Xerox
DocuShare®

DocuShare
Guia do Active Directory/LDAP

Data de publicação: Março de 2011

Este documento fornece suporte a DocuShare Versão 6.6.1

Preparado por:

Xerox Corporation
DocuShare Business Unit
3400 Hillview Avenue
Palo Alto, Califórnia 94304
EUA

Índice analítico

Capítulo 1 A estrutura LDAP

Capítulo 2 Configuração LDAP/DocuShare

A estrutura LDAP 1

Visão Geral LDAP

Ainda que algumas informações sejam fornecidas para compreender conceitos básicos, este guia não fornece instruções para implementação do LDAP ou Windows Active Directory. As informações deste guia pressupõem que o servidor do Active Directory já está instalado e sendo gerenciado pelo administrador do Active Directory ou pelo administrador LDAP. Os exemplos mostrados neste anexo usam o Servidor Microsoft Windows 2000 com o Microsoft Internet Explorer (IE) V.6.X.

O LDAP, ou Protocolo de Acesso ao Diretório Leve, é uma alternativa leve para o Protocolo de Acesso ao Diretório X.500 (DAP). O LDAP usa a pilha do protocolo TCP/IP da pilha do protocolo OSI requerido pelo X.500. Como alternativa leve, o LDAP simplifica algumas operações, mas não têm assistência de alguns dos recursos do X.500 DAP.

O LDAP é o protocolo que está sendo usado entre um cliente do diretório e um servidor. O LDAP define o conteúdo das mensagens trocadas entre um cliente LDAP e um servidor LDAP. O cliente LDAP, no caso do servidor DocuShare, se comunica com o servidor LDAP. O servidor LDAP, atuando como um portal, acessa o diretório LDAP. O diretório LDAP pode ser implementado como servidor individual LDAP ou como diretório em um servidor X.500.

O DocuShare envia as consultas de conteúdo do diretório ao servidor LDAP. O servidor LDAP acessa o diretório, seja LDAP ou X.500, e devolve os resultados ao DocuShare. O protocolo LDAP permite leitura e atualização de operações do cliente nos dados do diretório.

Nota: O DocuShare não atualiza os dados do diretório LDAP. O DocuShare apenas lê os resultados das consultas que envia ao servidor LDAP.

Estrutura LDAP

As entradas em um diretório LDAP são organizadas em uma estrutura hierárquica específica.

Diretórios

Um diretório é um tipo especial de banco de dados. Os diretórios são otimizados para receber um alto volume de solicitações de **leitura** junto ao acesso à **gravação** que geralmente é limitado aos administradores do sistema. De modo semelhante às páginas em branco de um catálogo telefônico, um diretório LDAP é mais lido do que atualizado.

Do mesmo modo que o catálogo telefônico lista indivíduos, empresas e organizações, o diretório LDAP lista objetos como usuários, servidores e impressoras. Do mesmo modo como o catálogo telefônico contém informações sobre cada listagem, como nome, número e endereço, as entradas em um diretório LDAP contêm as informações pertinentes sobre cada objeto. Essas informações de objetos são chamadas de **atributos**.

Atributos

Cada entrada de objeto dentro de um diretório LDAP contém um ou mais atributos. Cada atributo compreende um **tipo** e um **valor**. Uma entrada do catálogo telefônico tem atributos como nome de uma pessoa e um número de telefone correspondente. Os atributos LDAP aparecem no formato **Nome comum=Jane Smith número de telefone=555-555-5555**. Tabela 1–1

Tabela 1–1:

Atributo LDAP	Alias de Atributo	Descrição de Atributo	Exemplo
Nome comum	cn	Nome comum de uma entrada	Jane Doe
Sobrenome	sn	Sobrenome da pessoa	Doe
ID do usuário	uid	ID do usuário ou nome de logon	jdoe
número de telefone	-	Número de telefone	555-123-4567
Nome da Unidade Organizacional	ou	Nome da Unidade Organizacional	meu departamento
organização	o	Nome da organização	minha empresa
Componente de domínio	dc	Componente DNS	xyz.com

Nome Diferenciado relativo

O Nome Diferenciado Relativo ou **RDN** é representado na forma de um **par de dados de atributo** (tipo e valor), como:

cn=Jane Doe

uid=smith

ou=marketing

dc=Xerox

Nome Diferenciado

Entradas no diretório são organizadas pelo Nome Diferenciado (DN). O Nome Diferenciado é semelhante ao caminho absoluto para um arquivo no sistema de arquivos Windows. O DN de um objeto é feito do nome e da localização da entrada no diretório.

Um DN é composto de pares de dados de atributo RDN, separados por vírgulas, como:

cn=John Smith,ou=marketing,dc=Xerox,dc=com

cn=John Smith,ou=engenharia,dc=Xerox,dc=com

O caminho para um DN é da ordem mais baixa para a mais alta. Essa ordem é oposta àquela usada no sistema de arquivos Windows. Assim como o sistema de arquivos Windows permite uma variedade de arquivos com o mesmo nome, se cada um for de um diretório diferente, vários usuários podem usar o mesmo RDN desde que o DN seja exclusivo. Como mostra o exemplo DN abaixo, um John Smith pode ser listado no departamento de marketing e um no de engenharia.

