições de ambiente

O administrador de identidades importa os ambientes atualizados de volta no CA Identity Manager.

Siga estas etapas:

1. Diferentemente das exportações de diretório, a exportação do ambiente está na forma de um arquivo zip. Arraste uma cópia do arquivo *name*.xml para fora do arquivo zip.
2. Copie o arquivo *name*.xml. Insira uma referência ao agente de proteção (não ao agente do SM 4.x) no fim do elemento ImsEnvironment, antes do sinal de fechamento />: *agent="idmadmin"*
3. Salve e cole o arquivo de volta no arquivo zip.
4. Abra o Management Console do CA Identity Manager, clique em Environments e em Import.
5. Insira o nome do arquivo zip do ambiente atualizado.
6. Clique em Finish e analise a saída da importação.
7. Repita esse processo para todos os ambientes restantes.
8. Reinicie o servidor de aplicativos.

Instalar o plugin do servidor proxy web

Com base no aplicativo instalado, o administrador de identidades instala um dos seguintes plugins que o servidor web usa para encaminhar solicitações ao servidor de aplicativos:

- WebSphere (na página 324)
- JBoss (na página 331)
- WebLogic (na página 335)

Instalar o plugin de proxy no WebSphere

O servidor web no qual você instalou o agente web encaminha solicitações ao servidor de aplicativos que hospeda o servidor do CA Identity Manager. O plugin de proxy do servidor web concedido pelo fornecedor proporciona esse serviço.

Use os procedimentos que são aplicáveis à sua implantação:

1. Configurar o servidor HTTP do IBM (na página 324) (todos os servidores web)
2. Configurar o plugin de proxy (na página 325) (todos os servidores web)
3. Execute uma destas ações:
   - Concluir a configuração no IIS (na página 328)
   - Concluir a configuração no iPlanet ou Apache (na página 330)

Configurar o servidor HTTP do IBM

Para todos os servidores web, instale o plugin de proxy e use o comando configurewebserver.

Siga estas etapas:

1. Instale o plugin de proxy do WebSphere Launch Pad.
2. Adicione o servidor web à célula do WebSphere executando o comando configurewebserver1.bat da seguinte maneira:
   a. Edite *base_do_websphere*\Plugins\bin\configurewebserver1.bat/,sh em um editor de texto.
   b. Adicione um nome de usuário e uma senha depois de wsadmin.bat/.sh, como se segue:
   ```
   wsadmin.bat -user wsadmin -password senha -f
   configureWebserverDefinition.jacl
   ```
   c. Execute configurewebserver1,bat/.sh.

   Observação: consulte a documentação do IBM WebSphere para obter mais informações sobre o comando configurewebserver.
3. Continue o procedimento para Configurar o plugin de proxy (na página 325).

Configurar o plugin de proxy

Em todos os servidores web, atualize o plugin usando o comando GenPluginCfg do WebSphere:

Siga estas etapas:

1. Efetue logon no sistema onde o WebSphere está instalado.
2. Na linha de comando, navegue até *base_do_websphere*\bin, onde *base_do_websphere* é o local de instalação do WebSphere.

   Por exemplo:

   - **Windows:**

     C:\Arquivos de programas\WebSphere\AppServer\profile\AppSrv01\bin

   - **UNIX:**

     /*dir_início*/WebSphere/AppServer/profile/AppSrv01/bin

3. Execute o comando GenPluginCfg.bat ou GenPluginCfg.sh.

   A execução desse comando gera um arquivo plugin-cfg.xml no seguinte local:

   base_do_websphere\AppServer\profiles\AppSrv01\config\cells

4. Continue com um dos seguintes procedimentos:

   - Concluir a configuração no IIS (na página 328)
   - Concluir a configuração no iPlanet ou Apache (na página 330)

Concluir a configuração no IIS (7.x)

Antes de iniciar este procedimento, verifique se você está usando uma versão 6.1.0.9 ou mais recente do plugin do servidor web. As versões anteriores do plugin não oferecem suporte ao sistema operacional Windows Server 2008.

Siga estas etapas:

1. Instale o IIS versão 7.x com os componentes de Compatibilidade com gerenciamento do IIS versão 6.0. Os componentes de Compatibilidade com Gerenciamento do IIS versão 6.0 não são instalados por padrão.
2. Execute as etapas a seguir para abrir a janela Gerenciador de Servidor no Windows Server 2008:
    1. Clique em Iniciar, Ferramentas Administrativas, Gerenciadores de Servidores.
    2. Clique em Ação, Adicionar Funções e clique em Avançar.
    3. Selecione a função Servidor Web (IIS) na página Selecionar Funções do Servidor e clique em Avançar.
    4. Clique em Adicionar Recurso, Avançar, quando um prompt para o recurso Serviço de Ativação de Processos do Windows for exibido
    5. Clique em Avançar na página de introdução do IIS.
3. Quando a janela Serviços de Função for exibida, verifique se as opções a seguir estão selecionadas, além das opções padrão que já estão selecionadas.
    - Serviços de Informações da Internet: Ferramentas de Gerenciamento
    - Compatibilidade com Gerenciamento do IIS versão 6.0: Console de Gerenciamento do IIS versão 6.0, Ferramentas de Script do IIS versão 6.0, Compatibilidade com VMI do IIS versão 6.0 e Compatibilidade de Metabase do IIS
    - Desenvolvimento de Aplicativos: Extensões ISAPI, Filtros ISAPI
4. Clique em Avançar para ativar as opções selecionadas e clique em Instalar na próxima janela para executar a instalação.
5. Clique em Fechar na janela Resultados da Instalação quando a instalação for concluída.
6. Abra o prompt de comando e vá para: \Arquivos de Programas\IBM\WebSphere\AppServer\profiles\Dmgr01\bin.
7. Execute este comando: GenPluginCfg.bat.

   O arquivo plugin-cfg.xml será gerado neste local C:\Arquivos de Programas\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells.
8. Crie um diretório em c:\, por exemplo, c:\plugin.
9. Copie o arquivo plugin-cfg.xml no diretório c:\plugin.

10. Copie o arquivo iisWASPlugin_http.dll no diretório c:\plugin.
11. Selecione Iniciar, Todos os Programas, Ferramentas Administrativas, Gerenciador do Serviços de Informações da Internet (IIS) em um sistema operacional Windows Server 2008. Essa ação inicia o aplicativo IIS e cria um novo diretório virtual para a instância do Site. Essas instruções pressupõem que você esteja usando o Site Padrão.
12. Expanda a árvore da esquerda até ver Site Padrão.
13. Clique com o botão direito do mouse em Site Padrão,Adicionar Diretório Virtual para criar o diretório com uma instalação padrão.
14. Insira setPlugins no campo Alias na janela Alias do Diretório Virtual do Assistente para Criação de Diretório Virtual.
15. Navegue para o diretório c:\plugin no campo Caminho Físico da janela Diretório de Conteúdo do Site do assistente e clique em OK.
16. Clique no botão Configurações de teste. Se o teste de configurações falhar, você poderá alterar as permissões do diretório físico. Se preferir, selecione Conectar como e permita que o IIS se conecte como uma conta de usuário do Windows que tenha autoridade para arquivos nesse caminho físico.
17. Clique em OK para adicionar o diretório virtual setPlugins ao seu site.
18. Selecione o diretório virtual setPlugins que você acabou de criar na árvore de navegação.
19. Clique duas vezes em Mapeamentos de Manipulador e clique em Editar Permissões de Recurso no painel Ações.
20. Selecione Script e Executar, se ainda não estiverem selecionados.
21. Clique em OK.
22. Retorne à janela Gerenciador do IIS e expanda a pasta Sites na árvore de navegação à esquerda da janela.
23. Selecione Site Padrão na árvore de navegação.
24. Conclua as etapas a seguir no painel Propriedades do Site Padrão para adicionar o filtro ISAPI:
    1. Clique duas vezes na guia Filtros ISAPI.
    2. Clique para abrir a caixa de diálogo Adicionar/Editar Propriedades do Filtro.
    3. Insira iisWASPlugin no campo Nome do filtro.
    4. Clique em Procurar para selecionar o arquivo plugin localizado no diretório c:\plugin\iisWASPlugin_http.dll.
    5. Clique em OK para fechar a caixa de diálogo Adicionar/Editar Propriedades do Filtro.
25. Selecione o nó do servidor de nível superior na árvore de navegação.

26. Clique duas vezes em Restrições ISAPI e CGI no painel Recursos.

    Para determinar o valor a ser especificado para a propriedade do Caminho ISAPI ou CGI , procure e selecione o mesmo plugin que você selecionou na etapa anterior. Por exemplo: c:\plugin\iisWASPlugin_http.dll.

27. Clique em Adicionar no painel Ações.

28. Insira WASPlugin no campo Descrição , selecione Permitir que o caminho da extensão seja executado e clique em OK para fechar a janela da caixa de diálogo Restrições ISAPI e CGI .

29. Crie o novo arquivo plugin-cfg.loc no local c:\plugin. Defina o valor no arquivo plugin-cfg.loc para o local do arquivo de configuração. O local padrão é C:\plugin\plugin-cfg.xml.

Atualizar o agente web

Após configurar o IIS 7.x, faça as seguintes alterações no agente web:

1. Clique em Pools de aplicativos e altere Pool de Aplicativos Padrão para o modo Clássico.
2. Clique em Enviar.
3. Certifique-se de que o agente esteja mais no topo da lista de prioridade de filtros ISAPI do que o plugin para o servidor de aplicativos usado pelo CA Identity Manager.
4. Reinicie o IIS versão 7.x e seu perfil do Servidor de aplicativos do WebSphere.

Concluir a configuração no IIS

Depois de configurar o servidor HTTP do IBM e o plugin de proxy, certifique-se de que plugin-cfg.xml do proxy esteja no local certo e execute as etapas para configurar um arquivo plugin adicional.

Siga estas etapas:

1. Copie o plugin-cfg.xml da seguinte maneira:
   a. Efetue logon no sistema onde o agente web está instalado.
   b. Crie uma pasta sem espaços na unidade C:. Por exemplo: C:\plugin.
   c. Copie o arquivo plugin-cfg.xml na pasta c:\plugin.
2. Crie um arquivo chamado plugin-cfg.loc na pasta C:\plugin e adicione a seguinte linha no arquivo:

   C:\plugin\plugin-cfg.xml

3. Faça download do instalador do Plugin do WebSphere, em www.ibm.com, no sistema onde o WebSphere está instalado.
4. Vá até o local do instalador do Plugin do WebSphere.
5. Gere o arquivo iisWASPlugin_http.dll usando este comando:

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   Responda às perguntas apresentadas de acordo com a sua configuração.

   Quando o assistente terminar, o arquivo iisWASPlugin_http.dll será salvo na pasta C:\IBM\WebSphere\Plugs\bin. Procure uma subpasta de 32 bits de 64 bits.
6. Copie o arquivo iisWASPlugin_http.dll na pasta C:\plugin no sistema com o agente web.
7. Crie um diretório virtual, como se segue:
   a. Abra o Gerenciador do IIS.
   b. Clique com o botão direito do mouse em Sites Padrão.
   c. Clique em Novo diretório virtual e forneça estes valores:

      Alias: sePlugins (diferencia maiúsculas de minúsculas.)

      Caminho: c:\plugin

      Permissão: Ler + Executar (ISAPI ou CGI)
8. Adicione um filtro ISAPI da seguinte maneira:
   a. Clique com o botão direito do mouse em Site Padrão.
   b. Clique em Propriedades.
   c. Clique em Adicionar na guia Filtro ISAPI.
   d. Forneça estes valores:

      Nome do filtro: sePlugins

      Executável: c:\plugin\ iisWASPlugin_http.dll
9. Crie uma extensão de serviço web, como segue:
   a. No Gerenciador do IIS6, expanda o nome do computador.
   b. Crie uma extensão de serviço web e a defina como permitida.

      Nome da extensão: WASPlugin

      Caminho: C:\plugin\ iisWASPlugin_http.dll
   c. Clique com o botão direito em cada extensão de serviço web para alterá-la para o status Permitido.

10. Reinicie o servidor web do IIS.

    No serviços WWW mestre, verifique se o plugin do WebSphere (sePlugin) é exibido após o plugin do agente web do SiteMinder e que o plugin do WebSphere foi iniciado com êxito.

Concluir a configuração no iPlanet ou Apache

Depois de configurar o servidor HTTP do IBM e o plugin de proxy, certifique-se de que plugin-cfg.xml do proxy esteja no local certo e reinicie o servidor web.

Siga estas etapas:

1. Copie o plugin-cfg.xml no sistema em que você instalou o plugin de proxy, no seguinte local:

   base_do_websphere\AppServer\profiles*nome_do_servidor*\config\cells*célula_do_websphere*\nodes\webserver1_node\servers\webserver1\

2. Certifique-se de que o plugin do WebSphere (libns41_http.so) seja carregado depois do plugin do Agent web (NSAPIWebAgent.so) do SiteMinder em todos os servidores web iPlanet.

3. Verifique a ordem dos plugins em *base_do_iplanet*/https-*instância*/config/magnus.conf para Servidores web do IPlanet 6.0.

