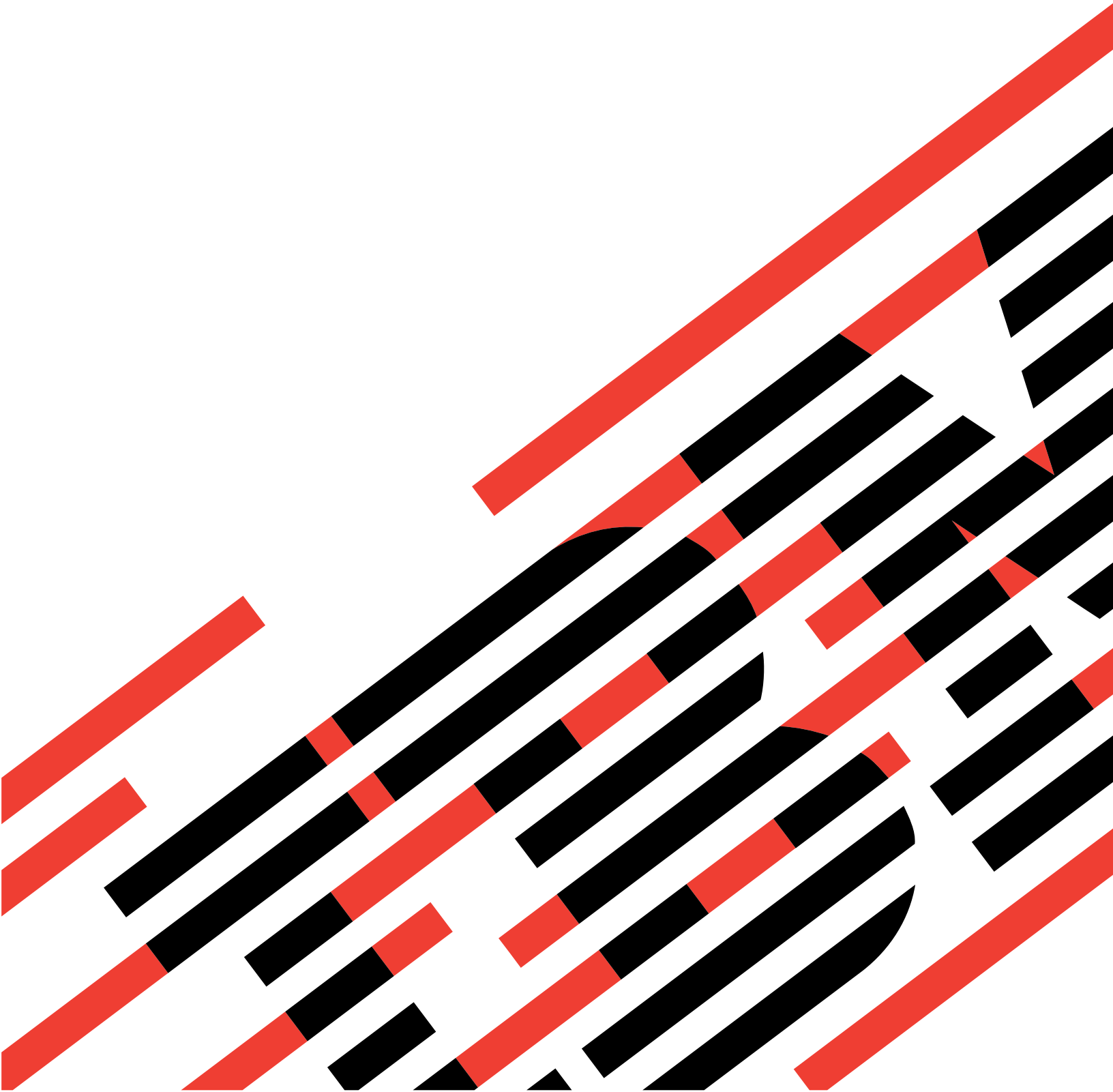
IBM

eserver

iSeries

IBM Directory Server (LDAP)

Versão 5, Edição 3



IBM

@server

iSeries

IBM Directory Server (LDAP)

Versão 5, Edição 3

Nota

Antes de utilizar as informações contidas neste manual, bem como o produto a que elas se referem, não deixe de ler as “Informações especiais”, na página 243.

Sétima edição (Agosto de 2005)

Esta edição aplica-se à versão 5, edição 3, modificação 0 do IBM Operating System/400 (número de produto 5722–SS1) e a todas as edições e modificações seguintes, salvo indicação em contrário nas novas edições. Não é possível executar esta versão em todos os modelos de computador de conjunto de instruções reduzido (RISC - Reduced Instruction Set Computer), nem em todos os modelos de computador de conjunto de instruções complexo (CISC - Complex Instruction Set Computer).

Índice

Capítulo 1. IBM Directory Server for iSeries (LDAP)

O IBM® Directory Server for iSeries™ (a partir daqui referido como Directory Server) fornece um servidor de Lightweight Directory Access Protocol (LDAP) para o servidor iSeries. O LDAP é executado no Transmission Control Protocol/Internet Protocol (TCP/IP) e está a ganhar popularidade como um serviço de directório para aplicações de Internet e sem ser de Internet.

Os tópicos que se seguem fornecem informações que o ajudam a compreender e a utilizar o Directory Server no seu servidor iSeries:

Capítulo 2. O que há de novo na V5R3

O Directory Server para iSeries (anteriormente conhecido como IBM Directory Server para iSeries) apresenta os seguintes melhoramentos e novas funções na V5R3:

- **Administração e acessibilidade dos utilizadores:** A nova Ferramenta de Administração da Web do IBM Directory Server substitui a IBM Directory Management Tool. A ferramenta de administração da Web inclui a funcionalidade para administrar as entradas de utilizador, os processos do Directory Server e a árvore de directórios, a partir de uma interface comum da Web. O protocolo LDAP é agora utilizado para consultar e actualizar as opções de configuração do Directory Server.
- **Grupos Dinâmicos:** A função Grupos Dinâmicos permitem a criação de um grupo cujos membros são entradas correspondentes a um filtro de procura.
- **Grupos Imbricados:** A função Grupos Imbricados permitem a criação de um grupo cujos membros incluem todos os membros de outros grupos.
- **Política de palavras-passe:** Agora, o Directory Server suporta uma política de palavras-passe que inclui regras de sintaxe de palavras-passe, histórico de palavras-passe e a desactivação de entradas após demasiadas tentativas de utilização de palavras-passe incorrectas.
- **Controlos de acesso baseados em filtros:** A autoridade para entradas já pode ser especificada com a utilização do controlo de acesso baseado em filtros. Por exemplo, é possível especificar permissões para entradas com departmentNumber=abc ou conceder acesso a tipos específicos de entradas.
- **Replicação:** Os melhoramentos à função de replicação a possibilidade de ter vários servidores principais (servidores de unidades), replicação de sub-árvores, programação e controlo de replicação, supervisão melhorada e funções de replicação mais robustas.
- **Procura Ordenada:** O controlo de procura ordenada permite que um cliente receba resultados de procura ordenados com base numa lista de critérios em que cada critério representa uma chave de ordenação. Esta faculdade passa a responsabilidade da ordenação da aplicação do cliente para o servidor, onde poderá ser executada mais eficientemente. O comando ldapsearch foi melhorado com novos parâmetros para permitir que os resultados da procura sejam ordenados. Também existem novas APIs de LDAP para ordenar resultados de procura.
- **Procura por Página:** O controlo de resultados por página permite gerir a quantidade de dados devolvidos por um pedido de procura. É possível pedir um subconjunto de entradas (uma página) em vez de receber todos os resultados de uma só vez. Os pedidos de procura subsequentes apresentam a página seguinte de resultados, até a operação ser cancelada ou após ser devolvido o último resultado. O comando ldapsearch foi melhorado com novos parâmetros para permitir que os resultados da procura sejam apresentados por página. Também existem novas APIs de LDAP para paginar resultados de procura.
- **Utilitários da linha de comandos:** São novos os seguintes utilitários de linha de comandos:
  - ldapexop - fornece a capacidade de ligação a um directório e emite uma única operação expandida juntamente com quaisquer dados que formem o valor da operação expandida.
  - ldapdiff - sincroniza um servidor de réplica com o respectivo servidor principal.
  - ldapchangepwd - envia pedidos de modificação de palavra-passe para um servidor de LDAP.
- **Rendimento:** O rendimento foi melhorado em todas as operações. Além disso, todas as operações já podem ser executadas simultaneamente por vários clientes.
- **Caracteres Especiais em Nomes Exclusivos (DN):** Agora, um DN já pode conter os seguintes caracteres especiais: vírgula, sinal de igual, sinal de mais, menor que, maior que, libra, ponto e vírgula, barra invertida e aspas.
- **Regras de Correspondência para Atributos de Cadeias:** Se um atributo for definido com uma das duas sintaxes de cadeia, Cadeia de Directórios ou Cadeia IA5, o servidor passa a respeitar a correspondência especificada no esquema para o atributo, o que vem corrigir um erro das edições anteriores. Pode definir um atributo como sensível a maiúsculas e minúsculas, ou não, quando

estabelecer uma correspondência. Anteriormente, o servidor permitia que fosse definida uma regra de correspondência, mas ignorava-a. Internamente, o servidor tratava a Cadeia IA5 como sensível a maiúsculas e minúsculas e a Cadeia de Directórios como não sensível a maiúsculas e minúsculas. Se o seu servidor tiver atributos definidos como uma Cadeia IA5 com caseIgnoreMatch, ou Cadeia de Directórios com caseExactMatch, o servidor passa a ter um comportamento correcto para esses atributos.

Capítulo 3. PDF imprimível

Para visualizar ou descarregar a versão em PDF deste documento, seleccione Directory Server (LDAP) (cerca de 2 700 KB).

Outras informações

Para ver ou imprimir PDFs de manuais e Redbooks™ relacionados, consulte Capítulo 10, “Informações relacionadas”, na página 241.

Guardar ficheiros PDF

Para guardar um ficheiro PDF na estação de trabalho para visualização ou impressão:

1. No browser, faça clique com o botão direito do rato no ficheiro PDF (faça clique com o botão direito do rato na ligação acima).
2. Faça clique na opção que permite guardar o PDF localmente.
3. Navegue até ao directório no qual pretende guardar o ficheiro PDF.
4. Faça clique em **Save** (Guardar).

Descarregar o Adobe Reader

É necessário ter o Adobe Reader instalado no sistema para visualizar ou imprimir estes PDFs. Pode descarregar uma cópia gratuita a partir do sítio da Web da Adobe (www.adobe.com/products/acrobat/readstep.html). 

Capítulo 4. Conceitos do Directory Server

O Directory Server implementa as especificações de LDAP V3 da Internet Engineering Task Force (IETF). Também inclui melhoramentos adicionados pela IBM em áreas funcionais e de rendimento. Esta versão utiliza a IBM DB2® como armazenamento para fornecer a integridade das transacções por operação de LDAP, operações de alto rendimento e capacidade de cópia de segurança e restauros online. Funciona de forma interoperacional com clientes baseados no LDAP V3 de IETF. Para ver conceitos e considerações relacionados com o Directory Server, consulte:

Directórios

O Directory Server permite o acesso a um tipo de base de dados que armazena informações numa estrutura hierárquica semelhante à forma como o sistema de ficheiros integrado do i5/OS™ está organizado.

Se o nome de um objecto for conhecido, podem ser obtidas as respectivas características. Se o nome de um objecto individual específico não for conhecido, é possível procurar no directório uma lista de objectos que correspondam a um determinado requisito. Normalmente, é possível procurar critérios específicos em directórios, não apenas um conjunto predefinido de categorias.

Um directório é uma base de dados especializada com características que a distinguem das bases de dados relacionais para fins gerais. Uma das características de um directório é ser acedido (lido ou pesquisado) com muito mais frequência do que é actualizado (escrito). Como os directórios têm de conseguir suportar grandes volumes de pedidos de leitura são, normalmente, optimizados para acesso de leitura. Uma vez que os directórios não se destinam a fornecer tantas funções como as bases de dados para fins gerais, podem ser optimizados de forma a fornecerem, de modo económico, a mais aplicações, um acesso rápido aos dados de directórios em ambientes distribuídos de grandes dimensões.

Um directório pode ser centralizado ou distribuído. Se um directório for distribuído, existe um Directory Server (ou um conjunto de unidades do servidor) numa localização que fornece acesso ao directório. Se o directório for distribuído, existem, normalmente, vários servidores geograficamente dispersos, que fornecem acesso ao directório.

Quando um directório é distribuído, as informações nele armazenadas podem ser divididas por partições ou replicadas. Quando as informações são divididas por partições, cada Directory Server armazena um subconjunto exclusivo e não sobreposto das informações. Ou seja, cada entrada de directório é armazenada por apenas um servidor. A técnica para criar partições no directório é utilizar referências de LDAP. As referências de LDAP permitem que os utilizadores refiram pedidos de Lightweight Directory Access Protocol (LDAP) para o mesmo espaço de nome, ou para um diferente, armazenado no mesmo servidor (ou num servidor diferente). Quando as informações são replicadas, a mesma entrada de directório é armazenada por vários servidores. Num directório distribuído, certas informações podem ser divididas por partições e outras podem ser replicadas.

O modelo do Directory Server de LDAP baseia-se em entradas (que também são referidas como objectos). Cada entrada consiste num ou mais atributos, como o nome ou endereço e um tipo. Normalmente, os tipos consistem em cadeias de mnemónicas, como cn para nome comum ou mail para endereço de correio electrónico.