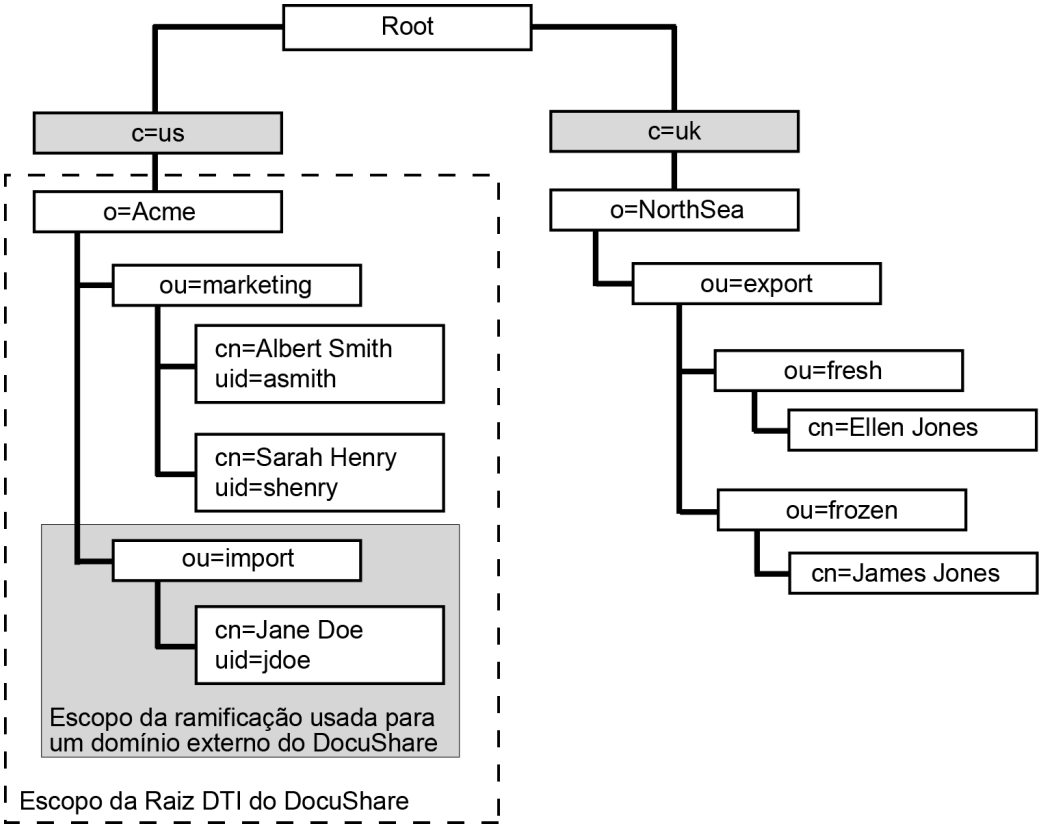
Árvore de Informações do Diretório

O diretório arranja entradas em uma estrutura hierárquica semelhante a uma árvore chamada Árvore de Informações de Diretório ou **DIT**. Um DIT se baseia em um Nome Diferenciado das entradas, com os Nomes Diferenciados organizados em ramificações que geralmente representam uma estrutura organizacional e geográfica. O Microsoft Active Directory muitas vezes é organizado por domínios geográficos ou por DNS.

Organização DIT baseada em domínios geográficos

A ilustração abaixo mostra como o administrador da corporação de importação de frutos do mar pode organizar a hierarquia do diretório LDAP de acordo com a geografia. Para hospedar um servidor DocuShare para a empresa Acma nos EUA, o administrador definiria a **Raiz DIT** como **o=Acme, c=us**.

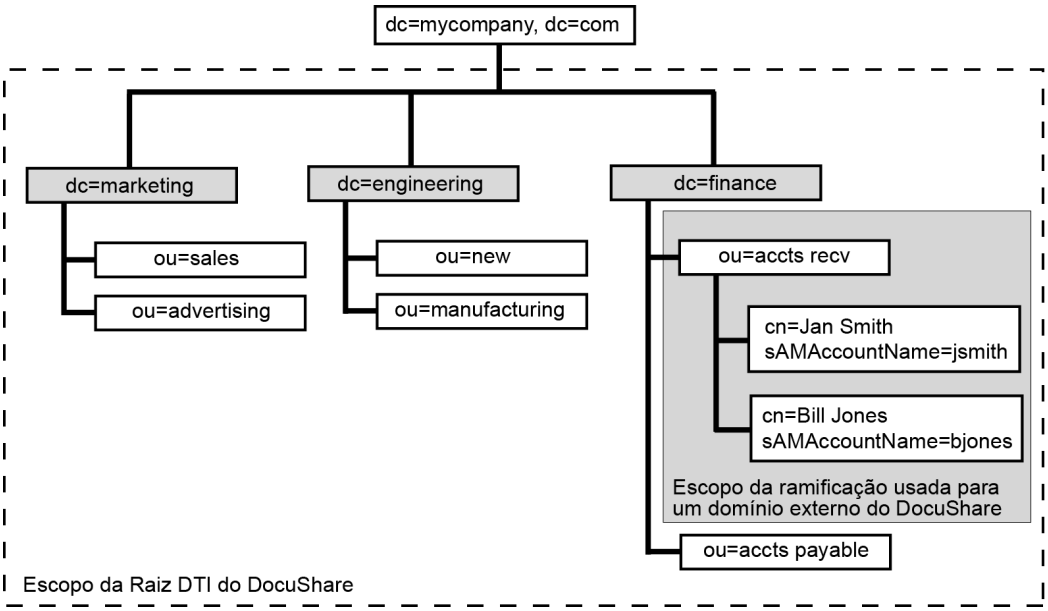
Para definir um **domínio externo** para o departamento de importação da Acme, o administrador definiria o Localizador de Serviço de Diretório e Autenticação Relativa como **ou=importação**.



Organização DIT baseada em DNS

A ilustração abaixo mostra como o administrador da corporação pode organizar a hierarquia do diretório LDAP de acordo com o DNS. A empresa usa os servidores do domínio Windows para as divises de marketing, engenharia e finanças. Ao definir a raiz DIT como **dc=minha empresa**, **dc=com**, o administrador pode criar um domínio externo DocuShare para cada departamento em uma divisão.

Para definir um **domínio externo** para o departamento de Contas a receber na divisão de Finanças, o administrador definiria o Localizador de Serviço de Diretório e Autenticação Relativa como **ou=contas a receber**, **dc=finanças**.



Configuração LDAP/DocuShare 2

Configuração DocuShare

Para configurar seu site DocuShare para usar o LDAP/Active Directory, faça logon como admin em seu site DocuShare e realize os procedimentos de A a F. Para configurar o DocuShare corretamente, use a **Ferramenta de administração do Active Directory** ou o **comando LDIFDE do Active Directory** para coletar as informações necessárias. Ambos os processos de coleta de informações estão descritos neste capítulo.

A — Configuração LDAP

Use a página **Configuração LDAP** de administração do DocuShare para estabelecer uma conexão entre seu servidor DocuShare e seu servidor LDAP, assim como para definir a Árvore de Informações do Diretório que é usada para criar domínios externos ao DocuShare.