4. Copie as seguintes linhas de *base_do_iplanet*/https-*instância*/config/magnus.conf em *base_do_iplanet*/https-*instância*/config/obj.conf (Servidores web do IPlanet 5.x):

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/plugin-cfg.xml"
   ```

   Adicione o código a seguir após AuthTrans fn="SiteMinderAgent" no arquivo obj.conf:

   ```
   Service fn="as_handler"
   ```

5. Certifique-se de que o plugin do Agente web (mod2_sm.so) do SiteMinder esteja carregado antes do plugin do WebSphere (mod_ibm_app_server_http.so) nos Servidores web Apache. Esse comando está na seção Suporte ao DSO (Dynamic Shared Object) de *base_do_apache*/config/httpd.conf.

6. Reinicie o servidor web.

Instalar o plugin de proxy do JBoss

Depois que o agente web do SiteMinder autentica e autoriza uma solicitação para um recurso do CA Identity Manager, o servidor web encaminha a solicitação ao servidor de aplicativos que hospeda o servidor do CA Identity Manager. Para transferir essas solicitações, instale e configure um Conector JK no sistema onde o Agente web do SiteMinder está instalado. Consulte o site do Projeto Jakarta a seguir para obter mais informações sobre o Conector JK:

http://community.jboss.org/wiki/usingmodjk12withjboss

As Ferramentas administrativas do CA Identity Manager incluem arquivos de configuração de amostra que podem ser usados para configurar o Conector JK. Para obter instruções, consulte o arquivo readme.txt no diretório indicado na seguinte tabela:

Plataforma	Local
Servidor web do IIS em um sistema Windows	<caminho_de_instalação>\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Servidor web do Sun Java System em um sistema Solaris	<caminho_de_instalação2>/tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Servidor web do Apache em um sistema Solaris	<caminho_de_instalação2>/tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

Instalar e configurar um plugin do aplicativo JBoss (IIS 7.x)

Este procedimento descreve a configuração do Plugin do JBoss Apache a partir do IIS 7.0

Siga estas etapas:

1. Implante e atualize os filtros ISAPI no Sistema de Arquivos.

   Implante a pasta ISAPI na raiz da unidade C.

2. Edite o arquivo jakarta.reg localizado na pasta descompactada.

   Se você colocou a pasta ISAPI na raiz de C:\, não altere esse arquivo. Se a colocou em outra pasta, especifique essa pasta nas linhas 9, 11 e 12.

3. Salve as alterações e clique duas vezes para atualizar o Registro.

4. Edite o arquivo workers.properties especificando o local de seu servidor de aplicativos JBoss. A porta e tipo não precisam ser alterados.

5. Instale o IIS7 ou IIS7.5 no Windows 2008.

6. Abra o Gerente do sistema e verifique se a Extensão ISAPI e o filtro ISAPI do IIS estão instalados.
7. Inicie inetmgr na janela Executar.
8. Selecione o nome m/c e clique duas vezes na Restrições ISAPI e CGI.
9. Clique no botão Adicionar no lado direito do painel.
10. A janela Adicionar Restrições ISAPI ou CGI é exibida.
11. Selecione isapi_redirect.dll e insira a descrição como ISAPI.
12. Selecione Permitir que o caminho de extensão seja executado.
13. Clique em OK na janela Adicionar restrições ISAPI ou CGI.
14. Expanda Sites na seção Conexão, selecione o Site Padrão e clique com o botão direito do mouse em Adicionar Diretório Virtual.
15. Insira o alias como "jakarta" e insira o local do arquivo isap_redirect.dll (c:\ajp) no caminho físico.
16. Clique no botão Configurações de teste:
    - Se a autenticação e a autorização foram aprovadas, clique em OK.
    - Se houver falha de autorização, clique no botão Conectar como.
17. Selecione o usuário específico e forneça o nome de usuário e a senha do administrador.
18. Clique novamente no botão Configurações de teste. Dessa vez a autorização foi aprovada.
19. Clique no Site Padrão à esquerda e clique duas vezes no filtro ISAPI.
20. Clique no botão Adicionar no lado direito do painel.
21. Insira o nome e forneça o local do arquivo isapi_redirect.dll.
22. Clique em OK.
23. Expanda o Site Padrão e clique no diretório virtual jakarta.
24. Clique duas vezes no Mapeamento do Manipulador.
25. Selecione o ISAPI-dll e clique em Editar Permissão do Recurso.

26. Verifique se todas as permissões (Leitura, Script, Execução) estão selecionadas.
27. Clique em OK.

Atualizar o agente web

Após configurar o IIS 7.x, faça as seguintes alterações no agente web:

1. Clique em Pools de aplicativos e altere Pool de Aplicativos Padrão para o modo Clássico.
2. Clique em Enviar.
3. Certifique-se de que o agente esteja mais no topo da lista de prioridade de filtros ISAPI do que o plugin para o servidor de aplicativos usado pelo CA Identity Manager.

O plugin do JBoss está configurado.

Instalar e configurar um plugin do aplicativo JBoss (IIS 6.0)

Essa integração supõe que o SiteMinder autentica e autoriza um usuário antes de chegar ao CA Identity Manager. É necessário que um usuário tenha um cookie SMSESSION para chegar ao CA Identity Manager. Use um plugin de aplicativo (redirecionamento de proxy) protegido por um Agente web do SiteMinder. Com essa configuração, um usuário é autenticado pelo SiteMinder e redirecionado para o CA Identity Manager depois que um cookie SMSESSION tiver sido criado.

Este procedimento é para a implantação e configuração do Plugin do JBoss Apache para o IIS 6.0:

Siga estas etapas:

1. Implante e atualize o filtro ISAPI no Sistema de Arquivos.

   Certifique-se de implantar a pasta ISAPI na raiz da unidade C.

2. Edite o arquivo jakarta.reg localizado na pasta descompactada.

   Se você colocou a pasta ISAPI na raiz de C:\, não altere esse arquivo. Se a colocar em outra pasta, especifique essa pasta nas linhas 9, 11 e 12.

3. Salve as alterações e clique duas vezes para atualizar o Registro.
4. Edite o arquivo workers.properties especificando o local de seu servidor de aplicativos JBoss. A porta e tipo não precisam ser alterados.
5. Implante o filtro ISAPI no IIS.
6. Abra o Gerenciador de Serviços de Informações da Internet em Ferramentas Administrativas.
7. Expanda os níveis até que o Site Padrão esteja visível. Clique com o botão direito do mouse e selecione Novo, Diretório Virtual.

8. Insira *jakarta* como o alias.
9. Faça referência ao caminho em que você instalou o plugin ISAPI.
10. Selecione Ler, Executar scripts (como ASP) e Executar (como aplicativos ISAPI ou CGI).
11. Clique em Avançar para continuar e finalizar o assistente.
12. Clique com o botão direito do mouse no Site Padrão e selecione Propriedades, selecione a guia Filtros ISAPI e clique em Adicionar.
13. Insira *jakarta* para o nome do filtro e clique em procurar para selecionar o isapi_redirect.dll. Clique em OK duas vezes.
14. Para o IIS 6.0, ative este filtro nas Extensões de serviço web.
15. Selecione a pasta Extensões de serviço web. Clique no link azul à esquerda para Adicionar uma nova extensão de serviço web.
16. Forneça Jakarta-Tomcat para o nome. Clique em Adicionar e procure o mesmo dll acima. Clique em OK. Clique em Definir status da extensão como permitido e clique em OK.
17. Reinicie o Servidor do IIS.

Agora, com o proxy definido, você pode acessar o CA Identity Manager pelo IIS. Por exemplo, aqui estão os links para acessar o CA Identity Manager antes e depois da configuração de proxy:

Antes

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

Depois

http://smserver.forwardinc/idmmanage http://smserver.forwardinc/idmmanage

Observação: uma barra "/" pode ser necessária no fim desse URL para que o proxy funcione. Faça referência aos logs do proxy se você não tiver sido encaminhado para o Management Console.

Instalar o plugin de proxy no WebLogic

Depois que o Agente web autentica e autoriza uma solicitação para um recurso do CA Identity Manager, o Servidor web encaminha a solicitação ao servidor de aplicativos que hospeda o Servidor do CA Identity Manager.

1. Instale o plugin de proxy do WebLogic para seu Servidor web, conforme descrito na documentação do WebLogic.

   Observação: para os usuários do IIS, ao instalar o plugin de proxy, certifique-se de configurar o proxy por extensão de arquivo e por caminho. Quando você configura o proxy por extensão de arquivo, adicione um mapeamento de aplicativos na guia Mapeamento de Aplicativo com as seguintes propriedades:
   Executável: IISProxy.dll
   Extensão: .wlforward

2. Configure o plugin de proxy para o CA Identity Manager, conforme descrito em uma das seções a seguir:

   - Plugin de proxy do IIS (na página 338)
   - Plugin de proxy do iPlanet (na página 339)
   - Plugin de proxy do Apache (na página 342)

Configurar o plugin de proxy para IIS (7.x)

O procedimento a seguir explora a implantação e a configuração do plugin de proxy do WebLogic para o IIS 7.x.

Observação: essas instruções são para ambientes operacionais de 32 bits. As mesmas instruções se aplicam a ambientes operacionais de 64 bits. O local da instalação do arquivo .dll é diferente:

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

Siga estas etapas:

1. Instale o Agente web e configure-o no IIS7.
2. Crie uma pasta com o nome plugin na unidade C.
3. Copie os arquivos a seguir na pasta plugin:

   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   Você pode encontrar esses arquivos em \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7.

4. Instale os serviços de função Ferramentas de Desenvolvimento e Gerenciamento de Aplicativos no IIS7.
5. Abra Gerenciador Inet e selecione o Site Padrão.
6. Clique em Mapeamentos de Manipulador.
7. Clique duas vezes no Arquivo Estático e modifique o caminho da Solicitação para *.*.
8. Clique no botão Restrições da Solicitação.
9. Na guia Mapeamentos, selecione Invocar manipulador somente se a solicitação estiver mapeada para um arquivo ou uma pasta.
10. Na caixa de diálogo Mapeamentos de Manipulador, clique em Adicionar Mapeamento de Script... nas opções de menu do lado direito. Insira os seguintes valores:
    - Caminho da solicitação : *
    - Executável: iisProxy.dll
    - Nome: proxy
11. Clique no botão Restrições da Solicitação.
12. Limpe Invocar manipulador somente se a solicitação estiver mapeada para.
13. Clique em Sim para o prompt sobre permitir essa extensão IASPI.
14. Clique no nó Raiz (Nome da máquina) da árvore do Gerenciador do IIS e clique em Restrições ISAPI e CGI.
15. Clique em Adicionar no painel Ações e insira os valores a seguir:
    - Caminho ISAPI ou CGI: C:\plugin\ iisproxy.dll.
    - Descrição: Weblogic
    - Selecione Permitir que o caminho de extensão seja executado.
16. Clique no nó Raiz (Nome da máquina) da árvore do Gerenciador do IIS e clique nas Restrições ISAPI e CGI. Selecione a opção Weblogic e clique em Editar configurações de recurso no painel direito.
17. Selecione Permitir módulos ISAPI não especificados e Permitir módulos CGI não especificados.
18. Faça o mesmo para o Agente web.
19. Em Exibição de Recursos, no Site Padrão, clique duas vezes em Mapeamentos de Manipulador.

20. Na página Mapeamentos de Manipulador, no painel Ações, clique em Adicionar Mapeamento de Script e insira os seguintes valores:
    - Caminho de solicitação: .jsp
    - Executável: iisproxy.dll
    - Nome: JSP
21. Clique em Restrições de solicitação.
22. Na guia Mapeamento selecione Invocar manipulador somente se a solicitação estiver mapeada para Arquivo.
23. Clique em OK.
24. Clique em Adicionar Mapeamento de Script e insira os seguintes valores:
    - Caminho da solicitação: .do
    - Executável : C:\plugin\iisproxy.dll
25. Clique em Restrições de solicitação. As configurações são as mesmas para .jsp.
26. Clique em OK.
27. Clique em Adicionar Mapeamento de Script e insira os seguintes valores:
    - Caminho da solicitação : .wlforward
    - Executável : C:\plugin\iisproxy.dll
28. Clique em Restrições de solicitação. As configurações são as mesmas para .jsp.
29. Clique em Site Padrão e clique duas vezes em Filtros ISAPI.
30. Clique em Exibir Lista de Solicitações no painel direito.
31. Coloque o executável do Agente do SiteMinder em segundo lugar na lista. Depois dessa entrada, somente o executável do Weblogic estará na lista.

    Observação: se o executável do Agente do SiteMinder for exibido após o executável do Weblogic, mova o Agente do SiteMinder usando a ação MOVE UP.
32. Clique em Pools de aplicativos e altere Pool de Aplicativos Padrão para o modo Clássico.

O plugin do WebLogic está configurado.

(WL)Configurar o plugin de proxy do IIS 6.0

Este procedimento se aplica às configurações do plugin de proxy do WebLogic para o IIS 6.0.x:

Siga estas etapas:

1. Crie uma pasta no sistema onde o agente web está instalado. Por exemplo: c:\weblogic_proxy.
2. Efetue logon no sistema em que o servidor do CA Identity Manager está em execução.
3. Vá para esta pasta: *base_do_Weblogic*\wlserver_11\server\plugin
4. Copie os seguintes arquivos na pasta de proxy do weblogic criado na etapa 1.
   - iisforward.dll
   - iisproxy.dll
5. Crie um arquivo chamado iisproxy.ini na mesma pasta e inclua o seguinte conteúdo:

   ```
   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.
   WebLogicHost=nome-do-host
   WebLogicPort=7001
   ConnectTimeoutSecs=20
   ConnectRetrySecs=2
   WlForwardPath=/castylesr5.1.1,/iam,/im, /ca/Odata/
   WLLogFile= c:\weblogic_proxy \proxy.log
   DebugConfigInfo=ON
   ```

   Substitua *nome-do-host* pelo nome do host real.
6. Inicie o Gerenciador do IIS.
7. Expanda Sites.
8. Clique com o botão direito do mouse em Site Padrão.
9. Selecione Propriedades.
10. Adicione um filtro da seguinte maneira:
    a. Clique em Filtros ISAPI.
    b. Clique em Adicionar e preencha a caixa de diálogo da seguinte forma:

       Para Nome do Filtro: WebLogic

       Para Executável: Caminho do iisforward.dll

11. Forneça o local do arquivo iisproxy.dll como se segue:
    a. Clique em Diretório Base.
    b. Clique em Configuração.
    c. Clique em Adicionar.
    d. Insira o caminho do arquivo iisproxy.dll.
    e. Insira .jsp no campo Extensão.
    f. Desmarque a opção Verificar se o arquivo existe.
12. Repita a etapa 11 para as extensões .do e .wlforward.
13. Adicione uma extensão de serviço web para wlforward (tudo em letras minúsculas) apontando para o local de iisforward.dll.

    Defina o status da extensão como Permitido.
14. Clique com o botão direito em cada extensão de serviço web para alterá-la para o status Permitido.
15. Reinicie o servidor web do IIS.

Configurar o plugin de proxy do iPlanet

Para configurar o plugin, modifique os arquivos de configuração do iPlanet a seguir:

- magnus.conf
- obj.conf

Os arquivos de configuração do iPlanet têm regras rígidas quanto ao posicionamento de texto. Para evitar problemas, observe os seguintes pontos:

- Elimine espaços em branco irrelevantes à esquerda e à direita. Espaços extras em branco podem causar falhas no servidor do iPlanet.
- Se você precisar inserir mais caracteres do que é possível em uma única linha, coloque uma barra invertida (\) no fim da linha e continue digitando na linha seguinte. A barra invertida acrescenta diretamente o fim da primeira linha ao início da próxima linha. Se for necessário um espaço entre as palavras ao fim da primeira linha e no início da segunda linha, use um espaço no fim da primeira linha (antes da barra invertida) ou no início da segunda linha.
- Não divida atributos em várias linhas.

Os arquivos de configuração do iPlanet para sua instância do iPlanet são encontrados no seguinte local:

base_do_iplanet/https-*nome_da_instância*/config/

onde *base_do_iplanet* é o diretório raiz da instalação do iPlanet e *nome_da_instância* é sua configuração de servidor específica.

Siga estas etapas:

1. No diretório *base_do_weblogic*/server/lib, copie o arquivo libproxy.so que corresponde à sua versão do Servidor web do iPlanet no sistema de arquivos em que você instalou o iPlanet.
2. Em um editor de texto, modifique o arquivo magnus.conf do iPlanet.

   Para instruir o iPlanet a carregar o arquivo libproxy.so como um módulo do iPlanet, adicione as seguintes linhas ao início do arquivo magnus.conf:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=caminho no sistema de arquivos da etapa 1/libproxy.so
   Init fn="wl_init"
   ```