O directório exemplo na Figura 1 na página 9 mostra uma entrada para Tiago Jesus que inclui os atributos mail e telephoneNumber. Outros atributos possíveis incluem fax, title, sn (para apelido) e jpegPhoto.

Cada directório tem um esquema, que é um conjunto de regras que determina a estrutura e conteúdo do directório. Pode ver o esquema utilizando a ferramenta de administração da Web. Para obter mais informações sobre o esquema, consulte “Esquema” na página 16.

Cada directório tem um atributo especial chamado objectClass. Este atributo controla os atributos que são necessários e os atributos que são permitidos numa entrada. Por outras palavras, os valores do atributo objectClass determinam as regras do esquema a que a entrada tem de obedecer.

Para além dos atributos definidos pelo esquema, as entradas também têm um conjunto de atributos que são mantidos pelo servidor. Estes atributos, conhecidos como atributos operacionais, incluem detalhes como a data de criação da entrada e informações de controlo de acesso. Para obter mais informações sobre atributos operacionais, consulte “Atributos operacionais” na página 77.

Tradicionalmente, as entradas do directório de LDAP são dispostas numa estrutura hierárquica, que reflecte limites políticos, geográficos ou organizacionais (consulte Figura 1 na página 9). As entradas que representam países ou regiões aparecem no topo da hierarquia. As entradas que representam estados ou organizações nacionais ocupam o segundo nível da hierarquia. As entradas abaixo dessas podem representar pessoas, unidades organizacionais, impressoras, documentos ou outros itens.

O LDAP refere-se a entradas com Nomes exclusivos (DNs - Distinguished Names). Os Nomes exclusivos são compostos pelo nome da entrada e pelos nomes, por ordem ascendente, dos objectos que se encontram acima deles no directório. Por exemplo, o DN completo da entrada no canto inferior esquerdo da Figura 1 na página 9 é cn=Tiago Jesus, o=IBM, c=PO. Cada entrada tem, pelo menos, um atributo utilizado para atribuir um nome à entrada. Este atributo de nomenclatura chama-se o Nome exclusivo relativo (RDN - Relative Distinguished Name) da entrada. A entrada acima de um RDN™ específico é designada Nome exclusivo ascendente. No exemplo anterior, cn=Tiago Jesus dá o nome à entrada, pelo que é o RDN. o=IBM, c=PO é o DN ascendente de cn=Tiago Jesus. Para obter mais informações sobre DNs, consulte “Nomes exclusivos (DNs)” na página 11.

Para dar a um servidor de LDAP a possibilidade de gerir parte de um directório de LDAP, especifique os Nomes exclusivos ascendentes de nível superior na configuração do servidor. Estes nomes distintos chamam-se sufixos. O servidor pode aceder a todos os objectos do directório que estejam por baixo do sufixo especificado na hierarquia de directórios. Por exemplo, se um servidor de LDAP contivesse o directório mostrado na Figura 1 na página 9, teria de ter o sufixo o=ibm, c=po especificado na respectiva configuração para conseguir responder a consultas de clientes relacionadas com Tiago Jesus.

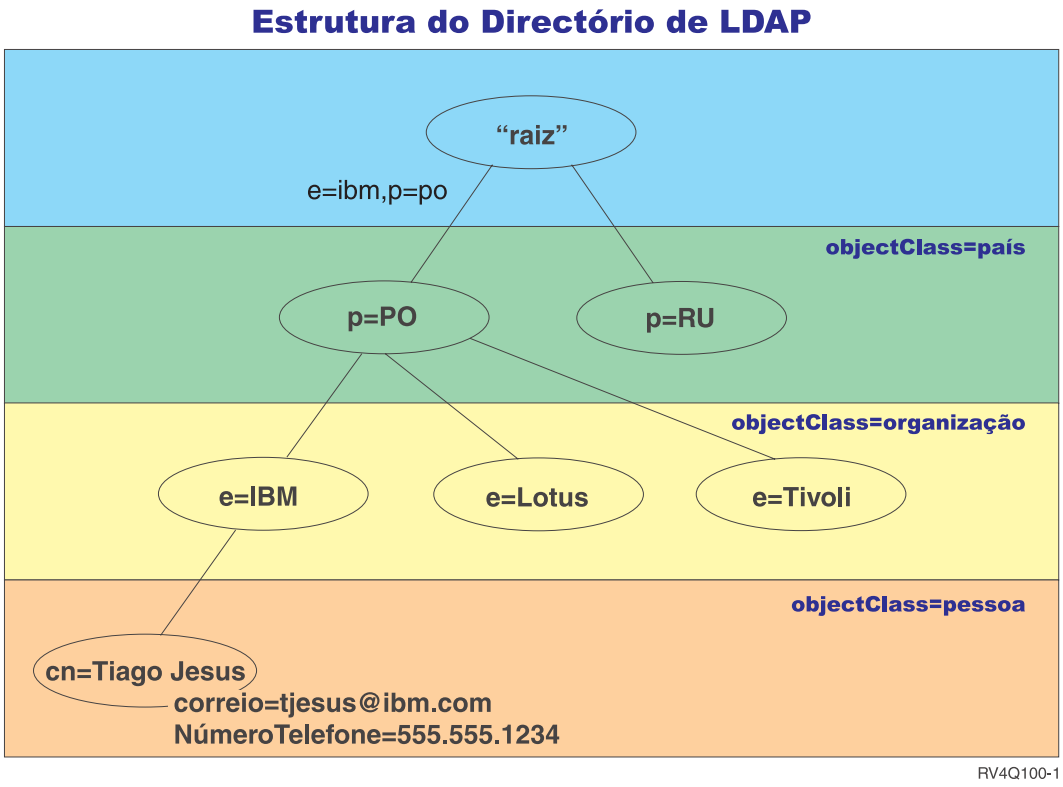


Figura 1. Estrutura do directório de LDAP

O utilizador não está limitado à hierarquia tradicional quando estruturar o seu directório. A estrutura do componente de domínio, por exemplo, é cada vez mais popular. Com esta estrutura, as entradas são compostas por partes de nomes de domínio de TCP/IP. Por exemplo, dc=ibm,dc=com pode ser preferível a o=ibm,c=po.