1. Abra a página **Configuração LDAP** da interface de usuário de administração.
2. Insira no campo **Host(s)** o nome do Host ou endereço IP ou o nome DNS do servidor do LDAP/Active Directory (FQDN preferencial ou endereço IP se não for FQDN). Use um espaço para separar várias entradas de endereço do servidor LDAP.
3. Insira no campo **Porta** o número da porta usado por seu servidor LDAP se não for o número de porta padrão 389.
4. **Opcional**: Insira no campo **SSL** o número da porta usado para a Secure Socket Layer.
5. Insira no campo **Raiz de DIT** as informações obtidas usando a busca da Ferramenta de Administração do Active Directory para uma referência ao contexto de nomenclatura. Por exemplo, essas informações seriam em formato de dc=adoc,dc=Xerox,dc=com.
6. Insira o atributo **cn** no campo **Chave RDN do usuário**. Esse é o alias para o atributo nome comum. O atributo pode ser diferente, dependendo do tipo de servidor LDAP usado (iPlanet, etc.).
7. Selecione o **Agente** no campo **Agente do sistema**.

   A maioria dos servidores do Active Directory requer um login de conta de Serviço ou de Agente.
8. Insira o nome diferenciado (DN) da conta do agente no campo **DN**.

   Por exemplo, cn=john,cn=usuários,dc=adoc,dc=xerox.

9. Insira a senha da conta do Agente no campo **Senha**.
10. Vá à seção Testar LDAP na parte inferior da página Configuração LDAP.

    Use Testar LDAP para verificar se há uma conexão válida e logon bem-sucedido no servidor LDAP.
11. Selecione o **Agente** no campo Conexão DN.
12. Insira o nome diferenciado que inseriu no campo DN na etapa 8 no campo **Nome**.
13. Insira a senha que inseriu no campo Senha na etapa 9 no campo **Senha**.
14. Clique em **Aplicar e testar**

    Você verá uma mensagem "Sucesso" se tiver estabelecido corretamente a conexão com o servidor LDAP.
15. Repita as etapas de 11 a 14, mas selecione o **Usuário** no campo Conexão DN.

Nota: Este teste não verifica a validade da Raiz DIT nem do Localizador de Autenticação Relativo de quaisquer domínios externos. O teste verifica apenas se o DocuShare recebeu uma resposta positiva do servidor LDAP.

B — Configuração avançada

Use a configuração LDAP avançada para definir como classes de objeto específicas são definidas em seu servidor LDAP.

1. Clique em **Avançado** localizado na parte inferior da página Configuração LDAP.

   A página Configuração LDAP avançada aparece
2. Na parte inferior da página Configuração LDAP avançada, localize o título da seção **Classes de Objeto**.
3. No campo **Usuário**, substitua a entrada padrão **person** pela palavra **usuário** (tudo em letras minúsculas).
4. No campo **Grupo estático**, substitua a entrada padrão **groupOfUniqueNames** pela palavra **grupo** (tudo em letras minúsculas).
5. Clique em **Aplicar**.

C — Ativar os Provedores LDAP

Use os **Serviços de Segurança** da administração DocuShare e páginas de **Serviço de Diretório** para ativar ambos os Serviços do Provedor do Diretório e de Segurança para LDAP. Isso permite que os usuários selecionem os Domínios Externos LDAP da lista suspensa Domínios nos prompts do Logon.

1. Abra a página **Serviços de Segurança** da interface de usuário de administração.
2. Na página Serviços de Segurança, selecione a caixa **LDAP** para ativar o LDAP como provedor de autenticação para todos os domínios externos, e clique em **Aplicar**.
3. Abra a página **Serviços do Diretório** da interface de usuário de administração.
4. Na página Serviços do Diretório, selecione a caixa **LDAP** para ativar o LDAP como provedor de serviço de diretório para todos os domínios externos, e clique em **Aplicar**.

D — Associar usuário

Utilize a página **Associar usuário** da administração DocuShare para estabelecer uma associação entre as propriedades da conta DocuShare e os atributos da conta LDAP.

1. Abra a página **Associar usuário** da interface de usuário de administração.
2. No campo **Nome**, insira o atributo que o LDAP usa para o nome do usuário. De modo geral, este é seu **nome próprio**.
3. No campo **Nome de família**, insira o atributo que o LDAP usa para o nome de família do usuário. Normalmente, este é o **sobrenome** ou **sn**. Esse campo é obrigatório.
4. No campo **Nome do usuário**, insira o atributo que o LDAP usa para o nome de logon de um usuário. De modo geral, este é seu **sAMAccountName**. Esse campo é obrigatório.
5. Se o diretório LDAP contiver atributos para adição de atributos, tais como endereço de email, caixa de correio, telefone ou home page, insira tais atributos nos campos apropriados na página Associar usuário.
6. Clique em **Aplicar** e salve essa informação.

E — Associar grupo

Utilize a página **Associar grupo** da administração DocuShare para estabelecer uma associação entre as propriedades da conta DocuShare e os atributos da conta LDAP.

1. Use a informação obtida usando o comando LDIFDE e insira aqueles atributos nos campos adequados na página Associar grupo.

   Para mais informações, consulte a seção deste capítulo chamada **O Comando LDIFDE do Active Directory/Analisar o conteúdo do arquivo adexport.text/E. Propriedades de Associar grupo**.
2. Clique em **Aplicar** e salve essa informação.

F — Criar domínio

Use a página **Domínios** da administração DocuShare para criar domínios externos em seu site DocuShare local. Cada domínio externo DocuShare representa uma ramificação na árvore do diretório LDAP. E cada ramificação contém uma coleção de contas de grupo e usuário DocuShare.

1. Abra a página **Domínios** da interface de usuário de administração.
2. No campo **Adicionar**, insira o nome do domínio externo que quer adicionar a seu site local.

   Este pode ser simplesmente um nome descritivo, como Engenharia.
3. Selecione **LDAP** em ambos os Serviços de Segurança e de Provedores e as páginas Serviços de Diretório e de Provedores da interface de usuário do Admin.
4. No campo **Localizador de autenticação relativo**, insira um ou mais pares de atributos para definir o caminho para o diretório que contém as contas de grupo e do usuário.

Use os componentes do atributo do DN que estão à esquerda da raiz DIT e à direita do RDN do usuário.

Por exemplo, o DN para uma conta de usuário em um domínio é cn=nome dos usuários,ou=engenharia,ou=docushare,dc=adoc,dc=xerox,dc=com. O domínio Engenharia está na ramificação ou=engenharia, ou=docushare. A raiz de DIT é dc=adoc, dc=xerox, dc=com.