   Por exemplo:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   A função load-modules sinaliza a biblioteca compartilhada para carregamento quando o iPlanet for inicializado. Os valores wl_proxy e wl_init identificam as funções que o plugin executa.

3. Em um editor de texto, modifique o arquivo obj.conf do iPlanet como segue:

   a. Depois da última linha que começa com o seguinte texto:

      NameTrans fn=....

      Adicione a seguinte Diretiva de serviço à seção Objeto name="default":

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      Observação: é possível adicionar essa diretiva em uma linha seguinte às Diretivas de serviços existentes.

   b. Adicione o código a seguir ao fim do arquivo:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="nome_do_host"
      WebLogicPort="número_da_porta" PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="nome_do_host"
      WebLogicPort="número_da_porta" PathTrim="/weblogic"
      </Object>
      ```

      onde *nome_do_host* é o nome do servidor e o domínio do sistema em que você instalou o WebLogic e o *número_da_porta* é a porta do WebLogic (o padrão é 7001).

      Você pode ter mais de um entrada de Objeto.

      Por exemplo:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MeuServidor.MinhaEmpresa.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MeuServidor.MinhaEmpresa.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. Salve o arquivo de configuração do iPlanet.
5. Reinicie a instância do servidor web.

Configurar o plugin de proxy do Apache

A configuração do plugin de proxy do Apache exige o arquivo http.conf.

Siga estas etapas:

1. Pare o servidor web do Apache após a instalação de um Agente web no Solaris e copie o arquivo mod_wl_20.so do seguinte local:

   base_do_weblogic/server/lib/solaris

   em

   base_do_apache/modules

2. Edite o arquivo http.conf (localizado no *base_do_apache*/conf) e faça as seguintes alterações:

   a. Na seção Carregar o módulo, adicione o seguinte código:
   ```
   LoadModule weblogic_module      modules/mod_wl_20,so
   ```

   b. Edite o nome do servidor com o nome do sistema de servidor do Apache.

   c. Adicione um bloco If no fim do arquivo, como se segue:
   ```
   <IfModule mod_weblogic.c>
     WebLogicHost servidor_do_weblogic.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. Salve o arquivo http.conf.

4. Reinicie o servidor web do Apache.

Associar o agente do SiteMinder a um domínio do CA Identity Manager

O administrador de políticas executa essa tarefa após a conclusão das tarefas do CA Identity Manager. Ao carregar os ambientes no CA Identity Manager, faça referência ao agente do 4.X. O SiteMinder usa esse agente ao criar o Domínio/Realm no Servidor de políticas do SiteMinder. Esse agente valida os cookies SMSESSION. Atualize o Domínio/Realm e faça referência ao agente em pleno funcionamento que está no servidor web que é usado para acessar o CA Identity Manager. Este servidor web age como o ponto de acesso para o CA Identity Manager e cria cookies SMSESSION.

Siga estas etapas:

1. Efetue logon na Interface de usuário administrativa do SiteMinder.

2. Vá para Políticas, Domínios.

3. Modifique o domínio para o seu ambiente.
4. Na guia Realms, edite o primeiro realm listado: XXX_ims_realm.
5. Procure e selecione o agente no seu proxy.

   Observação: se você não tiver um agente proxy (agente do servidor web), crie um. Verifique se você tem um servidor web e um proxy definidos para a frente do CA Identity Manager.
6. Clique em OK duas vezes e repita esse processo para o realm Público território XXX_pub_realm.
7. Depois de atualizar ambos os realms, clique em Enviar.
8. Aguarde até que o agente seja atualizado ou reinicie o servidor web onde o agente proxy está localizado.

Configurar o parâmetro LogOffUrI do SiteMinder

Depois de adicionar o SiteMinder ao ambiente, o logoff no CA Identity Manager não terá nenhum efeito. Para ativar novamente essa funcionalidade, atualize o ACO (Agent Configuration Object - objeto de configuração do agente) para o agente no proxy.

Siga estas etapas:

1. Efetue logon na Interface de usuário administrativa do SiteMinder. Clique na guia Infraestrutura, Agentes, Expandir configuração do agente e clique em Modificar configuração do agente.
2. Localize seu ACO. Localize o parâmetro #LogoffUri. Clique no botão de reprodução (seta apontando para a direita) à esquerda do parâmetro.
3. Remova o sinal de cerquilha (#) do nome no campo Valor e insira /idm/logout.jsp.
4. Clique em OK e em Enviar para atualizar o objeto de configuração do agente.

   Na próxima vez que o agente recuperar sua configuração do servidor de políticas, a nova configuração será propagada.

Solução de problemas

Os tópicos a seguir descrevem erros comuns que podem ocorrer. Onde foi possível, uma resolução foi emparelhada com o erro para ajudar você com sua integração.

DDL ausente do Windows

Sintoma:

DLL ausente do Windows (MSVCP71.dll)

Observamos que depois que a conexão do SiteMinder foi ativada, o JBoss lançou um erro java reclamando sobre uma DLL ausente (MSVCP71.dll).

Observação: esse erro poderá não aparecer se o JBoss estiver sendo executado como um serviço. Se possível, teste a configuração sem executar o JBoss como um serviço.

Solução:

Siga estas etapas:

1. Localize MSVCP71.dll no Servidor de políticas do SiteMinder, caso esteja em execução no Windows.
2. Copie essa DLL (MSVCP71.dll) na pasta \Windows\system32.
3. Depois de posicionar esse arquivo no local correto, registre-o no sistema operacional.
4. Em uma janela de comando, execute o comando regsvr32. Depois que o arquivo for carregado, o processo estará concluído.
5. Reinicie o servidor de aplicativos.

Local do Servidor de políticas do SiteMinder incorreto

Sintoma:

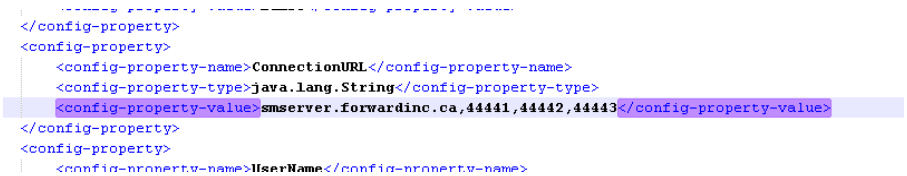
Local do Servidor de políticas do SiteMinder incorreto.

Solução:

Um local incorreto é referenciado no ra.xml. O erro "Cannot connect to policy server: xxx" é exibido.

Siga estas etapas:

1. Verifique o nome do host fornecido no ra.xml.



2. Na propriedade ConnectionURL, especifique o nome do host do Servidor de políticas do SiteMinder. Use um FQN (Fully Qualified Name - nome totalmente qualificado).

Nome de administrador incorreto

Sintoma:

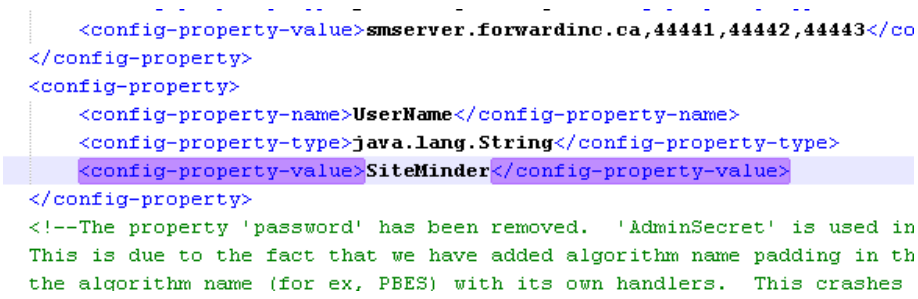
Nome de administrador incorreto

Solução:

Um administrador incorreto é referenciado no ra.xml. O erro "Unknown administrator" é exibido.

Siga estas etapas:

1. Verifique a propriedade UserName no ra.xml.



2. Na propriedade UserName, especifique a conta usada para se comunicar com o CA SiteMinder. Por exemplo, use a conta do SiteMinder (valor padrão).

Segredo do administrador incorreto

Sintoma:

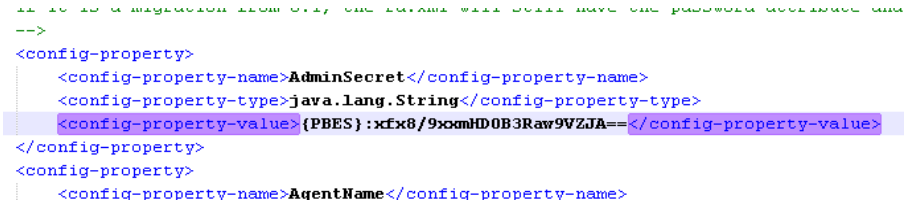
Segredo do administrador incorreto

Solução:

Um segredo de administrador incorreto é usado no ra.xml. O erro "Cannot connect to the policy server: Invalid credentials" é exibido.

Siga estas etapas:

1. Verifique a propriedade AdminSecret no ra.xml.



2. Na propriedade AdminSecret, especifique a senha criptografada para o nome de usuário apontado na propriedade UserName.

Mais informações:

Modificar uma senha ou um shared secret do SiteMinder (na página 376)

Nome do agente incorreto

Sintoma:

Nome do agente incorreto

Solução:

Um nome de agente incorreto é usado no ra.xml. O erro "Cannot connect to the policy server: Failed to init Agent API: -1" é exibido.

Siga estas etapas:

1. Verifique a propriedade AgentName no ra.xml.