Suponha que pretende criar um directório utilizando a estrutura de componentes de domínio que irá conter dados sobre empregados, como nomes, números de telefone e endereços de correio electrónico. Utilizará o contexto de sufixo ou nomenclatura baseado no domínio de TCP/IP. Este directório poderia ser visualizado de uma forma semelhante a:

```
/
|
+- ibm.com
   |
   +- empregados
      |
      +- Tiago Jesus
      |  555-555-1234
      |  tjesus@ibm.com
      |
      +- João Silva
         555-555-1235
         jsilva@ibm.com
```

Quando introduzidos no Directory Server, estes dados podem, na realidade, ficar semelhantes a:

```
# suffix ibm.com
dn: dc=ibm,dc=com
objectclass: superior
objectclass: domain
dc: ibm
```

```
# directório de empregados
dn: cn=empregados,dc=ibm,dc=com
objectclass: superior
objectclass: container
cn: empregados

# empregado Tiago Jesus
dn: cn=Tiago Jesus,cn=empregados,dc=ibm,dc=com
objectclass: superior
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: Tiago Jesus
cn: "Jesus, Tiago"
sn: Jesus
givenname: Tiago
telephonenumber: 555-555-1234mail: tjesus@ibm.com

# empregado João Silva
dn: cn=João Silva,cn=empregados,dc=ibm,dc=com
objectclass: superior
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: publisher
objectclass: ePerson
cn: João Silva
cn: "Silva, João"
sn: Silva
givenname: João
telephonenumber: 555-555-1235
mail: jsilva@ibm.com
```

Como poderá notar, cada entrada contém valores de atributo chamados objectclass. Os valores de objectclass definem os atributos permitidos na entrada, como telephonenumber ou givenname. As classes de objecto permitidas são definidas no esquema. O esquema é um conjunto de regras que define o tipo de entradas permitidas na base de dados.

Clientes e servidores de directórios

Normalmente, os directórios são acedidos com a utilização do modelo de comunicação cliente-servidor. Os processos do cliente e do servidor podem encontrar-se ou não na mesma máquina. Um servidor consegue servir vários clientes. Uma aplicação que pretenda ler ou escrever informações num directório não acede directamente ao directório. Em vez disso, chama uma função ou interface de programação de aplicações (API) que envia uma mensagem para outro processo. Este segundo processo acede às informações existentes no directório em substituição da aplicação solicitadora. Os resultados da leitura ou escrita são, em seguida, devolvidos à aplicação solicitadora.

Uma API define a interface de programação utilizada por uma linguagem de programação específica para aceder a um serviço. O formato e o conteúdo das mensagens trocadas entre o cliente e o servidor têm de aderir a um protocolo acordado entre ambos. O LDAP define um protocolo de mensagens utilizado por clientes e servidores de directórios. Também existe uma API de LDAP associada para a linguagem C e métodos de acesso ao directório a partir de uma aplicação de Java utilizando a Interface de Nomenclatura e Directórios de Java (JNDI - Java Naming and Directory Interface).

Segurança de directório

Um directório deverá suportar as capacidades base necessárias à implementação de uma política de segurança. O directório pode não fornecer directamente as capacidades de segurança subjacentes, mas pode ser integrado num serviço de segurança de rede fidedigno que forneça os serviços de segurança

base. Primeiro, é necessário um método para autenticar utilizadores. A autenticação verifica a identidade dos utilizadores. Um nome de utilizador e palavra-passe é um esquema de autenticação base. Assim que os utilizadores sejam autenticados, é necessário determinar se têm a autorização ou permissão para executar a operação pedida no objecto específico.

A autorização baseia-se frequentemente em listas de controlo de acesso (ACLs). Uma ACL é uma lista de autorizações que podem ser associadas a objectos e atributos existentes no directório. Uma ACL indica o tipo de acesso para o qual cada utilizador ou grupo de utilizadores tem ou não autorização. Para tornar as ACLs mais curtas e facilitar a respectiva gestão, os utilizadores com os mesmos direitos de acesso são frequentemente colocados em grupos.

Nomes exclusivos (DNs)

Cada entrada do directório tem um nome exclusivo (DN - distinguished name). O DN é o nome que identifica, de modo exclusivo, uma entrada do directório. Um DN é composto por pares atributo=valor, separados por vírgulas como, por exemplo:

```
cn=Rui Graça,ou=edição,o=Correio da Manhã,c=PO
cn=Lúcia Branco,ou=edição,o=Correio da Manhã,c=PO
cn=Tomás Bento,ou=jornalista,o=Correio da Manhã,c=PO
```

Qualquer um dos atributos definidos no esquema do directório pode ser utilizado para constituir um DN. A ordem dos pares atributo-valor do componente é importante. O DN contém um componente para cada nível da hierarquia de directórios desde a raiz até ao nível onde a entrada reside. Os DNs de LDAP começam pelo atributo mais específico (normalmente, um nome) e continuam com atributos progressivamente mais alargados, muitas vezes terminando por um atributo de país. O primeiro componente do DN é referido como um Nome exclusivo relativo (RDN - Relative Distinguished Name). Este identifica de forma distinta uma entrada de quaisquer outras entradas que tenham o mesmo ascendente. Nos exemplos anteriores, o RDN ″cn=Rui Graça″ separa a primeira da segunda entrada (com o RDN ″cn=Lúcia Branco″). Estes dois DNs exemplo são equivalentes em tudo o resto. O par atributo=valor que constitui o RDN para uma entrada também tem de estar presente na entrada. (Esta condição não é verdadeira para os outros componentes do DN.)

Siga este exemplo para criar uma entrada para uma pessoa:

```
dn: cn=Tiago Jesus,o=ibm,c=po
objectclass: superior
objectclass: person
cn: Tiago Jesus
sn: Jesus
telephonenumber: 555-555-1234
```

Regras de indicação de mudança de código de DNs

Certos caracteres têm um significado especial num DN. Por exemplo, = (sinal de igual) separa o nome e o valor do atributo e , (vírgula) separa pares atributo=valor. Os caracteres especiais são **,** (vírgula), **=** (igual a), **+** (sinal de mais), **<** (menor que), **>** (maior que), **#** (cardinal), **;** (ponto e vírgula), **** (barra invertida) e **"** (aspas, ASCII 34).

Um carácter especial pode indicar uma mudança de código num valor de atributo por forma a retirar o significado especial. Para indicar uma mudança de código destes caracteres especiais ou de outros caracteres num valor de atributo numa cadeia de DN, utilize os seguintes métodos:

1. Se o carácter a indicar uma mudança de código for um dos caracteres especiais, deverá ser precedido de uma barra invertida ('\' ASCII 92). Este exemplo mostra um método de indicação de mudança de código de uma vírgula no nome de uma empresa:

   ```
   CN=L. Águia,O=Sue\, Importação e Exportação,C=GB
   ```

   Este é o método preferencial.

2. Caso contrário, substitua o carácter indicador de uma mudança de código por uma barra invertida e dois dígitos hexadecimais, que formam um único byte no código do carácter. O código do carácter **tem de** pertencer ao conjunto de códigos UTF-8.

   ```
   CN=L. Águia,O=Sue\2C Importação e Exportação,C=GB
   ```

3. Rodeie todo o valor do atributo de **""** (aspas) (ASCII 34), que não fazem parte do valor. Entre o par de aspas, todos os caracteres são aceites como estão, excepto a \ (barra invertida). A \ (barra invertida) pode ser utilizada para indicar uma mudança de código de uma barra invertida (ASCII 92) ou aspas (ASCII 34), qualquer um dos caracteres anteriormente mencionados ou pares de caracteres hexadecimais como, por exemplo, no método 2. Por exemplo, para indicar uma mudança de código das aspas em `cn=xyz"qrs"abc`, esta cadeia tornar-se-á `cn=xyz\"qrs\"abc`, ou para indicar uma mudança de código de uma \:

   ```
   "é necessário indicar uma mudança de código de uma única barra invertida desta forma \\"
   ```

   Outro exemplo, `"\Zoo"` não é permitido, porque 'Z' não pode indicar uma mudança de código neste contexto.