5. No campo **Localizador do Serviço de Diretório Relativo**, digite um ou mais pares de atributos.

   Utilize os mesmos pares de atributos que inseriu no campo Localizador de Autenticação Relativo.

   O DocuShare 6.5 é compatível apenas com LDAP para serviços de Diretório e Autenticação, assim os valores para o Localizador de Autenticação Relativo e para o Localizador de Serviço de Diretório Relativo são idênticos.

6. Clique em **Adicionar** para adicionar este domínio externo a seu menu de logon local.

G — Adicionar

Após ter preenchido as páginas de Configuração LDAP, Provedores, Associar usuários e Domínios, você está pronto para adicionar contas de grupo e usuários ao domínio externo em seu site DocuShare. Se você fosse Listar usuários ou Listar Grupos no novo domínio externo, o domínio estaria vazio. Agora, você precisa abrir o domínio no servidor LDAP e selecionar as contas de grupo e de usuário que quer como membros de seu domínio externo local.

1. Abra a página **Adicionar** da interface de usuário de administração.

   Essa não é a mesma página que **Adicionar usuário**.

2. Selecione um **Tipo de conta** e um **Domínio** externo.
3. Selecione como quer filtrar a lista de contas do domínio externo e inclua um filtro simples como o nome ou nome parcial ou uma propriedade de objeto específica.
4. Clique em **Ir** para exibir uma lista dos tipos de conta que selecionou.
5. Selecione as contas que você deseja que apareçam localmente no site e clique na seta **Adicionar** para movê-las para o campo **Selecionado**. Se não incluir uma conta no campo Selecionado, impossibilita que usuários ou grupos acessem seu site.
6. Quando concluído, clique em **Adicionar conta**. O DocuShare adiciona as contas de usuário ou de grupo à lista local do domínio externo.
7. Na página **Ir para Listar/Localizar/Adicionar Usuário** você verá os usuários designados ao novo domínio externo.

H — Exibir Logon

1. Volte para a home page do DocuShare.
2. Na seção de logon da home page, o novo domínio externo deve aparecer no menu **Domínio Logon**
3. Um usuário de um domínio externo deve selecionar o domínio correto para logon ou o DocuShare exibe uma mensagem de erro de logon e uma solicitação para tentar novamente.

LDAP e SSL

Secure Socket Layer, ou SSL, é um protocolo que foi desenvolvido pela Netscape para transmissão de documentos confidenciais via Internet. SSL funciona utilizando uma chave pública para criptografar dados que são transferidos por uma conexão SSL. Tanto o navegador Netscape quanto o Internet Explorer são compatíveis com SSL. Muitos websites usam SSL para obter informações do usuário confidenciais, como um número de cartão de crédito e senhas de contas. Uma sessão SSL é iniciada ao usar uma URL que comece com **https** ao invés de **http**.

Certificados

Quando usar o SSL, os servidores e clientes usam certificados para dar prova de identidade antes de estabelecer uma conexão segura. Um certificado também contém chaves públicas e privadas que são usadas para estabelecer uma sessão. Servidores e clientes usam **chaves de sessão** para criptografar e descriptografar dados.

Certificados podem ser autoassinados ou podem ser emitidos por uma autoridade de certificação (CA) tal como Entrust, Equifax, Valicert ou Verisign. Certificados emitidos por uma CA são considerados advindos de uma **autoridade independente confiável**. Basicamente, a autoridade independente garante a identidade de um usuário. A maioria dos navegadores de clientes são configurados para reconhecer e autorizar certificados emitidos por CAs.

Quando os certificados são autoassinados, o usuário atua como uma autoridade de certificação. Um certificado autoassinado deve estar instalado no repositório de autoridades dos navegadores e os certificados não são reconhecidos como autoridade independente confiável.

Os certificados são emitidos como certificados de servidor ou de cliente. O DocuShare não é compatível com certificados sediados no cliente. O DocuShare utiliza uma cópia do certificado do servidor LDAP para estabelecer a sessão LDAP com o servidor LDAP.

Importar o certificado para o DocuShare

Dependendo da CA que emitiu o certificado, o administrador pode precisar importar o certificado do servidor LDAP para o repositório de certificados do navegador do servidor DocuShare. Se o certificado for autoassinado, o administrador **deve** importar o certificado para o repositório de certificados do navegador do servidor DocuShare.

Para importar o certificado de um servidor LDAP específico:

1. Abra um navegador no servidor DocuShare.
2. Conecte ao servidor LDAP usando o endereço - https://<your.ldap.server>:636.

   Porta 636 é o porta padrão para SSL.
3. Se o certificado não tiver sido instalado no navegador do servidor DocuShare, uma janela Alerta de Segurança aparece solicitando que instale o certificado.
4. Para instalar o certificado, clique em **Exibir Certificado** na parte inferior da janela Alerta de Segurança.

   Uma janela Certificado é exibida.
5. Clique na guia **Detalhes** e no botão **Copiar para Arquivo**.

Exportar o certificado e salvar como um arquivo CER

Após ter importado o certificado do servidor LDAP, você precisa exportar o certificado para o diretório DocuShare e salvá-lo como arquivo certificado.

Para exportar o certificado e salvá-lo como arquivo certificado:

1. Clique em **Avançar** na parte inferior da janela Assistente.

   Se o certificado contiver uma chave privada, a janela Exportar Chave Privada é exibida.

2. Na janela Exportar Chave Privada, selecione **Não, não exporte a chave privada**.

   O DocuShare não precisará de uma chave privada para estabelecer uma sessão SDL com o servidor LDAP.

3. Clique em **Avançar**.

   A janela Exportar Formato de Arquivo aparece.

4. Selecione **Base-64 codificado X.509 (.CER)** na janela Exportar Formato de Arquivo.

5. Clique em **Avançar**.

   A janela de prompt Arquivo para Exportar aparece.

6. Insira no campo **Nome de arquivo** o caminho do diretório para um local em sua unidade de disco para a qual queira exportar o certificado. Por exemplo **D:**.

7. Insira no campo Nome do arquivo, atrás do caminho do diretório, um nome de arquivo para o certificado com a extensão **.cer**. Por exemplo **D:\SSL_Cert4LDAP.cer**.

8. Clique em **Avançar** para concluir a exportação do certificado.

   A janela Assistente Concluindo a Exportação do Certificado é exibida.

9. Clique em **Concluir** para fechar o Assistente.

   O certificado LDAP é salvo como arquivo .cer em seu site DocuShare.