```
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>idmagent</config-property-value>
</config-property>
<config-property>
```

2. Especifique o nome do agente 4.X que você criou durante a 3ª etapa das configurações do SiteMinder.

Segredo de agente incorreto

Sintoma:

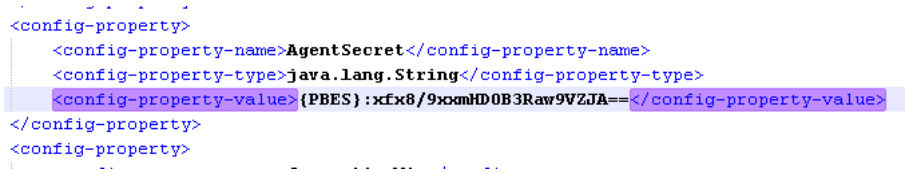
Segredo de agente incorreto

Solução:

Um segredo de agente incorreto é usado no ra.xml. O erro "Cannot connect to the policy server: Failed to init Agent API: -1" é exibido com um erro de manipulador criptografado precedente.

Siga estas etapas:

1. Verifique a propriedade AgentSecret no ra.xml.



2. Especifique a senha criptografada que foi usada durante a criação desse agente.

Mais informações:

Modificar uma senha ou um shared secret do SiteMinder (na página 376)

Nenhum contexto de usuário no CA Identity Manager

Sintoma:

Nenhum contexto de usuário no CA Identity Manager.

Se um usuário tentar acessar o CA Identity Manager sem um cookie SMSESSION, o CA Identity Manager não poderá autenticar o usuário. Nesse caso, você pode esperar para ver a interface de usuário do CA Identity Manager em branco.

Se você tiver ativado o fluxo de trabalho para o seu ambiente, espere ver uma falha muito semelhantes a esta.

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

Solução:

Alguns itens podem causar esse problema, mas geralmente é um destes:

- Você acessou o CA Identity Manager diretamente.
- O agente do SiteMinder no proxy está desativado (ou seja, nada será protegido - o cookie SMSESSION não está sendo criado).
- O domínio do SiteMinder para o ambiente do CA Identity Manager foi configurado incorretamente.

As duas primeiras causas são bastante simples e diretas. Certifique-se de usar o servidor web com o agente web em pleno funcionamento ativado. Se, no entanto, você estiver examinando a o servidor web e o agente estiver ativado, será necessário modificar o Domínio.

Siga estas etapas:

1. Efetue logon na Interface de usuário administrativa do SiteMinder.
2. Localize o Domínio do CA Identity Manager e clique nas camadas para modificá-lo. Clique na guia Realm e no primeiro realm da lista.
3. O local padrão da barra é sob o realm. Exclua-a.
4. Clique na Regra sob este Realm.

   O recurso eficaz padrão para a regra é um asterisco "*".
5. Adicione a barra "/" na frente do asterisco.

   Você moveu a barra do realm para a regra. A proteção é a mesma, mas o SiteMinder a trata de forma diferente.

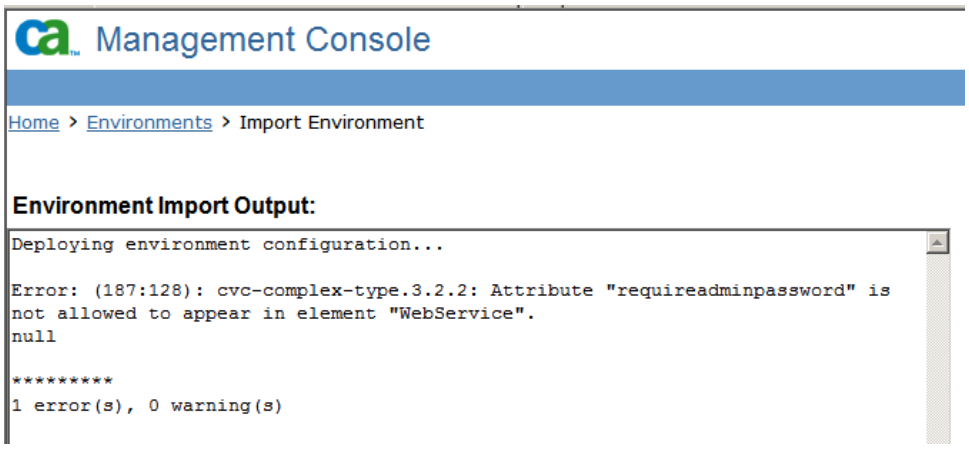
   É possível efetuar logon com êxito no CA Identity Manager usando o SiteMinder. Para validar a proteção adequada, examine os logs do agente do SiteMinder.

Erro ao carregar ambientes

Sintoma:

Ao importar um ambiente de volta no CA Identity Manager após a integração com o SiteMinder, será exibido um erro sobre o atributo "requireadminpassword" e o elemento "WebService".

Observação: esse problema também pode ocorrer quando o SiteMinder não fizer parte da implantação.



Solução:

Esse erro permite a implantação parcial do ambiente. A implantação parcial pode criar elementos vazios no repositório de objetos do CA Identity Manager. Corrija um dos XMLs do ambiente e reimporte.

Siga estas etapas:

1. Localize o arquivo ZIP arquivado e explore-o.
2. Crie uma cópia do XXX_environment_settings.xml.
3. Edite esse arquivo e localize o elemento "WebService".
4. Exclua a tag "requireadminpassword="false".

   Observação: remova a tag *e* o valor. Não remova apenas o valor.
5. Salve as alterações e coloque o arquivo de volta no arquivo ZIP.
6. Reimporte o arquivo zip arquivado do ambiente.

   Você não deve excluir o ambiente que foi criado na tentativa que falhou. Reimportar um arquivo corrigido elimina os erros da tentativa que falhou.

Não é possível criar um diretório ou ambiente do CA Identity Manager

Sintoma:

Não é possível criar um diretório ou ambiente do CA Identity Manager, quando a integração do SiteMinder é ativada.

Solução:

Esse problema pode ser causado pela falta de uma entrada no Registro.

Verifique se a configuração de Registro a seguir existe na máquina do Servidor de políticas do SiteMinder:

- Solaris ou Linux:

  Verifique se a seguinte entrada existe em sm.registry:
  ImsInstalled=8.0; REG_SZ

- Windows:

  Verifique se a configuração "ImsInstalled=8.0; REG_SZ" existe no seguinte local:
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  Observação: se o caminho do Registro \Netegrity\SiteMinder\CurrentVersion não existir, crie-o manualmente.

Se você alterar o Registro, não se esqueça de reiniciar o Servidor de políticas para que as alterações entrem em vigor.

Importante: antes de modificar o registro, execute um backup completo do sistema.

O usuário não pode efetuar logon

Sintoma:

Um novo usuário não pode efetuar logon em um ambiente com uma senha em texto não criptografado.

Solução:

Verifique se a seguinte classificação de dados não está incluída na definição do atributo de senha no arquivo de configuração de diretório (directory.xml):

<DataClassification name="AttributeLevelEncrypt"/>

Em ambientes que incluem os componentes a seguir, ativar a criptografia em nível de atributo impede os usuários de efetuar logon:

- CA SiteMinder e
- Um banco de dados relacional

Como definir as configurações de agente do CA Identity Manager

Quando o CA Identity Manager integra-se ao SiteMinder, o CA Identity Manager usa um agente interno do CA Identity Manager para se comunicar com o Servidor de políticas do SiteMinder. Para ajustar o desempenho, defina as seguintes configurações de conexão para o agente do CA Identity Manager.

1. Execute uma das seguintes etapas:
   - Se o CA Identity Manager estiver em execução em um servidor de aplicativos do WebLogic ou WebSphere, edite o adaptador de recursos no descritor do conector policyserver_rar, no console do servidor de aplicativos.
   - Se o CA Identity Manager estiver em execução em um servidor de aplicativos do JBoss, abra o policyserver-service.xml em <JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.
2. Defina as configurações da seguinte maneira:

   ConnectionMax

   Define o número máximo de conexões com o servidor de políticas, por exemplo, 20.

   ConnectionMin

   Define o número mínimo de conexões com o servidor de políticas, por exemplo, 2.

   ConnectionStep

   Define o número de conexões adicionais a serem abertas quando todas as conexões de agente estiverem em uso.

   ConnectionTimeout

   Especifica o tempo, em segundos, que o agente precisa aguardar para se conectar ao SiteMinder antes de exceder o tempo limite.
3. Reinicie o servidor de aplicativos.

Configurar a alta disponibilidade do SiteMinder

Se você criou um cluster de Servidores de políticas do SiteMinder, será possível configurar um cluster de servidores de aplicativos para usá-lo para balanceamento de carga e tolerância a falhas.

Siga estas etapas:

1. Edite o arquivo ra.xml neste local:
   WebSphere:
   PERFIL_WAS/config/cells/*NOME_DA_CÉLULA*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss:*base_do_jboss*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic: *domínio_wl*/applications/iam_im.ear/policyserver_rar/META-INF
2. Modifique esses itens, que são explicados nas seções a seguir:
   - Configurações de conexão para o Servidor de políticas
   - O número de Servidores de políticas
   - A seleção de balanceamento de carga ou tolerância a falhas para o cluster.
3. Repita essas etapas para cada servidor do CA Identity Manager no cluster.
4. Reinicie o servidor de aplicativos para que as alterações entrem em vigor.

Observação: quando você estiver criando um diretório ou ambiente do CA Identity Manager, ou modificando as configurações de ambiente ou diretório, defina Failover e FailoverServers do SiteMinder para false. Caso contrário, o objeto de diretório poderá ser criado, mas não replicado em tempo de ser usado. Por exemplo, crie um diretório no Servidor 1. Em seguida, crie um atributo usando a ID de objeto desse diretório no Servidor 2, mas o segundo diretório ainda não existe. Você recebe um erro de objeto não encontrado.

Modificar as configurações de conexão do Servidor de políticas

As informações de conexão do Servidor de políticas devem refletir o servidor principal do ambiente de produção. Essa informação consiste no ConnectionURL, no nome de usuário e na senha da conta do administrador do SiteMinder, bem como no nome e no shared secret do Agente.

No exemplo a seguir, os valores editáveis são exibidos em LETRAS MAIÚSCULAS.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-
value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</config-
                property-value>
</config-property>
```

```
<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

Observação: para os valores que exigem texto criptografado, use a ferramenta de senha do CA Identity Manager. Para obter mais informações, consulte o *Guia de Configuração*.

Adicionar mais Servidores de políticas

Para adicionar mais Servidores de políticas à instância de instalação do CA Identity Manager, edite a entrada FailoverServers no arquivo ra.xml.

Observação: inclua o Servidor de políticas principal e todos os servidores de tolerância a falhas na entrada FailoverServers.

Para cada Servidor de políticas, insira um endereço IP e os números de porta para serviços de autenticação, autorização e contabilidade. Use um ponto e vírgula para separar as entradas, como mostrado aqui:

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

Selecionar o balanceamento de carga ou a tolerância a falhas

O comportamento padrão do CA Identity Manager é usar o balanceamento de carga round-robin que usam os servidores que são identificados por ConnectionURL e FailoverServers. O balanceamento de carga ocorrerá se você deixar FailOver definido como false.

Para selecionar a tolerância a falhas, defina FailOver como true:

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

Removendo o SiteMinder de uma implantação existente do CA Identity Manager

Esta seção apresenta instruções detalhadas para remover o CA SiteMinder de um ambiente existente do CA Identity Manager.

Siga estas etapas:

Importante: as informações históricas de senha não poderão ser acessadas após a migração.

1. Pare o servidor de aplicativos.
2. Desative o Servidor de políticas no arquivo ra.xml localizado em \iam_im.ear\policyserver.rar\META-INF definindo o valor de Enabled config-property para false.
3. Edite o arquivo web.xml localizado em \iam_im.ear\User_console.war/WEB-INF e defina a propriedade FrameworkAuthFilter para Enabled = true.

   Observação: para o WebSphere, o arquivo web.xml está localizado em *base_do_WebSphere*/AppServer/profiles/*Nome_do_perfil*/config/cells/*Nome_da_célula*/applications/iam_im.ear/deployments/IdentityMinder/user_console.war/WEB-INF.

4. Inicie o servidor de aplicativos.
5. (Apenas WebSphere) Atualize o objeto policyServer no Console administrativo com os mesmos valores do arquivo ra.xml.

Operações do SiteMinder

As seções a seguir descrevem como modificar os recursos do SiteMinder, incluindo os domínios de política e os esquemas de autenticação, para oferecer suporte ao CA Identity Manager:

Coletar credenciais do usuário usando um esquema de autenticação personalizado (na página 357)

Altera o método que o CA Identity Manager usa para coletar as credenciais de usuários que tentam acessar um Ambiente do CA Identity Manager.

Configurar funções de acesso (na página 358)

Fornece acesso a funções em um aplicativo.

Configurar o URL de LogOff (na página 373)

Impede o acesso não autorizado a um Ambiente do CA Identity Manager aplicando um logoff completo.

Atualizar um alias em realms do SiteMinder (na página 375)

Atualiza os realms que protegem um Ambiente do CA Identity Manager quando você altera o alias do Ambiente.

Senhas do SiteMinder (na página 376)

Permite alterar a senha da conta do administrador que o CA Identity Manager usa para se comunicar com o SiteMinder, bem como o shared secret do agente do SiteMinder que protege um Ambiente do CA Identity Manager.

Definir as configurações do agente do CA Identity Manager (na página 352)

Ajusta o desempenho do agente do CA Identity Manager que se comunica com o Servidor de políticas do SiteMinder.

Usar diretórios diferentes para autenticação e autorização (na página 378)

Permite que os administradores que possuam perfis em um diretório gerenciem usuários em um diretório diferente.

Aprimorar o desempenho das operações do diretório LDAP (na página 380)

Aumenta a taxa de transferência das solicitações do CA Identity Manager para o repositório de usuários configurando o SiteMinder para abrir várias conexões com o mesmo diretório.

Coletar credenciais do usuário usando um esquema de autenticação personalizado

O SiteMinder usa um esquema de autenticação para coletar as credenciais de usuário e determinar a identidade de um usuário no momento do logon. Quando um usuário é identificado, o CA Identity Manager gera um Console de usuário personalizado com base nos privilégios do usuário.

É possível implementar qualquer esquema de autenticação do SiteMinder para proteger o Ambiente do CA Identity Manager.

Por exemplo, você pode implementar um Esquema de autenticação de formulários HTML, que coleta credenciais em um formulário HTML. O uso de um formulário HTML permite criar uma página de logon que pode incluir elementos de marca, como um logotipo da empresa, e links para as páginas de autorregistro e senha esquecida.

Observação: para obter informações sobre esquemas de autenticação, consulte o *Guia de Configuração do Servidor de Políticas do CA SiteMinder*.

Siga estas etapas:

1. Efetue logon em uma das interfaces a seguir:
   - No CA SiteMinder Web Access Manager r12 ou superior, efetue logon na Interface de usuário administrativa.
   - No CA eTrust SiteMinder 6.0 SP5, efetue logon na Interface de usuário do servidor de políticas.

   Observação: para obter informações sobre como usar essas interfaces, consulte a documentação da versão do SiteMinder que você está usando.
2. Crie um esquema de autenticação, conforme descrito no *Guia de Configuração do Servidor de Políticas do CA SiteMinder*.
3. Modifique o realm que protege o Ambiente do CA Identity Manager adequado para usar o esquema de autenticação que você criou na Etapa 1.

   O nome do realm tem o seguinte formato:

   *ambiente-do-Identity Manager*_ims_realm

   Observação: se você configurou o suporte para tarefas públicas, será exibido um realm adicional, *ambiente-do-Identity Manager*_pub_realm. Esse realm usa um esquema de autenticação anônima para permitir que usuários desconhecidos usem os recursos de autorregistro e senha esquecida sem fornecer credenciais. Não modifique os esquemas de autenticação para esses realms.

Importar definições de dados no repositório de políticas

Você pode controlar o acesso de um usuário a funções de aplicativo usando as políticas do SiteMinder. A instalação do Servidor de políticas inclui as definições de dados necessárias para permitir esse controle. Importe o arquivo IdmSmObjects.xdd deste local:

base_do_siteminder\xps\dd

base_do_siteminder é o caminho de instalação do Servidor de políticas.

Como configurar as funções de acesso

As funções de acesso permitem o gerenciamento centralizado de privilégios de usuário nos aplicativos externos que o SiteMinder protegeu. Os administradores do CA Identity Manager podem criar e atribuir funções no Console de usuário do CA Identity Manager que determinam o acesso dos usuários aos aplicativos fora do CA Identity Manager. Por exemplo, um Administrador de função pode criar funções no Console de usuário que controla o acesso a um aplicativo financeiro e concede a capacidade de atribuir as funções ao administrador do Suporte técnico. O administrador do Suporte técnico pode atribuir ou revogar essa função por meio do Console de usuário.

As funções de acesso são ativadas pela integração com o SiteMinder. O SiteMinder associa funções a políticas para determinar quais usuários podem acessar um recurso protegido e fornecer as informações de tarefa e funções específicas de usuário a recursos protegidos.

As funções de acesso exigem configuração no CA Identity Manager e no SiteMinder. Dois administradores são envolvidos:

- O administrador do CA Identity Manager cria funções e tarefas de acesso no CA Identity Manager. As funções padrão de Gerente do sistema e Gerente de função de acesso incluem essas tarefas.
- O administrador do SiteMinder gerencia objetos de Sistema e Domínio no CA SiteMinder. O administrador do SiteMinder deve ter o escopo de Sistema.

  Observação: para obter mais informações, consulte o *Guia de Configuração do Servidor de Políticas*.

O procedimento a seguir descreve as etapas para criar uma função de acesso. Analise estas etapas *antes* de configurar as funções de acesso para uso com o SiteMinder.

1. Um administrador do CA Identity Manager executa as seguintes tarefas:
   a. Ativa as tarefas e funções de acesso para uso com o SiteMinder.
   b. Cria tarefas de acesso.
   c. Cria uma função de acesso.
   d. Comunica informações de função e tarefa ao administrador do SiteMinder para fins de criação de políticas de controle de acesso com base em função do SiteMinder.
2. Um administrador do SiteMinder cria uma política de controle de acesso com base em função, seguindo as etapas abaixo:
   a. Atribuindo um diretório de usuários que esteja associado a um ou mais ambientes do CA Identity Manager a um Domínio da política.
   b. Associando um ou mais ambientes do CA Identity Manager ao Domínio da política na etapa 1.
   c. Criando realms e regras no Domínio da política (se ainda não existirem). Os realms e as regras devem corresponder aos recursos para os quais as funções de acesso concedem acesso.
   d. Criando políticas e vinculando-as a funções do ambiente do CA Identity Manager.
   e. (opcional) Especificando respostas que fornecem informações de direitos aos recursos protegidos.

   Observação: para obter instruções detalhadas sobre essas etapas, consulte o *Guia de Configuração do Servidor de Políticas*.

Mais informações:

Ativar funções de acesso para uso com o SiteMinder (na página 359)