Pseudo-DNs

Os pseudo-DNs são utilizados na definição e avaliação do controlo de acesso. O directório de LDAP suporta vários pseudo-DNs (por exemplo, ″grupo:CN=ESTE″ e ″ID-acesso:CN=TODOS″), que são utilizados para referir um elevado número de DNs que partilham uma característica comum, em relação à operação que está a ser executada ou ao objecto em que a operação está a ser executada. Para obter mais informações sobre o controlo de acesso, consulte "Segurança do Directory Server" na página 43.

São suportados três pseudo-DNs pelo Directory Server:

- id-acesso: CN=ESTE

  Quando especificado como parte de uma ACL, este DN refere-se a bindDN, que corresponde ao DN em que a operação está a ser executada. Por exemplo, se for executada uma operação no objecto ″cn=pessoaA, ou=IBM, c=PO″ e bindDn for ″cn=pessoaA, ou=IBM, c=PO″, as permissões concedidas são uma combinação das fornecidas a ″CN=ESTE″ e a ″cn=pessoaA, ou=IBM, c=PO″.

- grupo: CN=TODOS

  Quando especificado como parte de uma ACL, este DN refere-se a todos os utilizadores, mesmo aqueles que não se tenham autenticado. Os utilizadores não podem ser removidos deste grupo e este grupo não pode ser removido da base de dados.

- grupo: CN=AUTENTICADO

  Este DN refere qualquer DN que tenha sido autenticado pelo directório. O método de autenticação não é tomado em consideração.

  Nota: ″CN=AUTENTICADO″ refere um DN que foi autenticado em qualquer parte do servidor, independentemente da localização do objecto que representa o DN. No entanto, deve ser utilizado com precaução. Por exemplo, sob um sufixo, ″cn=Secreto″ pode estar um nó chamado ″cn=Material Confidencial″, que tem uma entrada de ACL″grupo:CN=AUTENTICADO:normal:rsc″. Sob outro sufixo, ″cn=Comum″ pode estar o nó ″cn=Material Público″. Se estas duas árvores residirem no mesmo servidor, uma ligação a″cn=Material Público″ seria considerada como autenticada e obteria permissão para a classe normal do objecto ″cn= Material Confidencial″.

Alguns exemplos de pseudo-DNs:

Exemplo 1

Considere a seguinte ACL para o objecto: cn=pessoaA, c=PO

```
AclEntry: id-acesso: CN=ESTE:crítico:rwsc
AclEntry: grupo: CN=TODOS: normal:rsc
AclEntry: grupo: CN=AUTENTICADO: sensível:rcs
```

Ligação de Utilizador como	Receberia
cn=pessoaA, c=PO	normal:rsc:sensível:rcs:crítico:rwsc
cn=pessoaB, c=POS	normal:rsc:sensível:rsc
Anónimo	normal:rsc

Neste exemplo, pessoaA recebe permissões concedidas ao ID ″CN=ESTE″ e as permissões concedidas a ambos os grupos de pseudo-DNs ″CN=TODOS″ e ″CN=AUTENTICADO″.

Exemplo 2

Considere a seguinte ACL para o objecto: cn=pessoaA, c=PO AclEntry: id-acesso:cn=pessoaA, c=PO: objecto:ad

```
AclEntry: id-acesso: CN=ESTE:crítico:rwsc
AclEntry: grupo: CN=TODOS: normal:rsc
AclEntry: grupo: CN=AUTENTICADO: sensível:rcs
```

Para uma operação executada em cn=pessoaA, c=PO:

Ligação de Utilizador como	Receberia
cn=pessoaA, c=PO	objecto:ad:crítico:rwsc
cn=pessoaB, c=POS	normal:rsc:sensível:rsc
Anónimo	normal:rsc

Neste exemplo, pessoaA recebe permissões concedidas ao ID″CN=ESTE″ e as concedidas ao próprio DN ″cn=pessoaA, c=PO″. Note que as permissões de grupo não são concedidas porque existe uma entrada de acl mais específica (″id-acesso:cn=pessoaA, c=PO″) para o DN de ligação (″cn=pessoaA, c=PO″).

Processamento melhorado de DNs

Um RDN composto de um DN pode consistir de vários componentes ligados pelos operadores ‘+’. O servidor melhora o suporte para procuras nas entradas que tenham um DN desse tipo. Um RDN composto pode ser especificado em qualquer ordem como base para uma operação de procura.

```
ldapsearch -b "cn=miguel+ou=almada,o=ibm,c=po" "(objectclass=*)"
```

O servidor suporta uma operação expandida de normalização de DNs. As operações expandidas de normalização de DNs normalizam DNs utilizando o esquema do servidor. Esta operação expandida pode ser útil para as aplicações que utilizam DNs. Para obter mais informações sobre operações expandidas, consulte “Controlos e operações expandidas” na página 77.

Sintaxe de nomes distintos

A sintaxe formal para um Nome exclusivo (DN - Distinguished name) baseia-se no RFC 2253. A sintaxe Backus Naur Form (BNF) é definida do seguinte modo:

```
<nome> ::= <componente-nome> ( <separador-espaço> )
         | <componente-nome> <separador-espaço> <nome>

   <separador-espaço> ::= <espaço-opcional>
                          <separador>
                          <espaço-opcional>

   <separador> ::=  "," | ";"

   <espaço-opcional> ::= ( <CR> ) *( " " )

   <componente-nome> ::= <atributo>
           | <atributo> <espaço-opcional> "+"
             <espaço-opcional> <componente-nome>
```

```
<atributo> ::= <cadeia>
        | <chave> <espaço-opcional> "=" <espaço-opcional> <cadeia>

<chave> ::= 1*( <carchave> ) | "OID." <oid> | "oid." <oid>
<carchave> ::= letras, números e espaço

<oid> ::= <cadeiadígitos> | <cadeiadígitos> "." <oid>
<cadeiadígitos> ::= 1*<dígito>
<dígito> ::= dígitos 0-9

<cadeia> ::= *( <carcadeia> | <par> )
         | '"' *( <carcadeia> | <especial> | <par> ) '"'
         | "#" <hex>


<especial> ::= "," | "=" | <CR> | "+" | "<" |  ">"
         | "#" | ";"

<par> ::= "\" ( <especial> | "\" | '"')
<carcadeia> ::= qualquer carácter excepto <especial> ou "\" ou '"'


<hex> ::= 2*<carhex>
<carhex> ::= 0-9, a-f, A-F
```

Pode utilizar o carácter ponto e vírgula (;) para separar RDNs num nome exclusivo, embora o carácter vírgula seja a notação comum.