10. Siga as instruções na página seguinte, **Colocar o certificado no DSTrustStore**

Colocar o certificado no DSTrustStore

Agora que salvou o certificado como arquivo certificado, precisa colocá-lo no arquivo **DSTrustStore**.

Para colocar o arquivo .cer do certificado no arquivo DSTrustStore:

1. Localize o arquivo .cer que exportou usando o Assistente Exportação de Certificado.
2. Copie o arquivo .cer no diretório DocuShare que contém o arquivo DSTrustStore **jdk1.5.0\jre\lib\security**.
3. Abra a janela de prompt de comando e navegue ao diretório que contém **dstruststore**.

```
Microsoft Windows 2000 [Versão 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>cd\xerox\docushare\jdk1.5.0\jre\lib\security
C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security\dir
 Volume na unidade C é Disco Local
 Volume no Número de Série é 508B-0D2F
 Diretório do C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security
18-11-02   15:55         <DIR>          -
18-11-02   15:55         <DIR>          --
02-10-02   12:25                7,365 cacerts
02-10-02   12:26                  589 dstruststore
02-10-02   12:26                2,271 java.policy
02-10-02   12:26                4,115 java.security
10-11-02   15:43                  844 SLL_Cert4LDAP.cer
          5 arquivo(s)         15,184 bites
          2 Dir(s)    1,486,024,704 bites livre

C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security
```

4. No prompt do comando, insira o comando **set PATH** para definir a variável do ambiente PATH. Use **set PATH=%PATH%;**<seu diretório DocuShare>**\jdk1.5.0\jre\bin**.

```
C:\Xerox\Docushare\jdk1.5.0\jre\lib\security>set
PATH=%PATH%;C:\XEROX\DocuShare\jdk1.5.0\jre\bin
```

5. Após ter definido a variável PATH, no prompt de comando, insira **keytool**, sem argumentos.

   A ajuda do Utilitário keytool é exibida. O utilitário keytool coloca o certificado SSL no DSTrustStore.

6. No prompt de comando, insira o comando do utilitário keytool **keytool -import -alias <alias_name> -file <cert_file> -keystore dstruststore**

   Substitua **<alias_name>** por um nome exclusivo para o arquivo certificado.

   Substitua **<cert_file>** pelo nome do arquivo certificado (.cer) que tinha exportado e copiado para o diretório que contém o arquivo dstruststore.

7. Pressione **Enter** para iniciar o comando.

   Uma solicitação de senha é exibida.

8. Insira a **senha** e pressione **Enter**.

```
C:\Xerox\Docushare\jdk1.5.0\jre\lib\security>keytool -import -alias Test LDAPss1 -file
SDL_Cert4LDAP.cer -keystore dstruststore

Insira a senha do keystore: senha

Proprietário: Certificado de Criptografia do Arquivo OU=EFS, L=EFS,
CN=Administrador

Emissor: Certificado de Criptografia do Arquivo OU=EFS, L=EFS, CN=Administrador

Número de Série: 5ee8abd44c2cd2b14ffbee159f03d354

Válido de: Ter 19 fev 10:57:21 PST 2002 até: Qui 26 jan10:57:21 PST 2102

Impressões digitais do certificado:

        MD5: 78:C7:A3:04:32:69:EB:97:76:FE:F4:8A:11:A2:65:26

        SHA1: 02:DD:9A:BE:BE:DE:3C:AA:22:AE:14:9A:F2:F2:5B:11:61:6D:5A:5F

Autoriza esse certificado? [não]: sim

O certificado foi adicionado ao keystore

C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security>
```

9. Examine a saída da tela para garantir que o keytool adicionou com sucesso o certificado ao keystore. Se o keytool tiver concluído a operação, seu servidor DocuShare estará pronto para usar o certificado para estabelecer a sessão SSL com seu servidor LDAP.

10. Quando tiver terminado de importar o certificado, reinicialize seu servidor DocuShare.

A ferramenta de administração do Active Directory

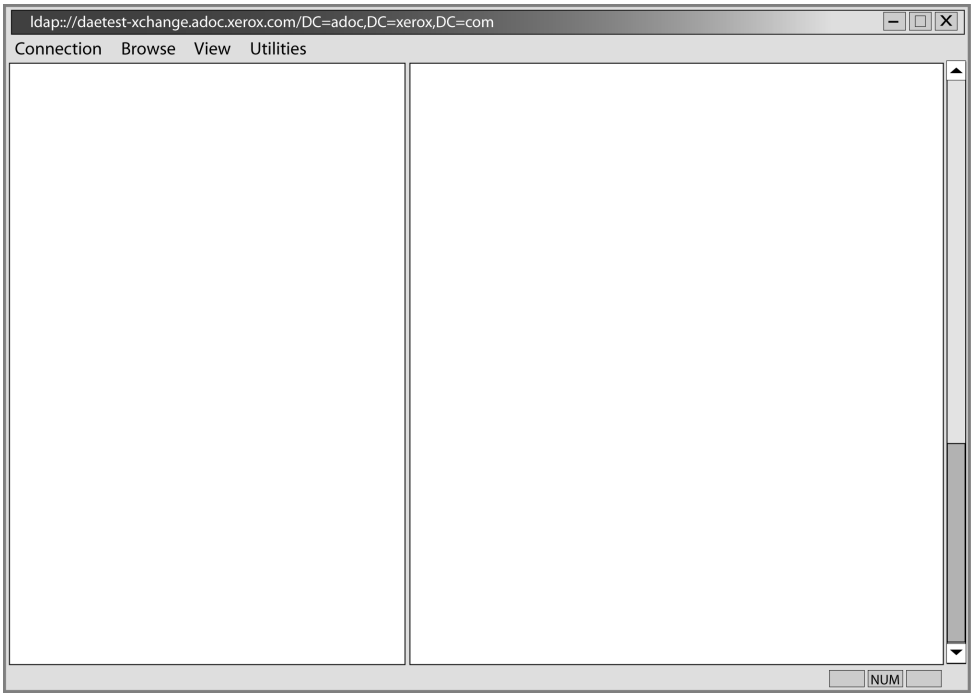
Você pode usar a Ferramenta de Administração do Active Directory (ldp.exe) para desempenhar várias operações em um Active Directory e consultar um servidor do diretório LDAP.