Ativar funções de acesso para uso com o SiteMinder

Para usar as funções de acesso com o CA SiteMinder, o CA Identity Manager espelha todos os objetos no repositório de objetos do CA Identity Manager que estão relacionados a essas funções de acesso no repositório de políticas do SiteMinder. Para ativar as funções de acesso para uso com o SiteMinder, configure uma propriedade no Management Console do CA Identity Manager.

Siga estas etapas:

1. Abra o console de gerenciamento.
2. Selecione Environment, *Your Environment*, Advanced Settings, Miscellaneous.

3. Adicione uma propriedade fornecendo as seguintes informações:
   - No campo Property, insira o seguinte texto:

     EnableSMRBAC
   - No campo Value, insira o seguinte texto:

     true
4. Clique em Adicionar. Em seguida, clique em Save.

   Uma mensagem é exibida indicando que o ambiente deve ser reiniciado.
5. Clique em Restart Environment.

   O CA Identity Manager agora oferece suporte às funções e tarefas de acesso para uso com o CA SiteMinder.

Assim que você ativar as funções de acesso para uso com o CA SiteMinder, observe os seguintes pontos:

- Se você usou as funções de acesso no CA Identity Manager r8x, execute uma etapa de migração adicional para gerenciar essas funções de acesso na versão atual do CA Identity Manager. Para obter mais informações, consulte o *Guia de Atualização*.
- Para desativar o suporte a funções de acesso no SiteMinder, exclua os objetos de tarefa e função de acesso do CA Identity Manager do repositório de políticas do SiteMinder. Em seguida, remova a propriedade EnableSMRBAC da lista Miscellaneous Properties e reinicie o Ambiente.

Adicionar tarefa de acesso à função administrativa

Por padrão, as tarefas de acesso não aparecem na guia Roles and Tasks, você precisa adicioná-las à função administrativa do usuário conectado.

Siga estas etapas:

1. Efetue logon em uma conta do CA Identity Manager com uma função que inclui uma tarefa para a criação de funções de acesso.
2. Clique em Funções e tarefas, Modificar função administrativa.
3. Selecione a função administrativa do usuário conectado.
4. Clique na guia Tarefas, no campo Filtrar por categoria, selecione Funções e tarefas na caixa suspensa.
5. Selecione Criar tarefa de acesso na lista suspensa Adicionar tarefa.
6. Clique em Enviar.

Criar uma tarefa de acesso

Uma tarefa de acesso é uma única ação que um usuário pode executar em um aplicativo de negócios, como a geração de uma ordem de compra em um aplicativo financeiro. Os usuários podem executar essa ação quando recebem uma função de acesso que inclua a tarefa de acesso.

Importante: para criar tarefas de acesso, você precisa adicionar as Tarefas de acesso (na página 360) à Função administrativa do usuário conectado.

Siga estas etapas:

1. Selecione Funções e tarefas, Tarefas de acesso, Criar tarefa de acesso.
2. Selecione uma das seguintes opções:
   - Criar uma tarefa de acesso
   - Criar uma cópia de uma tarefa de acesso
3. Preencha estes campos:

   Nome

   Um nome exclusivo que você pode atribuir à tarefa, como Gerar ordem de compra.

   Qualificador

   Um qualificador exclusivo para a tarefa. O qualificador deve começar com uma letra ou um caractere de sublinhado contendo letras, números ou sublinhados.

   Descrição

   Uma nota opcional sobre a finalidade da tarefa.

   ID do aplicativo

   O identificador de um aplicativo, como o nome do aplicativo associado à tarefa. A ID do aplicativo não pode conter espaços ou caracteres que não sejam alfanuméricos.

   Anote essa ID; você precisará dela quando ativar a função no SiteMinder.
4. Para concluir a tarefa de acesso, clique em Enviar.

Como criar uma função de acesso

Uma função de acesso contém tarefas de acesso, que fornecem acesso a funções em um aplicativo. Por exemplo, uma função pode conter tarefas que permitem aos integrantes da função fazer um pedido em um aplicativo de compra e atualizar quantidades em um aplicativo de controle de inventário.

Conclua as etapas a seguir para criar uma função de acesso:

1. Inicie a criação da função de acesso. (na página 362)
2. Defina as propriedades básicas para a função de acesso na guia Perfil. (na página 362)
3. Selecione as tarefas de acesso para a função. (na página 363)
4. Defina políticas de integrantes para a função. (na página 364)
5. Defina políticas administrativas para a função. (na página 364)
6. Defina regras de proprietário para a função. (na página 365)

Iniciar a criação da função de acesso

Siga estas etapas:

1. Efetue logon em uma conta do CA Identity Manager com uma função que inclui uma tarefa para a criação de funções de acesso.
2. Clique em Funções de acesso, Criar função de acesso.

   Escolha a opção de criar uma cópia de uma função ou a função. Se selecionar a opção Copiar, pesquise a função.
3. Prossiga para a próxima seção, Definir o perfil de uma função de acesso.

Definir o perfil de uma função de acesso

Siga estas etapas:

1. Insira um nome e uma descrição e preencha os atributos personalizados definidos para a função.

   Observação: é possível especificar atributos personalizados na guia Perfil que especificam informações adicionais sobre as funções de acesso. Você pode usar essas informações adicionais para facilitar as pesquisas de funções em ambientes que incluem um número significativo de funções.
2. Selecione Ativado se estiver pronto para tornar a função disponível para uso assim que criá-la.
3. Prossiga para a próxima seção, Definir políticas de integrante para uma função de acesso.

Selecionar Tarefas de acesso para a função

Clique na guia Tarefas:

1. Selecione as tarefas a serem incluídas nessa função. Primeiramente, selecione os aplicativos e, em seguida, a tarefa. Você pode incluir tarefas em diferentes aplicativos:

   Observação: se outra função tiver as tarefas necessárias, clique em Copiar tarefas de outra função. Você pode editar a lista exibida.

   Na criação de uma função ou tarefa, você verá os ícones de adição, edição e remoção de itens:

   Avance ou selecione o item atual a ser exibido ou editado.

   Se o JavaScript estiver desativado, pressione o botão avançar para selecionar em uma lista suspensa.

   Retorne ou desfaça uma seleção anterior.

   Insira um elemento, como uma tarefa ou regra.

   Exclua a tarefa atual ou, em uma regra, a expressão que se segue.

   Mova o item atual para cima na lista.

   Mova o item atual para baixo na lista.

2. Prossiga para a próxima seção, Definir políticas administrativas para uma função de acesso.

Definir políticas de integrante para uma função de acesso

Um política de integrante define uma regra de integrante e regras de escopo para uma função. Você pode definir várias políticas de integrante para uma função. Para cada política, os usuários que atendem à condição na regra de integrante têm o escopo para usar a função que é definida na política.

Siga estas etapas:

1. Selecione a guia Integrantes.
2. Selecione Adicionar para definir as políticas de integrante.
3. (Opcional) Na página Política de integrante, você tem a opção de definir uma regra de integrante para quem deve poder usar essa função.

   A definição de uma regra de integrante atribui automaticamente a função aos usuários que corresponderem aos critérios na política de integrante.

   Observação: defina as políticas de integrante que usam apenas atributos de diretório, por exemplo: title=Manager. Se você definir políticas de integrante que façam referência a esses objetos não armazenados no diretório de usuários, como funções administrativas, o SiteMinder não poderá resolver a referência.
4. Verifique se a Política de integrante é exibida na guia Integrantes.

   Para editar uma política, clique no símbolo de seta à esquerda. Para removê-la, clique no ícone do sinal de menos.
5. Na guia Integrantes, marque a caixa de seleção Os administradores podem adicionar e remover integrantes desta função.

   Ao ativar esse recurso, você pode definir Adicionar ação e Remover ação. Essas ações definem o que acontece quando um usuário é adicionado ou removido como um integrante da função.

Definir políticas administrativas para uma função de acesso

Uma política administrativa define regras administrativas, regras de escopo e privilégios de administrador para uma função. Você pode definir várias políticas administrativas para uma função. Cada política indica que se um administrador atender à condição na regra administrativa, ele possui o escopo e os privilégios de administrador que são definidos para a política.

Siga estas etapas:

1. Selecione a guia Administradores da função de acesso.
2. Se desejar tornar a opção Gerenciar administradores disponível, marque a caixa de seleção Os administradores podem adicionar e remover administradores desta função.

   Ao ativar esse recurso, defina as ações para quando um usuário é adicionado ou removido como um administrador da função.

3. Na guia Administradores, adicione as políticas administrativas que incluem regras administrativas e de escopo, bem como os privilégios de administrador. Cada política exige pelo menos um privilégio (Gerenciar integrantes ou Gerenciar administradores).

   Você pode adicionar várias políticas administrativas com regras e privilégios diferentes para administradores que atendam à regra.

   Observação: defina as políticas administrativas que usam apenas atributos de diretório, por exemplo: title=Manager. Se você definir políticas de integrante que façam referência a esses objetos não armazenados no diretório de usuários, como funções administrativas, o SiteMinder não poderá resolver a referência.

4. Para editar uma política, clique no símbolo de seta à esquerda. Para removê-la, clique no ícone do sinal de menos.

5. Prossiga para a próxima seção, Definir regras de proprietário para uma função de acesso.

Definir regras de proprietário para uma função de acesso

Uma regra de proprietário define quem pode modificar uma regra. Você pode definir várias regras de proprietário para uma função.

Siga estas etapas:

1. Selecione a guia Proprietários da função de acesso.

2. Defina as regras de proprietário, que determinam os usuários que podem modificar a função.

   Note: defina as regras de proprietário que usam apenas atributos de diretório, por exemplo: title=Manager. Se você definir regras de proprietário que façam referência a esses objetos não armazenados no diretório de usuários, como funções administrativas, o SiteMinder não poderá resolver a referência.

3. Clique em Enviar.

   Uma mensagem é exibida, indicando que a tarefa foi enviada. Um atraso momentâneo pode ocorrer antes que um usuário possa usar a função.

Funções de acesso no SiteMinder

Para configurar o controle de acesso com base em funções para recursos protegidos, um administrador do SiteMinder associa um Ambiente do CA Identity Manager a um Domínio da política na Interface de usuário do servidor de políticas. O administrador cria uma política para proteger um aplicativo e associa uma função ou funções a essa política. Os usuários que possuem uma função associada podem acessar o aplicativo protegido.

Um administrador do SiteMinder associa funções às políticas de segurança que definem como os usuários interagem com os recursos. As políticas se vinculam aos seguintes objetos:

- Usuários e grupos de usuários

  Identifique um conjunto de usuários afetados pela política.

- Funções

  Identifique os usuários que receberam um conjunto de privilégios no CA Identity Manager.

- Regras

  Identifique um recurso e as ações que são permitidas ou negadas para o recurso. Geralmente, o recurso é um URL, aplicativo ou script.

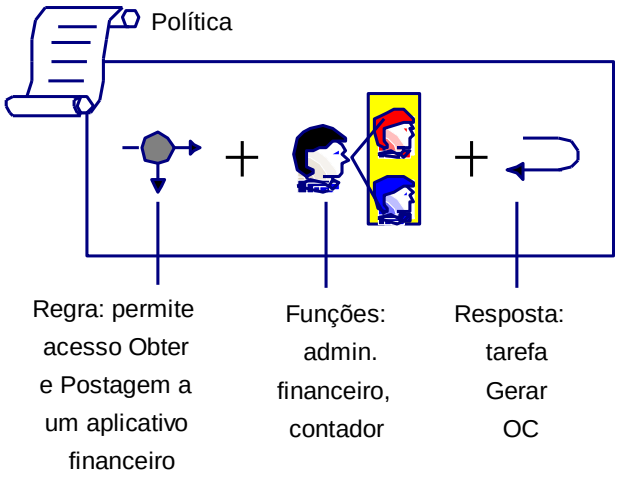
- Respostas

  Determine uma reação a uma regra. Quando uma regra é disparada, as respostas são retornadas para um Agente do SiteMinder.

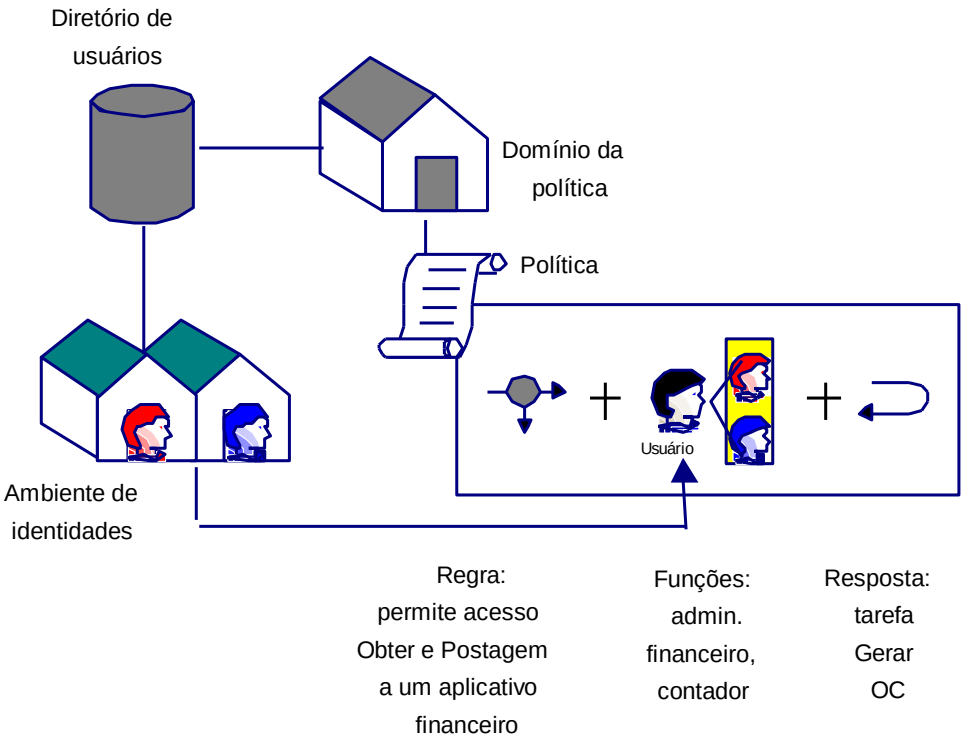
  O CA Identity Manager usa as respostas do SiteMinder para fornecer informações específicas de tarefa e função a um recurso protegido.

É possível vincular as políticas do SiteMinder a usuários, ou a funções, ou a usuários *e* funções. Suponha que um usuário ou integrante da função tente acessar um recurso protegido. O SiteMinder usa informações da política para determinar se é necessário conceder acesso e disparar respostas.

A figura a seguir ilustra a relação de objetos de política em uma política com base em função.



As políticas do SiteMinder são criadas nos domínios de política que, de forma lógica, vinculam diretórios de usuários a recursos protegidos. A figura a seguir ilustra a relação de objetos de política em uma política com base em função.



Para fornecer direitos de usuário a um aplicativo protegido, o administrador do SiteMinder combina uma regra com a política de um aplicativo com uma resposta. A resposta contém um atributo de resposta gerado pelo SiteMinder que recupera informações de direito do CA Identity Manager.

Quando o SiteMinder autoriza um integrante da função para um recurso protegido, os seguintes eventos ocorrem:

1. A regra de uma política é executada no SiteMinder, acionando a resposta combinada.
2. O Servidor de políticas obtém informações de direito do CA Identity Manager para incluir em uma resposta.
3. O Servidor de políticas transmite os atributos de resposta ao Agente web.
4. O Agente web disponibiliza as informações de direito ao aplicativo como uma variável de cabeçalho HTTP ou um cookie.

Atributos de resposta gerados pelo SiteMinder

O CA Identity Manager transmite informações de direito a aplicativos por meio de respostas do Agente web do SiteMinder. Essas respostas contêm variáveis de cabeçalho HTTP em atributos de resposta, que o aplicativo pode usar para determinar os privilégios de acesso de um usuário. As respostas são incluídas nas políticas do SiteMinder, que determinam como os usuários interagem com um recurso protegido.

Os administradores do SiteMinder podem configurar uma resposta que inclua dois tipos de atributos de resposta para transmitir informações a um aplicativo:

- SM_USER_APPLICATION_ROLES[:*id do aplicativo*] - retorna uma lista de funções que são atribuídas a um usuário.
- SM_USER_APPLICATION_TASKS[:*id de aplicativo*] - retorna uma lista de tarefas que um usuário pode executar com base nas funções que são atribuídas.

A ID de aplicativo limita o conjunto solicitado de funções e tarefas a um aplicativo específico. Por exemplo, se você criar o atributo de resposta a seguir:

SM_USER_APPLICATION_ROLES:Finance_application

O SiteMinder retornará as funções que têm tarefas no aplicativo Finance ao Agente web, que transmitirá as informações ao aplicativo Finance.

Observação: a *id de aplicativo* que você fornece deve corresponder a uma *id de aplicativo* fornecida quando você usou Criar tarefa de acesso no CA Identity Manager. Se a tarefa ainda não tiver sido criada, você poderá escolher qualquer nome para a ID de aplicativo, mas ele não poderá conter nenhum espaço nem caracteres que não sejam alfanuméricos.

Você pode especificar várias IDs de aplicativo em uma lista delimitada por vírgulas para retornar o conjunto de funções e tarefas de vários aplicativos em um único atributo de resposta. Por exemplo, para retornar a lista de funções que um usuário possui nos aplicativos Finance e Purchasing, especifique da seguinte maneira:

SM_USER_APPLICATION_ROLES:Finance, Purchasing

Como ativar funções de acesso no SiteMinder

As etapas abaixo pressupõem que o SiteMinder já protege o aplicativo ao qual a função de acesso concede acesso. Por exemplo, suponha que você esteja criando uma função de acesso para um aplicativo que o SiteMinder ainda não protege. Nesse caso, consulte um dos guias a seguir na biblioteca do SiteMinder:

- Para o SiteMinder 6.0 SP5, consulte o *Guia de Design de Política*.
- Para o SiteMinder 12.0 SP2, consulte o *Guia de Configuração do Servidor de Políticas*.

Observação: para configurar as funções de acesso no SiteMinder, use a Interface de usuário do servidor de políticas, um aplicativo com base em miniaplicativo, em vez da Interface de usuário administrativa do SiteMinder. No SiteMinder 12, esse miniaplicativo é chamado de Interface administrativa do FSS (Federation Security Services) do SiteMinder. É possível instalar a Interface de usuário administrativa do FSS usando o instalador do Servidor de políticas.

Para ativar as funções de acesso no SiteMinder, conclua as seguintes etapas de alto nível:

1. Na Interface de usuário do servidor de políticas, associe um diretório de usuários e um ambiente do CA Identity Manager a um Domínio da política (na página 370).
2. No Domínio da política, crie realms e regras (se ainda não existirem) correspondentes aos recursos para os quais a função de acesso concede acesso.

   Observação: para obter informações sobre como criar realms e regras, consulte um dos guias a seguir na biblioteca do SiteMinder:

   - Para o SiteMinder 6.0 SP5, consulte o *Guia de Design de Política*.
   - Para o SiteMinder 12.0 SP2, consulte o *Guia de Configuração do Servidor de Políticas*.

3. Crie uma resposta (na página 371) para transmitir informações de direito ao recurso.
4. Crie uma política e a associe aos objetos a seguir:
   - A função de acesso (na página 372)
   - Os realms e as regras criados na etapa 2.
   - As respostas criadas na etapa 3.

   Observação: para obter informações sobre como criar políticas, consulte o *Guia de Design de Política* (para o SiteMinder 6.0 SP5) ou o *Guia de Configuração do Servidor de Politicas* (para o SiteMinder 12.0 SP2).

Adicionar ambientes do CA Identity Manager a um domínio da política

Para ativar o SiteMinder para oferecer suporte a funções de acesso, você associa um ambiente do CA Identity Manager a um diretório de usuários e a um domínio da política no SiteMinder.

Observação: adicione o repositório de usuários associado ao ambiente do CA Identity Manager ao domínio da política *para que seja* possível adicionar o ambiente do CA Identity Manager ao domínio da política.

Siga estas etapas:

1. Na caixa de diálogo Domínio da política na Interface de usuário do servidor de políticas, adicione o repositório de usuários associado ao ambiente do CA Identity Manager a um domínio da política, como se segue:
   a. Selecione a guia Diretórios de usuários.
   b. Na caixa de listagem suspensa na parte inferior da guia, selecione o diretório de usuários a serem incluídos no domínio da política.
   c. Clique no botão Adicionar.

      A Interface de usuário do servidor de políticas adiciona o diretório à lista exibida na guia Diretórios de usuário.
   d. Clique em Aplicar.
2. Adicione o ambiente do CA Identity Manager ao domínio da política da seguinte forma:
   a. Selecione a guia Ambientes do CA Identity Manager.
   b. Selecione o Ambiente do CA Identity Manager que você deseja associar ao domínio da política na lista suspensa, na parte inferior da guia.

c. Clique em Adicionar.

A Interface de usuário do servidor de políticas adiciona sua seleção à lista de ambientes do CA Identity Manager na parte superior da guia.

3. Clique em OK para salvar suas seleções e feche a caixa de diálogo.

Os ambientes do CA Identity Manager que selecionados são disponibilizados quando você cria políticas.

Criar uma resposta do SiteMinder

Siga estas etapas:

1. Efetue logon na Interface de usuário do servidor de políticas.
2. Dependendo de seus privilégios administrativos, execute uma das seguintes tarefas:
   - Se você tiver o privilégio Gerenciar objetos do sistema e do domínio:
     a. No painel Objeto, clique na guia Domínios.
     b. Selecione o domínio da política ao qual você deseja adicionar uma resposta.
   - Se você tiver o privilégio Gerenciar objetos do domínio, selecione o domínio da política para adicionar uma resposta no painel Objeto.
3. Na barra de menus, selecione Editar, <nome do domínio>, Criar resposta.

   A caixa de diálogo Resposta do SiteMinder é exibida (consulte a caixa de diálogo Resposta).
4. Insira um nome e uma descrição para a nova resposta.
5. Na caixa de grupo Tipo de agente, selecione o botão de opção do SiteMinder.
6. Selecione a opção Agente web na lista suspensa da caixa de grupo Tipo de agente e clique em Aplicar para salvar as alterações.
7. Clique em Criar.

   A caixa de diálogo SiteMinder Response Attribute Editor é exibida.
8. Na lista suspensa Atributo, selecione o atributo de resposta WebAgent-HTTP-Header-Variable.
9. Na guia Configuração de atributos, selecione o botão de opção Atributo de usuário.
10. No campo Variável, insira o nome da variável que é transferido ao aplicativo.

    Por exemplo, se você especificar a variável TASKS, o seguinte cabeçalho será retornado ao aplicativo:

    HTTP_TASKS

11. No campo Nome do atributo, especifique o atributo de resposta como descrito a seguir:

    - SM_USER_APPLICATION_ROLES[:*id de aplicativo1, id_de_aplicativo2, ...id_de_aplicativon*] - retorna uma listas de funções que são atribuídas a um usuário.
    - SM_USER_APPLICATION_TASKS[:*id de aplicativo1, id_de_aplicativo2, ...id_de_aplicativon*]

    Os Atributos de resposta gerados pelo SiteMinder (na página 368) fornecem mais informações.

12. Clique em OK para salvar as alterações e retornar para a janela Administração do SiteMinder.

Adicionar funções a uma política do SiteMinder

Quando um usuário é atribuído a uma função de acesso apropriada que acessa um recurso protegido, o Servidor de políticas do SiteMinder verifica a atribuição de funções de acesso ao usuário. Após a verificação, ele dispara a regras incluídas na política para verificar se o usuário está autorizado a acessar o recurso ou não.

Siga estas etapas:

1. Na caixa de diálogo Política do SiteMinder, clique na guia Usuários.

   A guia Usuários contém guias para cada diretório de usuários e o ambiente do CA Identity Manager incluído no domínio da política.

2. Selecione o Ambiente do CA Identity Manager que contém as funções que deseja adicionar à política.

3. Clique no botão Adicionar/remover.

   A caixa de diálogo Função do CA Identity Manager da política do SiteMinder é exibida.

4. Para adicionar funções à política, selecione uma entrada na lista integrantes disponíveis e mova-a para a lista Integrantes atuais.

5. Clique em OK para salvar as alterações e retornar para a caixa de diálogo Política do SiteMinder.

Excluir funções em uma política

Além de usar as funções de acesso para conceder acesso a aplicativos, também é possível usá-las para impedir que os integrantes das funções de acesso acessem um aplicativo. Para impedir que os integrantes da função de acesso acessem um aplicativo, exclua as funções das políticas do SiteMinder. Quando um usuário que recebeu a função de acesso excluída no CA Identity Manager tenta acessar um recurso protegido, o Servidor de políticas verificará a exclusão da função do CA Identity Manager para o usuário atribuído. Após a verificação, ele bloqueará o acesso ao recurso.

Siga estas etapas:

1. Na caixa de diálogo Política do SiteMinder, clique na guia Usuários.

   A guia Usuários contém guias para cada diretório de usuários e o Ambiente do CA Identity Manager incluído no domínio da política.

2. Clique no Ambiente do CA Identity Manager que contém as funções que deseja excluir da política.

3. Clique no botão Adicionar/remover.

   A caixa de diálogo Função do CA Identity Manager da política do SiteMinder é exibida.

4. Para adicionar funções à política, selecione uma entrada na lista Integrantes disponíveis e clique no botão de Seta para a esquerda, que aponta para a lista Integrantes atuais.

   O procedimento oposto remove as funções da lista Integrantes atuais.

5. Na lista Integrantes atuais, selecione as funções a serem excluídas e clique no botão Excluir, localizado abaixo da lista.

   Um círculo vermelho com uma barra será exibido à esquerda das funções excluídas.

6. Clique em OK para salvar as alterações e retornar para a caixa de diálogo Política do SiteMinder.

Configurar o URI de LogOff

Para proteger um ambiente do CA Identity Manager, configure o Agente web do SiteMinder que protege o ambiente para encerrar uma sessão de usuário depois que o usuário efetua logoff no CA Identity Manager.

O Agente web encerra uma sessão de usuário excluindo a sessão do SiteMinder e os cookies de autenticação do navegador web e instruindo o Servidor de políticas a remover todas as informações da sessão.

Para encerrar a sessão do SiteMinder, configure a funcionalidade de logoff no campo LogOffURI do Objeto de configuração do agente do SiteMinder que protege o ambiente do CA Identity Manager.

Observações:

- Um agente do SiteMinder tem um URI de LogOff. Todos os aplicativos protegidos pelo agente usam a mesma página de logoff.
- Quando você configura páginas de logoff personalizadas no Management Console, conforme descrito em Configurar páginas de logoff personalizada, o CA Identity Manager envia a solicitação de logoff à página de logoff personalizada *e* ao URI de LogOff. No entanto, o CA Identity Manager exibe somente a página de logoff personalizada ao usuário.

Siga estas etapas:

1. Efetue logon em uma das interfaces a seguir:
   - No CA SiteMinder r12 ou superior, efetue logon na Interface de usuário administrativa.
   - No CA eTrust SiteMinder 6.0 SP5, efetue logon na Interface de usuário do servidor de políticas.

   Observação: para obter informações sobre como usar essas interfaces, consulte a documentação da versão do SiteMinder que você está usando.
2. Modifique a propriedade #LogOffUri no Objeto de configuração do agente que protege o ambiente do CA Identity Manager, como se segue:
   - Remova o sinal de cerquilha (#)
   - No campo Valor, especifique o seguinte URI:

     /iam/im/logout.jsp

   Observação: selecione um Objeto de configuração do agente ao instalar o Agente web. Para obter mais informações, consulte o *Guia de Instalação do Servidor de Políticas do CA SiteMinder Web Access Manager*.
3. Salve as alterações.
4. Reinicie o servidor web.

Aliases em realms do SiteMinder

Um *alias* é uma sequência de caracteres exclusiva adicionada ao URL para acessar um ambiente do CA Identity Manager. Por exemplo, quando o alias de um ambiente for *employees*, o URL para acessar esse ambiente será o seguinte:

`http://meu_servidor.minha_empresa.org/iam/im/employees`

meu_servidor.minha_empresa.org

Define o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado.

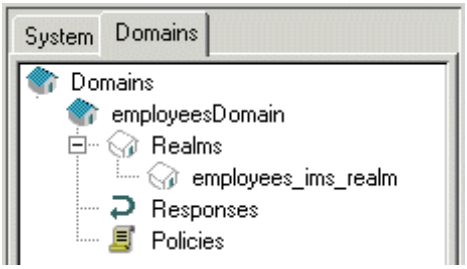
Especifique pelo menos um alias ao criar um ambiente do CA Identity Manager no Management Console. (Também é possível especificar um alias público.)

O SiteMinder usa o nome do ambiente para nomear os objetos que protegem o ambiente. Por exemplo, quando você especifica o nome *employees*, o SiteMinder cria objetos denominados *tipo_de_objetoemployee*.

tipo_de_objeto

Define o objeto do SiteMinder, como employees_ims_realm.

A ilustração a seguir mostra dois dos objetos que o SiteMinder cria:



Atualizar um alias em realms do SiteMinder

Se você modificar o alias protegido ou público no Management Console, o CA Identity Manager tenta atualizar os nomes de aliases no Servidor de políticas. Se o CA Identity Manager não puder atualizar os nomes, você poderá atualizá-los manualmente em uma das seguintes interfaces:

- Para o CA SiteMinder Web Access Manager r12 ou superior, use a Interface de usuário administrativa.
- Para o CA eTrust SiteMinder 6.0 SP5, use a Interface de usuário do servidor de políticas.

Siga estas etapas:

1. Localize os realms para o Ambiente do CA Identity Manager.

   Esses realms são criados automaticamente (juntamente com outros objetos do SiteMinder) quando o CA Identity Manager se integra ao SiteMinder.

   Os realms usam a seguinte convenção de nomenclatura:

   - *Ambiente-do-Identity Manager*_ims_realm — protege o Console de usuário.
   - *Ambiente-do-Identity Manager*_pub_realm — ativa o suporte para tarefas públicas, como tarefas de autorregistro e senha esquecida. Esse realm será exibido apenas se você tiver configurado um alias público.

     Observação: se você estiver usando a Interface de usuário do servidor de políticas para modificar o realm, primeiramente, localize o domínio da política (*ambiente-do-Identity Manager*Domain) para o ambiente do CA Identity Manager. Os realms estão localizadas sob o domínio.

2. Modifique o recurso para o realm da seguinte forma:

   /iam/im/*novo_alias*

   Não remova a opção /iam/im/que precede o alias no filtro de recursos.

3. Salve as alterações.

Observação: Modificar as propriedades do CA Identity Manager fornece instruções sobre como alterar o alias no Management Console.

Modificar uma senha ou um shared secret do SiteMinder

Quando você instala as Extensões do CA Identity Manager para o Servidor de políticas, forneça a senha para a conta de administrador do SiteMinder que o CA Identity Manager usa para se comunicar com o Servidor de políticas.

Você pode alterar a senha. No entanto, ela deve ser criptografada. Para criptografar uma senha, use a ferramenta de senha que é fornecida com o CA Identity Manager.

Observação: certifique-se de que a variável JAVA_HOME esteja definida para o seu ambiente antes de alterar a senha do SiteMinder.

Siga estas etapas:

1. Criptografe a senha da seguinte maneira:
   a. Na linha de comando, navegue até *ferramentas_administrativas*\PasswordTool, onde *ferramentas_administrativas* é o local de instalação das Ferramentas administrativas, como nos exemplos a seguir:
      - **Windows:** <caminho_de_instalação>\tools\PasswordTool
      - **UNIX:** <caminho_de_instalação2>/tools/PasswordTool
   b. Digite o seguinte comando:

      pwdtools *nova_senha*

      Nesse comando, *nova_senha* é a senha a ser criptografada.

      Observação: para obter informações sobre as opções do utilitário pwdtools, digite o seguinte comando:

      pwdtools help
   c. Copie a senha criptografada.
2. Execute a etapa relevante, como se segue:
   - Se o CA Identity Manager estiver em execução em um servidor de aplicativos do WebLogic, execute as seguintes tarefas:
     a. No console do WebLogic, edite o adaptador de recursos do WebLogic no descritor de conector policyserver_rar.
     b. Adicione a senha criptografada como o valor da propriedade Password.
   - Se o CA Identity Manager estiver em execução em um servidor de aplicativos do JBoss, execute as seguintes tarefas:

     a. Abra ra.xml de *base_do_JBoss*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF.

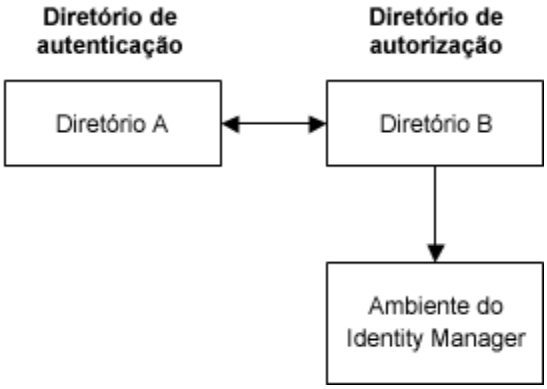
     b. Adicione a senha criptografada como o valor da config-property Password.
   - Se o CA Identity Manager estiver em execução em um servidor de aplicativos do WebSphere, execute as seguintes tarefas:

     a. No console do WebSphere, abra ra.xml.

     b. Adicione a senha criptografada como o valor da config-property Password.
3. Reinicie o servidor de aplicativos.

Configurar um ambiente do CA Identity Manager para usar diferentes diretórios para autenticação e autorização

Um administrador pode precisar gerenciar usuários cujos perfis existem em um repositório de usuários diferente daquele que é usado para autenticar o administrador. Em outras palavras, ao efetuar logon no Ambiente do CA Identity Manager, o administrador deve ser autenticado usando um diretório e autorizado a gerenciar usuários em um segundo diretório, como mostrado na ilustração a seguir:



Siga estas etapas:

1. Efetue logon em uma das interfaces a seguir:
   - No CA SiteMinder Web Access Manager r12 ou superior, efetue logon na Interface de usuário administrativa.
   - No CA eTrust SiteMinder 6.0 SP5, efetue logon na Interface de usuário do servidor de políticas.

   Observação: para obter informações sobre como usar essas interfaces, consulte a documentação da versão do SiteMinder que você está usando.
2. Crie dois diretórios de usuários.

   Um diretório faz referências aos dados de autenticação (perfis de administrador); o outro diretório faz referências aos dados de autorização (perfis de usuário).
3. No Management Console, crie um Ambiente do CA Identity Manager.

   Selecione o diretório de autorização com o diretório do CA Identity Manager.

4. Na interface da versão do SiteMinder usado, adicione o diretório de autenticação ao domínio do Ambiente do CA Identity Manager que você criou na etapa anterior.

   O domínio e outros objetos que são exigidos pelo SiteMinder são criados automaticamente quando você cria um Ambiente e o SiteMinder integra-se ao CA Identity Manager.

   O domínio usa a seguinte convenção de nomenclatura:

   *ambiente-do-Identity Manager*Domain

5. Verifique se esse diretório é exibido primeiro na lista de diretórios que estão associados ao domínio.
6. Localize o *ambiente-do-Identity Manager*_ims _realm.
7. Mapeie o diretório de autorização para o diretório de autenticação na seção Avançado da definição do realm.
8. Localize a seguinte resposta do *ambiente-do-Identity Manager*response_ims.
9. Adicione os atributos de resposta às respostas da seguinte maneira:

Campo	Valor
Atributo	Web-Agent-HTTP-Header-Variable
Tipo de atributo	atributo do usuário
Nome da variável	sm_userdn
Nome do atributo	SM_USERNAME

10. Salve as alterações.

    O CA Identity Manager agora usa diferentes diretórios para autenticação e autorização.

Como aprimorar o desempenho das operações do diretório LDAP

As operações do diretório podem levar mais tempo para serem processadas, pois todas as solicitações do CA Identity Manager para o diretório de usuários LDAP são roteadas por meio de um conjunto fixo de conexões.

Para aumentar a taxa de transferência das solicitações do CA Identity Manager para o repositório de usuários, configure o SiteMinder para abrir várias conexões com o mesmo diretório. Para tal procedimento, adicione o servidor LDAP várias vezes na caixa de diálogo Tolerância a falhas do diretório LDAP e configuração do balanceamento de carga na interface de usuário do Servidor de políticas.

O número de vezes para inserir o servidor LDAP (e o número de conexões a serem criadas) depende da carga do CA Identity Manager.

Apêndice A: Conformidade com a norma FIPS 140-2

Esta seção contém os seguintes tópicos:

Visão geral do FIPS

A publicação da norma FIPS (Federal Information Processing Standards) 140-2 é um padrão de segurança para as bibliotecas e os algoritmos de criptografia que um produto deve usar para criptografia. A criptografia FIPS 140-2 afeta a comunicação de todos os dados confidenciais entre componentes de produtos da CA e entre produtos da CA e produtos de terceiros. A FIPS 140-2 especifica os requisitos para o uso de algoritmos criptográficos em um sistema de segurança que protege dados confidenciais, não classificados.

O CA Identity Manager usa o AES (Advanced Encryption Standard - padrão de criptografia avançada) adaptado pelo governo dos Estados Unidos. O CA Identity Manager incorpora as bibliotecas criptográficas RSA Crypto-J v3.5 e Crypto-C ME v2.0, que foram validadas conforme cumprimento dos Requisitos de segurança da FIPS 140-2 para módulos criptográficos.

Comunicações

A criptografia FIPS abrange todas as comunicações de dados entre o CA Identity Manager e os seguintes componentes:

- Servidor do CA Identity Manager
- Servidor de provisionamento
- Gerenciador e clientes de provisionamento
- C++ Connector Servers
- Terminais do C++ Connector Server (se suportado pelo terminal)
- CA IAM Connector Servers (CA IAM CS)
- Terminais do CA IAM CS (se suportado pelo terminal)
- Connector Xpress (se suportado pelo terminal)
- Agentes de sincronização de senhas do Windows
- JIAM (Java Identity and Access Management)

Instalação

O instalador do CA Identity Manager permite que você configure o CA Identity Manager para estar em conformidade com a FIPS 140-2.

Todos os componentes em um ambiente do CA Identity Manager devem ser ativados para a FIPS 140-2 para que o CA Identity Manager ofereça suporte à FIPS 140-2. Você precisa de uma chave de criptografia FIPS para ativar a FIPS 140-2 durante a instalação. Para gerar uma chave de criptografia FIPS, execute a Ferramenta de senha (pwdtools.bat/pwdtools.sh) na qual você desempacota o pacote de instalação. A Ferramenta de senha está disponível nos seguintes locais:

- Windows: *raiz do pacote*\PasswordTool\bin\pwdtools.bat
- UNIX: *raiz do pacote*/PasswordTool/bin/pwdtools.sh

Observação: a Ferramenta de senha também é instalada no seguinte local:

```
<caminho_de_instalação>\PasswordTool\pwdtools.bat
```

Importante: use a mesma chave de criptografia FIPS 140-2 em todas as instalações e assegure a proteção o arquivo de chave gerado pela Ferramenta de senha.

Estabelecendo conexão com o SiteMinder

Ao estabelecer conexão com o CA SiteMinder durante a instalação do CA Identity Manager, esteja ciente de que o modo FIPS e as configurações da versão do produto são suportados somente conforme listado na tabela a seguir:

CA Identity Manager r12	SiteMinder	Versão do SiteMinder
Modo apenas FIPS	Modo apenas FIPS	r12
Modo apenas FIPS	Modo compatível com FIPS	r12
Modo não FIPS	Modo compatível com FIPS	r12
Modo não FIPS	Modo não FIPS	r6

Armazenamento de chave de arquivo

O CA Identity Manager usa o sistema de arquivos para o armazenamento de chave de criptografia FIPS. O administrador do CA Identity Manager é responsável por proteger arquivos contra acesso não autorizado. O administrador do CA Identity Manager pode proteger os arquivos definindo as permissões de acesso ao diretório para tipos específicos de grupo ou usuário, como o usuário que está autorizado a executar o CA Identity Manager.

A tabela a seguir lista o local dos arquivos de chave FIPS para cada componente do CA Identity Manager.

Componente	Local de instalação
Servidor do CA Identity Manager	*iam_im.ear*\config\com\netegrity\config\keys\FIPSkey.dat *iam_im.ear* é o local de instalação do CA Identity Manager no servidor de aplicativos.
Servidor de provisionamento	*Instalação do Servidor de provisionamento*\data\tls\keymgmt\imps_datakey
C++ Connector Server	*Instalação do Servidor de provisionamento*\data\tls\keymgmt\imps_datakey
Agente de sincronização de senhas	*Instalação do Servidor de provisionamento*\data\tls\keymgmt\imps_datakey

A Ferramenta de senha

O utilitário de ferramenta de senha compatível com a FIPS, pwdtools.bat (ou pwdtools.sh), pode gerar a chave de criptografia durante a instalação do CA Identity Manager, na linha de comando.

Edite o arquivo pwdtools.bat/pwdtools.sh antes de usar a ferramenta de senha e defina a variável JAVA_HOME conforme necessário.

Importante: o CA Identity Manager não oferece suporte à migração de dados ou à nova criptografia. Portanto, certifique-se de que as chaves de criptografia não sejam alteradas após a instalação.

Esse comando tem a seguinte sintaxe:

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <key file location>] [-f
<encrypting parameters file>]
```