Podem estar presentes caracteres espaços em branco de qualquer lado de uma vírgula ou ponto e vírgula. Os caracteres espaços em branco são ignorados e o ponto e vírgula é substituído por uma vírgula.

Além disso, podem estar presentes caracteres espaço (' ' ASCII 32) antes ou depois de um sinal '+' ou '='. Estes caracteres espaços são ignorados durante a análise.

O exemplo que se segue representa um nome exclusivo escrito com a utilização de uma notação conveniente para formas de nomes comuns. Primeiro, é especificado um nome que contém três componentes. O primeiro componente é um RDN composto. Um RDN composto contém mais de um par atributo:valor e pode ser utilizado para identificar de forma distinta uma entrada específica nos casos em que um único valor de CN pode ser ambíguo:

```
OU=Vendas+CN=J. Silva,O=Geringonças, SA.,C=PO
```

Sufixo (contexto de nomenclatura)

Um sufixo (também conhecido como contexto de nomenclatura) é um DN que identifica a entrada superior numa hierarquia de directórios mantida localmente. Devido ao esquema de nomenclatura relativo utilizado no LDAP, este DN também é o sufixo de todas as outras entradas dessa hierarquia de directórios. Um Directory Server pode ter vários sufixos, cada qual identificando uma hierarquia de directórios localmente mantida como, por exemplo, o=ibm,c=po.

Tem de ser adicionada ao directório a entrada específica correspondente ao sufixo. A entrada criada pelo utilizador tem de utilizar um atributo objectclass que contenha o atributo de nomenclatura utilizado. Pode utilizar a ferramenta de administração da Web ou o utilitário Qshell ldapadd para criar a entrada correspondente a este sufixo. Para obter mais informações, consulte “Gerir entradas de directório” na página 145 ou “ldapmodify e ldapadd” na página 175.

Em termos conceituais, existe um espaço de nome de LDAP global. No espaço de nome de LDAP global, pode encontrar DNs como:

- cn=João Silva,ou=Coimbra,o=IBM

- cn=Joana Silva,o=Minha Empresa,c=PO
- cn=administradora de sistema,dc=minhaemp,dc=com

O sufixo "o=IBM" indica ao servidor que apenas o primeiro DN se encontra num espaço de nome que pertence ao servidor. Quaisquer tentativas para referir objectos que não se encontrem num dos sufixos resultam num erro de objecto inexistente ou numa referência a outro Directory Server.

Um servidor pode ter vários sufixos. O Directory Server tem vários sufixos predefinidos que contêm dados específicos da implementação:

- cn=esquema contém a representação acessível de LDAP do esquema
- cn=registoalterações contém o registo de alterações do servidor, se activado
- cn=sistcentrallocal contém informações não replicadas que controlam certos aspectos do funcionamento do servidor como, por exemplo, objectos de configuração de replicação
- cn=políticappasse contém a política de palavras-passe de todo o sistema
- o sufixo "os400-sys=nome-sistema.meudomínio.com" fornece um LDAP acessível a objectos do i5/OS, actualmente limitado a perfis e grupos de utilizadores.

O Directory Server vem pré-configurado com um sufixo assumido, dc=nome-sistema,dc=nome-domínio, para facilitar o início de trabalho com o servidor. Não é obrigatório utilizar esse sufixo. O utilizador pode adicionar sufixos próprios e eliminar o sufixo pré-configurado.

Existem duas convenções de nomenclatura normalmente utilizadas para sufixos. Uma delas baseia-se no domínio de TCP/IP da sua empresa. A outra, no nome e localização da empresa.

Por exemplo, no caso de um domínio de TCP/IP minhaempresa.com, o utilizador poderia escolher um sufixo como `dc=minhaempresa,dc=com`, em que o atributo `dc` se refere ao componente do domínio. Neste caso, a entrada de nível superior criada no directório pode ser semelhante a (utilizando LDIF, um formato de ficheiros de texto para representar entradas de LDAP):

```
dn: dc=minhaempresa,dc=com
objectclass: domain
dc: minhaempresa
```

A objectclass `domain` também tem certos atributos especiais que podem ser utilizados. Visualize o esquema ou edite a entrada criada com a utilização da ferramenta de administração da Web para ver os atributos adicionais que podem ser utilizados. Para obter mais informações, consulte “Gerir o esquema” na página 134.

Se o nome da empresa for `Minha Empresa` e se a mesma estiver localizada em Portugal, pode escolher um sufixo como um dos seguintes:

```
o=Minha Empresa
o=Minha Empresa,c=PO
ou=Geringonças, SA,o=Minha Empresa,c=PO
```

Neste exemplo, `ou` é o nome da objectclass organizationalUnit, `o` é o nome da objectclass organização e `c` é a abreviatura padrão de duas letras do país utilizada para designar a classe de objecto país. Neste caso, a entrada de nível superior que criar pode ser semelhante a:

```
dn: o=Minha Empresa,c=PO
objectclass: organização
o: Minha Empresa
```

As aplicações que utilizar podem requerer a definição de sufixos específicos ou a utilização de uma convenção de nomenclatura específica. Por exemplo, se o directório for utilizado para gerir certificados digitais, poderá ter de estruturar uma parte do mesmo, de modo a que os nomes de entradas correspondam a DNs de sujeitos dos certificados nele contidos.

As entradas a adicionar ao directório têm de ter um sufixo que corresponda ao valor do DN como, por exemplo `ou=Marketing,o=ibm,c=po`. Se uma consulta contiver um sufixo que não corresponda a nenhum sufixo configurado para a base de dados local, a consulta tem como referência o servidor de LDAP identificado pela referência assumida. Se não for especificado uma referência assumida de LDAP, será devolvido o resultado Objecto não existente.

Para obter informações adicionais sobre como adicionar ou remover um sufixo, consulte "Adicionar e remover sufixos do Directory Server" na página 110.

Esquema

Um esquema é um conjunto de regras que controla o modo como os dados podem ser armazenados no directório. O esquema define o tipo de entradas permitidas, a respectiva estrutura de atributos e a sintaxe dos atributos.

Os dados são armazenados no directório com a utilização de entradas de directório. Uma entrada consiste numa classe de objecto, que é obrigatória, e nos respectivos atributos. Os atributos podem ser obrigatórios ou opcionais. A classe de objecto especifica o tipo de informações que a entrada descreve e define o conjunto de atributos nela contido. Cada atributo tem um ou mais valores associados. Consulte "Gerir entradas de directório" na página 145 para obter informações adicionais sobre como gerir entradas.

Para obter mais informações relacionadas com o esquema, consulte:

Esquema do IBM Directory Server

O esquema do Directory Server é predefinido, embora seja possível modificá-lo, se tiver requisitos adicionais. Para obter mais informações sobre como modificar o esquema, consulte "Gerir o esquema" na página 134.