Se usar o ldp.exe para conectar a um servidor LDAP habilitado por SSL, deve primeiro habilitar o certificado SSL em seu servidor DocuShare. Para importar e carregar um certificado SSL, siga as instruções **LDAP e SSL** no *Capítulo 2* deste guia.

Para instalar e usar a Ferramenta de Administração do Active Directory para ajudar a configurar seu site DocuShare:

1. Abra a mídia de software do servidor Windows 2000, localize e leia o arquivo **sreadme.doc**.
2. Localize o **setup.exe** do arquivo no Assistência\diretório Ferramentas.
3. Clique no arquivo **setup.exe** para começar a instalação do arquivo ldp.exe.
4. Siga as instruções na tela para instalar o **ldp.exe**.
5. Após a instalação ser concluída, abra o menu Iniciar do Windows e clique na **Ferramenta de Administração do Active Directory**.

   Isso inicia o ldp.exe, e a Ferramenta de Administração do Active Directory é exibida. A ferramenta tem uma barra de navegação com comandos e um quadro à esquerda e à direita em que exibe informações.



Usar a ferramenta de administração do Active Directory

Você pode usar a Ferramenta de Administração do Active Directory para coletar informações sobre o servidor LDAP que precisa configurar o site DocuShare e usar o servidor para domínios externos. Siga os procedimentos de A a F.

Nota: Esse procedimento se baseia no uso da ferramenta para coletar informações de uma configuração de servidor LDAP típica. Pode haver variações, dependendo de como o servidor estiver configurado.

A — Conectar

1. Selecione **Conexão** da barra de navegação Ferramenta de Administração do Active Directory. Depois selecione **Conectar** do menu Conexão.

   A caixa de diálogo Conexão é exibida.

2. Insira no campo **Servidor** o endereço IP ou o nome DNS do servidor do Active Directory LDAP.

3. Insira o número da porta a ser usado no campo **Porta**, se um diferente do padrão for exibido.

4. Clique em **OK**.

   Agora, seu endereço do servidor LDAP e o número da porta foram definidos.

B — Associar

Após configurar a conexão do servidor LDAP, você precisa associar o servidor a uma conta de administrador que tenha permissão para pesquisar o diretório.

1. Selecione **Conexão** da barra de navegação Ferramenta de Administração do Active Directory. Depois selecione **Associar** do menu Conexão.

   A caixa de diálogo Associar é exibida.

2. Insira o nome da conta de usuário no campo **Usuário**, a senha no campo **Senha** e o domínio no campo **Domínio**.

3. Clique em **OK**.

   Se tiver se conectado com sucesso e criado uma associação com um servidor LDAP, o servidor exibe um **texto de resposta no quadro direito** da Ferramenta de Administração do Active Directory.

C — Localizar o Nome Diferenciado base

O DN base será o ponto inicial de nossa avaliação da árvore do diretório.

1. Busque o texto de resposta no quadro direito da Ferramenta do Active Directory para uma referência ao **contexto de nomenclatura**.

   O formato do contexto de nomenclatura variará de acordo com o servidor LDAP que está usando.

2. O texto em destaque é o Nome Diferenciado base para o DIT.

   Por exemplo, o DN base em destaque pode ser **dc=adoc,dc=Xerox,dc=com**. Seu DN Base verdadeiro pode variar de acordo com a estrutura exclusiva de sua árvore do diretório LDAP. Anote essas informações para usar mais tarde.

D — Exibir a Árvore de Informações do Diretório

1. Selecione **Exibir** na barra de navegação Ferramenta de Administração do Active Directory. Depois selecione **Árvore** no menu Exibir.

   A caixa de diálogo Exibição em árvore aparece.

2. No campo **DNBase**, insira o **Nome Diferenciado base** que encontrou na busca por contexto de nomenclatura acima.

3. Clique em **OK**.

   O DIT para seu servidor LDAP é exibido no quadro esquerdo da janela Ferramenta de Administração do Active Directory.

4. Examine a Árvore para determinar onde sua raiz DIT ficará para qualquer dos domínios externos DocuShare que queira criar.

   A raiz deve ser alta o suficiente na hierarquia de modo que inclua todas as ramificações (tais como unidade de organização e componentes de domínio) que terão acesso ao servidor DocuShare.

   Como exemplo, usaremos dc=adoc, dc=xerox,dc=com como nossa raiz DIT porque queremos incluir apenas os usuários no domínio ADOC e não todos da Xerox.com.

E — Encontrar a Conta do Agente

Na maioria dos casos Active Directory não aceita consultas anônimas no diretório. Isso requer o uso de uma conta de Serviço ou Agente. Use o comando Pesquisar para encontrar o DN da conta do Agente.

1. Selecione **Navegar** da barra de navegação Ferramenta de Administração do Active Directory. Depois selecione **Pesquisar** do menu Navegar.

   A caixa de diálogo Pesquisa é exibida.

2. Insira o DN Base no campo **DN Base**.

   Dependendo do valor DN Base usado e da localização na hierarquia da conta do Agente, você pode precisa selecionar **Subárvore** para expandir o escopo da busca.

3. Insira um filtro no campo **Filtro**.

   Usamos o atributo sAMAccoutName para nosso filtro se soubermos o nome de logon da conta do Agente. Esse atributo é exclusivo do Active Directory e é uma transição do Windows NT. Se soubéssemos o nome comum (cn) da conta, poderíamos ter usado o nome comum=Peter Pan, por exemplo. Um servidor iPlanet pode usar o atributo uid ou nome comum (cn).

4. Especifique o **Escopo** da pesquisa.

   Selecionar **Subárvore** como **Nível Um** não é suficiente.

5. Clique em **Executar**.

   Os resultados de sua busca aparecem como texto no quadro direito da janela Ferramenta de Administração do Active Directory. Por exemplo, uma busca pode mostrar que o **nome diferenciado** para a conta do Agente é cn=usuárioteste1,cn=usuários,dc=adoc,dc=xerox,dc=com.

F — Próxima etapa

Após realizar os procedimentos de A a E, você deverá poder usar a Ferramenta de Administração do Active Directory para coletar informações necessárias para configurar o site DocuShare para usar o LDAP para autenticação da conta do usuário.