JSAFE

Criptografe um valor de texto simples usando o algoritmo PBE.

Exemplo:

```
pwdtools -JSAFE –p minha_senha
```

Observação: nas versões anteriores, a senha para o administrador de inicialização é armazenada em texto não criptografado. Se você estiver fazendo uma atualização ou migrando para o CA Identity Manager r12.6 SP1 ou superior, será necessário criptografar manualmente a senha em texto não criptografado. Certifique-se de que a opção JSAFE seja especificada ao usar a ferramenta e siga estas etapas:

1. Após atualizar ou migrar para o CA Identity Manager r12.6 SP1 e superior, vá para o banco de dados do armazenamento de objetos do CA Identity Manager e pesquise a seguinte tabela:
   `IM_AUTH_USER`
2. Criptografe a senha em texto não criptografado usando a ferramenta de senha com JSAFE.
3. Substitua o texto não criptografado pela senha criptografada na tabela.

FIPSKEY

Para o instalador, crie um arquivo de chave FIPS. Você gera a chave antes de instalar o CA Identity Manager.

Exemplo:

```
pwdtools -FIPSKEY –k C:\caminho_da_chave\FIPSkey.dat
```

Onde *caminho_da_chave* é o caminho completo para o local onde você deseja armazenar a chave FIPS.

A ferramenta de senha cria a chave FIPS no local especificado. Durante a instalação, você fornece o local do arquivo de chave FIPS ao instalador.

Observação: certifique-se de proteger a chave definindo as permissões de acesso ao diretório para tipos específicos de grupo ou usuário, como o usuário que está autorizado a executar o CA Identity Manager.

FIPS

Criptografe um valor de texto simples usando um arquivo de chave FIPS. A FIPS usa o arquivo de chave FIPS existente.

Exemplo:

```
pwdtools -FIPS –p firewall -k C:\caminho_da_chave\FIPSkey.dat
```

Onde *caminho_da_chave* é o caminho completo para o diretório da chave FIPS.

Observação: use o mesmo arquivo de chave FIPS que você especificou durante a instalação.

RC2

Criptografe um valor de texto simples usando o algoritmo RC2.

Importante: O CA Identity Manager usa o arquivo de chave FIPS para verificar se o aplicativo deve ser iniciado no modo FIPS ou não. Portanto, certifique-se de que o nome do arquivo de chave seja FIPSKey.dat com o seguinte caminho de implantação do servidor de aplicativos:

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

onde iam_im.ear está no diretório de implantação do servidor de aplicativos, por exemplo:

```
base_do_jboss\server\default\deploy
```

Detecção do modo FIPS

Para determinar se o CA Identity Manager está operando no modo FIPS ou em modo não FIPS, use a página de status do Ambiente do CA Identity Manager.

Para exibir a página de status, digite o seguinte URL em um navegador:

`http://nome_do_servidor/iam/im/status.jsp`

nome_do_servidor

Determina o nome de domínio totalmente qualificado do servidor em que o CA Identity Manager está instalado, por exemplo, meu_servidor.minha_empresa.com. Neste exemplo, o URL completo é:

http://meu_servidor.minha_empresa.com/iam/im/status.jsp

O status do FIPS é exibido na parte inferior da página.

Observação: você também pode verificar se o CA Identity Manager está operando no modo FIPS localizando o arquivo de chave a seguir:

`/config/com/netegrity/config/keys/FIPSkey.dat`

Se esse arquivo existir, o CA Identity Manager estará operando no modo FIPS.

O utilitário de ferramenta de senha, pwdtools.bat (ou pwdtools.sh) cria o arquivo de chave FIPSkey.dat durante a instalação do CA Identity Manager.

Formatos de texto criptografado

O nome do algoritmo é adicionado ao texto criptografado como um prefixo e informa o CA Identity Manager qual algoritmo foi usado na criptografia.

No modo FIPS, o prefixo é {AES}. Por exemplo, se você criptografar o texto "password", o texto criptografado será semelhante ao seguinte exemplo:

{AES}:eolQCTq1CGPyg6qe++0asg==

No modo não FIPS (ou modo JSAFE), dependendo do algoritmo, o prefixo (tag de algoritmo) é {PBES} ou {RC2}. Por exemplo, se você criptografar o texto "password", o texto criptografado será semelhante a este:

{PBES}:gSex2/BhDGzEKWvFmzca4w==

Você pode criar chaves dinâmicas usando a tarefa Chaves secretas em Sistema. Se você definir chaves dinâmicas, a ID de chave será inserida entre uma tag de algoritmo e um delimitador de tag (':'). A ausência de uma ID de chave nos dados criptografados indica que uma chave embutida em código foi usada para criptografia. Isso pode ser usado para fins de compatibilidade com versões anteriores ou se nenhuma chave dinâmica for definida para o algoritmo fornecido.

Informações criptografadas

As informações a seguir do CA Identity Manager são criptografadas:

- Senhas na configuração da origem de dados para Jboss
- Informações de recuperação de senha esquecida
- Segredo de retorno de chamada do Servidor de provisionamento
- Informações da sessão de fluxo de trabalho
- Informações de conexão do Servidor de políticas

O CA Identity Manager usa bibliotecas JSafe para criptografar ou descriptografar dados. Para garantir que as bibliotecas não sejam violadas, o CA Identity Manager usa o código de autoteste CryptoJ durante a inicialização.

Após a execução dos testes, mensagens CryptoJ, que informam o status do teste, aparecem no log do servidor de aplicativos. O log contém uma das seguintes mensagens:

```
[ims.default] * CryptoJ was initialized properly.

[ims.default] !!! CryptoJ was not initialized properly. !!!
```

Log do modo FIPS

Os seguintes componentes do CA Identity Manager indicam em arquivos de log se o modo FIPS está ativado:

- Servidor do CA Identity Manager
- Servidor de provisionamento
- C++ Connector Server
- CA IAM CS
- Gerenciador de provisionamento
- Agente de sincronização de senhas

Em todos os casos, a entrada de log que indica que o modo FIPS está ativado termina com a seguinte sequência de caracteres:

FIPS 140-2 MODE: ON

Apêndice B: Substituindo certificados do CA Identity Manager por certificados SSL assinados pelo SHA-2

O hash do certificado SSL SHA-2 é um algoritmo criptográfico desenvolvido pelo NIST (National Institute of Standards and Technology) e NSA (National Security Agency). Os certificados SHA2 são mais seguros do que todos os algoritmos anteriores. No CA Identity Manager, você pode configurar os certificados SSL assinados pelo SHA-2 no lugar de certificados que são assinados com a função hash SHA-1.

Observação: para obter mais informações sobre como configurar certificados SSL, consulte o *Guia de Instalação*.

A tabela a seguir mostra o local do caminho no servidor do CA Identity Manager, onde você poderá colocar os certificados assinados pelo SHA-2:

Certificados	Local de instalação	Descrição
Certificado do Servidor de provisionamento	[Dir de instalação do Servidor de provisionamento]/data/tls/server/eta2_servercert.pem [Dir de instalação do Servidor de provisionamento]/data/tls/server/eta2_serverkey.pem *instalação_cs*/ccs/data/tls/server/eta2_servercert.pem *instalação_cs*/ccs/data/tls/server/eta2_serverkey.pem *instalação_cs*/jcs/conf/eta2_server.p12	Usado pelo Servidor de provisionamento no formato .pem e pelo CA IAM CS no formato .p12 (incluindo certificado assinado, chave privada e certificado CA raiz). **Observação**: importe o eta2_server.p12 no *instalação_cs*/jcs/conf/ssl.keystore under the alias eta2_server e remova a entrada existente. A senha ssl.keystore é a senha do servidor de conectores que é fornecida durante a instalação.

Certificados	Local de instalação	Descrição
Certificado do Cliente de provisionamento	[Dir de instalação do Servidor de provisionamento]/data/tls/client/eta2_clientcert.pem [Dir de instalação do Servidor de provisionamento]/data/tls/client/eta2_clientkey.pem [Dir de instalação do Gerenciador de provisionamento]/data/tls/client/eta2_clientcert.pem [Dir de instalação do Gerenciador de provisionamento]/data/tls/client/eta2_clientkey.pem *instalação_cs*/ccs/data/tls/client/eta2_clientcert.pem *instalação_cs*/ccs/data/tls/client/eta2_clientkey.pem *instalação_cs*/jcs/conf/eta2_client.p12	Usado pelo Servidor de provisionamento no formato .pem e pelo CA IAM CS no formato .p12 (incluindo certificado assinado, chave privada e certificado CA raiz).
Certificado confiável do Diretório de provisionamento	*instalação_cadir*/config/ssld/impd_trusted.pem	Usado pelo CA Directory no formato .pem. Ele deve apresentar conteúdo de certificado na seguinte estrutura: -----BEGIN CERTIFICATE----- Conteúdo do certificado -----END CERTIFICATE-----
Certificado de personalidade do Diretório de provisionamento	*instalação_cadir*/config/ssld/personalities/impd-co.pem *instalação_cadir*/config/ssld/personalities/impd-inc.pem *instalação_cadir*/config/ssld/personalities/impd-main.pem *instalação_cadir*/config/ssld/personalities/impd-notify.pem *instalação_cadir*/config/ssld/personalities/impd-router.pem	Usado pelo CA Directory no formato .pem.

Certificados	Local de instalação	Descrição
Certificado CA raiz	[Dir de instalação do Servidor de provisionamento]/data/tls/et2_cacert.pem [Dir de instalação do Gerenciador de provisionamento]/data/tls/et2_cacert.pem *instalação_cs*/ccs/data/tls/ et2_cacert.pem *instalação_conxp*/lib/jiam.jar [Dir de instalação do servidor de aplicativos]/iam_im.ear/library/jiam.jar	O certificado é importado no keystore do Connector Xpress localizado em [dir de instalação do Connector Xpress]/conf/ssl.keystore. O certificado também deve ser importado no keystore jiam.jar. Para importar, extraia o jar, importe o certificado no admincacerts.jks e empacote novamente o conteúdo jar. A senha do keystore de admincacerts.jks é "changeit". Verifique se todas as cópias do jiam.jar foram substituídas.

Comandos úteis

O programa OpenSSL é uma ferramenta de linha de comando para usar as diversas funções de criptografia da biblioteca do OpenSSL. Essa ferramenta é fornecida com o IMPS localizado em [dir de instalação do Servidor de provisionamento]/bin.

A tabela a seguir mostra alguns comandos úteis do programa OpenSSL para executar vários comandos relacionados ao gerenciamento de certificados:

Comandos	Descrição
`openssl x509 –in cert.pem –text –noout`	Imprime o conteúdo do certificado .pem.
`openssl.exe pkcs12 -in my.pkcs12 –info`	Imprime o conteúdo do arquivo .p12.
`openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12`	Converte o cert/par de chaves .pem em .p12.
`keytool –list –v -keystore my.keystore`	Imprime o conteúdo de um keystore java.
`keytool –list –v –alias myalias –keystore my.keystore`	Imprime o conteúdo de um alias específico em um keystore java

Comandos		Descrição
	`keytool –delete –alias myalias –keystore my.keystore`	Exclui um alias de um keystore java
	`keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias`	Importa um arquivo .p12 em um keystore java.
	`keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore`	Importa um certificado CA raiz do .pem em um keystore java.