O Directory Server inclui suporte de esquemas dinâmicos. O esquema é publicado como parte das informações sobre directórios e está disponível na entrada Sub-esquema (DN="cn=esquema"). Pode consultar o esquema utilizando a APIldap_search() e modificá-lo utilizando ldap_modify(). Consulte o tópico "APIs do Directory Server" para obter mais informações sobre estas APIs.

O esquema tem mais informações de configuração do que as que estão incluídas nos Pedidos de Comentários (RFCs) de LDAP Versão 3 ou nas especificações padrão. Por exemplo, para um determinado atributo, pode indicar quais os índices remissivos a manter. Estas informações de configuração adicionais são mantidas na entrada de sub-esquema, como apropriado. É definida uma classe de objecto adicional para a entrada de sub-esquema IBMsubschema, que tem atributos "MAY" que contêm as informações expandidas sobre o esquema.

O Directory Server define um único esquema para todo o servidor, acessível através de uma entrada de directório especial, "cn=esquema". A entrada contém todo o esquema definido para o servidor. Para obter informações sobre o esquema, pode executar uma ldap_search utilizando:

```
 DN: "cn=esquema", âmbito de procura: base, filtro: objectclass=subschema
ou objectclass=*
```

O esquema fornece valores para os seguintes tipos de atributos:

- objectClasses (para obter mais informações sobre objectClasses, consulte "Classes de objecto" na página 18.)
- attributeTypes (para obter mais informações sobre attributeTypes, consulte "Atributos" na página 19.)
- IBMAttributeTypes (para obter mais informações sobre IBMAttributeTypes, consulte "O atributo IBMAttributeTypes" na página 23.)
- regras de correspondência (para obter mais informações sobre regras de correspondência, consulte "Regras de correspondência" na página 24).
- sintaxes de ldap (para obter mais informações sobre sintaxes de ldap, consulte "Sintaxe de atributos" na página 26).

A sintaxe destas definições de esquema baseia-se nos RFCs de LDAP Versão 3.

Uma entrada de esquema exemplo poderia conter:

```
objectclasses=( 1.3.6.1.4.1.1466.101.120.111
                NAME 'extensibleObject'
                SUP top AUXILIARY )

objectclasses=(  2.5.20.1
                 NAME 'subschema'
                 AUXILIARY MAY
                     ( dITStructureRules
                    $ nameForms
                    $ ditContentRules
                    $ objectClasses
                    $ attributeTypes
                    $ matchingRules
                    $ matchingRuleUse  ) )
objectclasses=( 2.5.6.1
                NAME 'alias'
                SUP top STRUCTURAL
                MUST aliasedObjectName )

attributeTypes=( 2.5.18.10
                 NAME 'subschemaSubentry'
                 EQUALITY distinguishedNameMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
                 NO-USER-MODIFICATION
                 SINGLE-VALUE USAGE directoryOperation )
attributeTypes=( 2.5.21.5 NAME 'attributeTypes'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.3
                 USAGE directoryOperation )
attributeTypes=( 2.5.21.6 NAME 'objectClasses'
                 EQUALITY objectIdentifierFirstComponentMatch
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.37
                 USAGE directoryOperation
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                 USAGE directoryOperation )

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binário' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Booleano' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Cadeia de Directórios' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Hora Generalizada' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'Cadeia IA5' )
```

```
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'NÚMERO INTEIRO' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Número de Telefone' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'Hora UTC' )

matchingRules=( 2.5.13.2 NAME 'caseIgnoreMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
matchingRules=( 2.5.13.0 NAME 'objectIdentifierMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.30 NAME 'objectIdentifierFirstComponentMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
matchingRules=( 2.5.13.4 NAME 'caseIgnoreSubstringsMatch'
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.58 )
```

As informações sobre o esquema podem ser modificadas através da API ldap_modify. Consulte o tópico "APIs do Directory Server" para obter informações adicionais. Com o DN "cn=esquema" pode adicionar, eliminar ou substituir um tipo de atributo ou uma classe de objecto. Consulte "Esquema dinâmico" na página 28 e "Gerir o esquema" na página 134, para obter mais informações. Também pode fornecer uma descrição total. Pode adicionar ou substituir uma entrada de esquema pela definição de LDAP Versão 3 ou pela definição de extensão de atributo da IBM ou ainda por ambas as definições.

Suporte de esquema comum

O IBM Directory suporta o esquema de directório padrão, tal como definido em:

- Os RFCs de LDAP Versão 3 de Internet Engineering Task Force (IETF) , como o RFC 2252 e 2256.
- A Directory Enabled Network (DEN)
- O Common Information Model (CIM) de Desktop Management Task Force (DMTF)
- O Lightweight Internet Person Schema (LIPS) do Network Application Consortium

Esta versão do LDAP inclui o esquema definido de LDAP Versão 3 na configuração de esquemas assumida. Também inclui as definições de esquema de DEN.

A IBM também fornece um conjunto de definições de esquema comum expandidas, partilhadas com outros produtos IBM quando exploram o directório de LDAP. Estas incluem:

- Objectos para aplicações de páginas brancas, como eperson, group, country, organization, organization unit and role, locality, state, etc.
- Objectos para outros subsistemas como accounts, services and access points, authorization, authentication, security policy, etc.

Classes de objecto

Uma classe de objecto especifica um conjunto de atributos utilizado para descrever um objecto. Por exemplo, se o utilizador criasse a classe de objecto **tempEmployee**, esta poderia conter atributos associados a um empregado temporário, como **idNumber**, **dateOfHire** ou **assignmentLength**. Pode adicionar classes de objecto personalizadas adequadas às necessidades da sua empresa. O esquema do IBM Directory Server fornece determinados tipos básicos de classes de objecto, incluindo:

- Groups
- Locations
- Organizations
- People

Nota: As classes de objecto específicas do Directory Server têm o prefixo 'ibm-'.

As classes de objecto são definidas pelas características de tipo, herança e atributos.

Tipo de classe de objecto

Uma classe de objecto pode ter um de três tipos:

Estrutural:
Todas as entradas têm de pertencer a uma única classe de objecto estrutural, que define o conteúdo base da entrada. Esta classe de objecto representa um objecto do mundo real. Uma vez que todas as entradas têm de pertencer a uma classe de objecto estrutural, este é o tipo mais comum de classe de objecto.

Abstracta:
Este tipo é utilizado como superclasse ou modelo para outras classes de objecto (estrutural). Define um conjunto de atributos comuns a um conjunto de classes de objecto estruturais. Estas classes de objecto, quando definidas como subclasses da classe abstracta, herdam os atributos definidos. Não é necessário definir atributos para cada uma das classes de objecto subordinadas.

Auxiliar:
Este tipo indica atributos adicionais que podem ser associados a uma entrada pertencente a uma classe de objecto estrutural específica. Embora uma entrada só possa pertencer a uma única classe de objecto estrutural, pode pertencer a várias classes de objecto auxiliares.