- O endereço IP ou nome DNS do servidor LDAP
- A Raiz DIT
- A conta do Agente para DocuShare

O comando Active Directory LDIFDE

Se estiver executando seu servidor LDAP em Windows 2000 ou Windows 2003, pode usar o comando **LDIFDE** para escrever os conteúdos do diretório LDAP inteiro em um arquivo de texto ou em um domínio específico no diretório LDAP. Este arquivo de texto contém a maior parte das informações necessárias para configurar o DocuShare para usar com LDAP.

O arquivo de texto gerado pelo LDIFDE é um arquivo primário usado pelo Suporte do DocuShare para resolver problemas de configuração LDAP.

Recursos: Para mais informações sobre a utilização do comando LDIFDE, vá para **http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q237/6/77.ASP&NoWebContent=1**

Utilização e Sintaxe do comando LDIFDE

Para usar o comando LDIFDE, abra a janela de prompt de comando em seu servidor LDAP e insira **C:\Windows\system32>idifde -?** e pressione **Enter**. LDIFDE responde o seguinte:

```
Troca de Diretório LDIF

Parâmetros Gerais
==================
-i                    Ligue o Modo Importar (o padrão é Exportar)
-f nome do arquivo    nome do arquivo de entrada ou saída
-s nome do servidor   O servidor a ser associado a (padrão para DC do Domínio conectado)
-c deDN paraDN        Substituir ocorrências de DeDN a ParaDN
-v                    Ligue o Modo Detalhado
-j                    Registrar Localização de Arquivo
-t                    Número de Porta (padrão = 389)
-u                    Usar formato Unicode
-?                    Ajuda

Exportar específico
===============
-d RaizDN             A raiz da pesquisa LDAP (padrão para contexto de nomenclatura)
-r Filtro             filtro de pesquisa LDAP (padrão para "(objectClass=*)")
-p EscopoPesquisa     Escopo de Pesquisa (Base/NívelUm/Subárvore)
-l lista              Lista de atributos (separados por vírgula) para busca em uma pesquisa
LDAP
-o lista              Lista de atributos (separados por vírgula) para omitir da entrada.
-g                    Disativar Pesquisa paginada.
-m                    Ativar a lógica SAM durante exportação.
-n                    Não exportar os valores binários

Importar
======
-k                    A importação continuará ignorando os erros "Violação Restrita" e
                      "Objeto já existe"
-y                    A importação usará a confirmação lenta para oferecer melhor
desempenho.

Estabelecimento de Credenciais
========================
Note que se nenhuma credencial for especificada, o LDIFDE será associado ao usuário
atualmente conectado, usando o SSPI.

-a DNusuário [senha | *]          Autenticação Simples
-b Método de associação SSPI do Domínio NomeUsuário [Senha | *]
Exemplo: importação simples do domínio atual
   ldifde -i -f INPUT.LDF

Exemplo: exportação simples do domínio atual
   ldifde -f OUTPUT.LDF

Exemplo: exportação para um domínio específico com credenciais
   ldifde -m -f OUTPUT.LDF
        -b NOMEDOMÍNIO NOMEUSUÁRIO *
        -s NOMESERVIDOR
        -d "cn=usuários,DC=NOMEDOMÍNIO,DC=Microsoft,DC=Com"
        -r "(objectClass=usuário)"
```

Exemplo de comando LDIFDE

A seguir, você encontra um exemplo de comando LDIFDE que grava o conteúdo do Active Directory em um servidor chamado Corvette, em um arquivo de texto chamado **adexport.txt**.

Executar o comando LDIFDE:

Insira o comando **C:\Windows\system32\LDIFDE.exe -f adexport.txt -s corvette** e pressione **Enter**.

O comando é executado e mostra seu progresso:

```
Conectando ao "corvette"
Fazendo o logon como usuário atual, utilizando o SSPI
Exportando o diretório para arquivo adexport.txt
Pesquisando entradas...
Gravando entradas.....................................................
.....................................................
132 entradas exportadas

O comando foi concluído com sucesso

C:\Documentos e Configurações\Administrador>LDIFDE -f adexport.txt -s corvette
Conectando ao "corvette"
Fazendo o logon como usuário atual, utilizando o SSPI
Exportando o diretório para arquivo adexport.txt
Pesquisando entradas...
Gravando entradas.....................................................
.....................................................
132 entradas exportadas

O comando foi concluído com sucesso
```

O arquivo adexport.txt gerado

Abaixo encontra-se o conteúdo do arquivo adexport.txt que o comando FDIFDE gerou em nosso exemplo. Esse exemplo mostra uma porção do conteúdo do arquivo total. Preste bastante atenção aos itens **em negrito**, você precisa configurar o DocuShare com esses itens para usar o servidor LDAP específico.

dn: DC=infodev,DC=dsbu,DC=xerox,DC=com
tipo de alteração: adicionar
controlado por:CN=Configurações NTDS, CN=CORVETTE, CN=Servidores, CN=infodev-dsbu-site, CN=Sites,CN=Configuração, DC=infodev, DC=dsbu, DC=xerox, DC=com
Política de auditoria: AAE=
tempo de criação: 127199619543431088
dc: infodev
forçar log off: -9223372036854775808
Proprietário função fSMOR:CN=Configurações NTDS, CN=CORVETTE, CN=Servidores, CN=infodev-dsbu-site, CN=Sites,CN=Configuração, DC=infodev, DC=dsbu, DC=xerox, DC=com

-
-
-

[Exemplo de Registro de Diretório para um Único Usuário]
dn: CN=Duncan Donkey, OU=Digital, OU=Atores, DC=infodev, DC=dsbu, DC=xerox, DC=com
tipo de alteração: adicionar
expiração da conta: 9223372036854775807
Horário senha errada: 0
Contagem senha errada: 0
Página de código: 0
cn: Duncan Donkey
Código do país: 0
Nome exibido: Duncan Donkey
mail: ddonkey@infodev.xerox.com
nome: Duncan
Tipo instância: 4
Último logoff: 0
Último logon: 0
Contagem logon: 0
Nome diferenciado: CN=Duncan Donkey, OU=Digital, OU=Atores, DC=infodev, DC=dsbu, DC=xerox, DC=com
Categoria objeto:CN=Pessoa, CN=Programa, CN=Configuração, DC=infodev, DC=dsbu, DC=xerox,DC=com
Classe objeto: usuário
objectGUID:: xmi02W78lEmpYca7AtiupQ==
objectSid: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0bgQAAA==
ID Grupo primário: 513
Última configuração de senha: 127293917905389760
nome: Duncan Donkey
sAMAccountName: duncan
Tipo sAMAccount: 805306368
sn: Donkey
Controle de conta do usuário: 512
Nome principal do usuário: duncan@infodev.dsbu.xerox.com
uSNModificado: 7353
uSNCriado: 7349
quando alterado: 20040518220950.0Z
quando criado: 20040518220933.0Z

-
-
-

Arquivo de texto continuou...

[Exemplo de Registro de Diretório para um Grupo]
dn: CN=usuários lab,CN=Usuários,DC=infodev,DC=dsbu,DC=xerox,DC=com
tipo de alteração: adicionar
membro: CN=Greg Wong,CN=Usuários,DC=infodev,DC=dsbu,DC=xerox,DC=com
membro: CN=Janet Gilmore,CN=Usuários,DC=infodev,DC=dsbu,DC=xerox,DC=com
membro: CN=Jennings\,
Ferris,CN=Usuários,DC=infodev,DC=dsbu,DC=xerox,DC=com
membro: CN=Cua\, Kiam T,CN=Usuários,DC=infodev,DC=dsbu,DC=xerox,DC=com
info: Usuário de logon autorizado para o InfoDev Lab
cn: usuários lab
descrição: Usuários InfoDev Lab
Tipo grupo: -2147483644
Tipo instância: 4
Nome diferenciado:CN=usuários lab, CN=Usuários, DC=infodev, DC=dsbu, DC=xerox,
DC=com
Categoria objeto:CN=Grupo, CN=Programa, CN=Configuração, DC=infodev,
DC=dsbu, DC=xerox,DC=com
Classe objeto: grupo
objectGUID:: Cm9phZkOn0ig4iEWMRPWsg==
objectSid:: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0VgQAAA==
nome: usuários lab
sAMAccountName: usuários lab
sAMAccountType: 536870912
uSNAlterado: 3975
uSNCriado: 2540
quando alterado: 20040302161513.0Z
quando criado: 20040130190128.0Z

Analisar o conteúdo do arquivo adexport.txt

Nosso exemplo de arquivo adexport.txt usa o Nome Diferenciado (DN) para Duncan Donkey, um membro da equipe de Atores Digitais no departamento InfoDev da DSBU na Xerox Corporation.

Em nosso exemplo, o DN para Duncan Donkey foi definido como: **CN=Duncan Donkey, OU=Digital, OU=Atores, DC=infodev, DC=dsbu, DC=xerox, DC=com**

Ao examinar um Nome Diferenciado de usuários, você pode encontrar as informações necessárias para identificar:

a. A Raiz da Árvore (DIT) de Informações do Diretório
b. A Chave RDN do usuário
c. Os Localizadores de Serviço de Diretório e Autenticação Relativa
d. Atributos de Associação de Usuários
e. Atributos de Associação de Grupo

A — A Raiz da Árvore (DIT) de Informações do Diretório

Defina a raiz DIT no nível da árvore do diretório que incluirá todas as ramificações do diretório que contém usuários que precisam acessar o servidor DocuShare. Em nosso exemplo, apenas membros da organização DSBU na Xerox terão acesso a nosso exemplo do servidor DocuShare.

A organização DSBU inclui muitos departamentos e equipes em um único departamento. Esses departamentos e equipes são organizados em um Diretório LDAP pelos Componentes do Domínio (DC) e Unidades Organizacionais (OU). Para nosso exemplo, configuraremos um Domínio externo no DocuShare para autenticar usuários que são membros da Equipe de Atores Digitais no departamento InfoDev na DSBU na Xerox Corporation.

Em nosso exemplo, a Raiz DIT do DN para Duncan Donkey é mostrada em negrito: CN=Duncan Donkey, OU=Digital, OU=Atores, DC=infodev, **DC=dsbu, DC=xerox, DC=com**

Ao definir a raiz DIT neste nível da hierarquia, domínios externos podem ser criados para cada departamento/equipe na DSBU.

B — A Chave RDN do usuário

A Chave RDN do Usuário é um alias do atributo usado para identificar o Usuário.

Em nosso exemplo, a chave RDN do usuário do DN para Duncan Donkey é mostrada em negrito: **CN=Duncan Donkey**, OU=Digital, OU=Atores, DC=infodev, DC=dsbu, DC=xerox, DC=com

C — Os Localizadores de Serviço de Diretório e Autenticação Relativa

Os Localizadores de Serviço de Diretório e Autenticação Relativa são os ponteiros para a ramificação do diretório do domínio externo que contém um usuário específico, usuários ou um grupo.

Em nosso exemplo, o Localizador de Serviço de Diretório e Autenticação Relativa é exibido em negrito: CN=Duncan Donkey, **OU=Digital, OU=Atores, DC=infodev**, DC=dsbu, DC=xerox, DC=com.

D — Atributos de associação de usuário

O arquivo de texto gerado pelo comando FDIFDE contém o alias de atributos que são usados para identificar o sobrenome, nome do usuário e endereço de email de cada usuário listado. Você vai usar esses aliases de atributos para configurar as propriedades de Associar Usuário LDAP DocuShare. No arquivo de texto de comando FDIFDE, usuários com o diretório LDAP são identificados com a entrada **Classe objeto: usuário**.

Em nosso exemplo, você encontrará os **aliases de atributo LDAP** para as propriedades a seguir:

Sobrenome = **sn**

Nome de usuário = **sAMAccountName**

Endereço de email = **mail**

Em nosso exemplo, os valores dados a esses aliases do atributo LDAP são:

sn: Donkey

sAMAccountName: duncan

mail: ddonkey@infodev.xerox.com

E — Atributos de associação de grupo

O arquivo de texto gerado pelo comando FDIFDE contém o alias de atributos que são usados para identificar o título, a descrição e as informações de resumo de cada grupo listado. Você vai usar esses aliases de atributos para configurar as propriedades de Associar Grupo LDAP DocuShare.

No arquivo de texto de comando FDIFDE, grupos com o diretório LDAP são identificados com a entrada **Classe objeto: grupo**.

Em nosso exemplo, você encontrará os **aliases de atributo LDAP** para as propriedades a seguir:

Título = **cn**

Descrição = **descrição**

Resumo = **info**

Em nosso exemplo, os valores dados a esses aliases do atributo LDAP são:

cn: usuários lab

descrição: Usuários InfoDev Lab

info: Usuário de logon autorizado para o InfoDev Lab