Herança de Classes de Objecto

Esta versão do Directory Server suporta a herança de objectos referente a definições de atributo e de classe de objectos. Pode ser definida uma nova classe de objecto com classes ascendentes (herança múltipla) e os atributos adicionais ou alterados.

Cada entrada está atribuída a uma única classe de objecto estrutural. Todas as classes de objecto herdam atributos da classe de objecto abstracta **superior**. Também podem herdar atributos de outras classes de objecto. A estrutura da classe de objecto determina a lista de atributos obrigatórios e permitidos para uma entrada específica. A herança da classe de objecto depende da sequência de definições da classe de objecto. Uma classe de objecto só pode herdar atributos das classes de objecto que a precedem. Por exemplo, a estrutura da classe de objecto para uma entrada person pode ser definida no ficheiro LDIF como:

```
objectClass: superior
objectClass: person
objectClass: organizationalPerson
```

Nesta estrutura, organizationalPerson herda atributos das classes de objecto person e superior, enquanto que a classe de objecto person apenas herda atributos da classe de objecto superior. Deste modo, quando atribui a classe de objecto organizationalPerson a uma entrada, ela herda automaticamente os atributos obrigatórios e permitidos da classe de objecto superior (neste caso, a classe de objecto person).

As operações de actualização de esquemas são comparadas com a hierarquia de classes de esquema, em termos de consistência, antes de serem processadas e consolidadas.

Atributos

Cada classe de objecto inclui um número de atributos obrigatórios e atributos opcionais. Os atributos obrigatórios são os atributos que têm de estar presentes nas entradas que utilizam a classe de objecto. Os atributos opcionais são os atributos que podem estar presentes nas entradas que utilizam a classe de objecto.

Atributos

Cada entrada de directório tem um conjunto de atributos associado através da respectiva classe de objecto. Embora a classe de objecto descreva o tipo de informações que uma entrada contém, os dados reais estão contidos nos atributos. Um atributo é representado por um ou mais pares nome-valor que

contêm um elemento de dados específico como um nome, um endereço ou um número de telefone. O Directory Server representa os dados como pares nome-valor, um atributo descritivo, como commonName (cn) e uma informação específica, como Joaquim Dias.

Por exemplo, a entrada para Joaquim Dias pode conter vários pares nome-valor de atributo.

```
dn: uid=jdias, ou=pessoas, ou=minhaempresa, c=po
objectClass: superior
objectClass: person
objectClass: organizationalPerson
      cn: Joaquim Dias
      sn: Dias
givenName: J.
givenName: João
```

Embora os atributos padrão já estejam definidos no esquema, pode criar, editar, copiar ou eliminar definições de atributo de acordo com as necessidades da sua empresa.

Os atributos podem ser definidos como tendo um único valor ou vários valores. Uma vez que os atributos com vários valores não são ordenados, uma aplicação não deve depender da devolução de um conjunto de valores de determinado atributo por uma ordem específica. Se necessitar de um conjunto de valores ordenado, opte por colocar a lista de valores num único valor de atributo:

```
preferences: 1ª-pref 2ª-pref 3ª-pref
```

Pode também considerar a inclusão de informações de ordenação no valor:

```
preferences: 2 yyy
preferences: 1 xxx
preferences: 3 zzz
```

Os atributos com vários valores são úteis quando uma entrada é conhecida por vários nomes. Por exemplo, cn (nome comum) tem vários valores. Uma entrada pode ser definida como:

```
dn: cn=João Silva,o=Minha Empresa,c=PO
objectclass: inetorgperson
sn: Silva
cn: João Silva
cn: J. Silva
cn: Joãozinho Silva
```

Isto permite que as procuras efectuadas para `João Silva` e `J. Silva` devolvam as mesmas informações.

Os atributos binários contêm uma cadeia de bytes arbitrária como, por exemplo, uma foto JPEG, e não podem ser utilizados para procurar entradas.

Os atributos booleanos contêm as cadeias `TRUE` ou `FALSE`.

Os atributos de DN contêm nomes distintos de LDAP. Os valores não têm de ser os DNs de entradas existentes, mas têm de ter uma sintaxe de DN válida.

Os atributos da Cadeia de Directórios contêm uma cadeia de texto que utiliza caracteres UTF-8. O atributo pode ser ou não sensível a maiúsculas e minúsculas, relativamente a valores utilizados em filtros de procura (com base na regra de correspondência definida para o atributo), embora o valor seja sempre devolvido como introduzido originalmente.

Os atributos de Hora Generalizada contêm uma representação de cadeia de uma data e hora preparadas para o ano 2000, utilizando horas TMG com um deslocamento de fuso horário TMG opcional. Consulte "Hora Generalizada e UTC" na página 34, para obter mais detalhes sobre a sintaxe destes valores.

Os atributos da Cadeia IA5 contêm uma cadeia de texto que utiliza o conjunto de caracteres IA5 (US ASCII de 7 bits). O atributo pode ser ou não sensível a maiúsculas e minúsculas, relativamente a valores

utilizados em filtros de procura (com base na regra de correspondência definida para o atributo), embora o valor seja sempre devolvido como introduzido originalmente. A Cadeia IA5 também permite utilizar um carácter global para procuras por subcadeias.

Os atributos de números inteiros contêm a representação da cadeia de texto do valor. Por exemplo, `0` ou `1000`.

Os atributos de Número de Telefone contêm uma representação de texto de um número de telefone. O Directory Server não impõe qualquer sintaxe específica para estes valores. Seguem-se os valores válidos: `(555)555-5555`, `555.555.5555` e `+1 43 555 555 5555`.

Os atributos de Hora UTC utilizam um formato de cadeia anterior, não preparado para o ano 2000, para representar datas e horas. Consulte "Hora Generalizada e UTC" na página 34, para obter mais detalhes.

Para obter mais informações, consulte:
- "Elementos comuns de sub-esquema"
- "O atributo objectclass"
- "O atributo attributetypes" na página 22
- "O atributo IBMAttributeTypes" na página 23
- "Regras de correspondência" na página 24
- "Regras de indexação" na página 25
- "Sintaxe de atributos" na página 26

Elementos comuns de sub-esquema

Os elementos seguintes são utilizados para definir a gramática dos valores de atributo de sub-esquema:
- alpha = 'a' - 'z', 'A' - 'Z'
- número = '0' - '9'
- anh = alpha / número / '-' / ';'
- anhstring = 1 * anh
- keystring = alpha [anhstring]
- numericstring = 1 * número
- oid = descr / numericoid
- descr = keystring
- numericoid = numericstring *("." numericstring)
- woid = whsp oid whsp ; conjunto de oids de qualquer formato (OIDs numéricos ou nomes)
- oids = woid / ("(" oidlist ")")
- oidlist = woid *("$" woid) ; descritores de objecto utilizados como nomes de elementos de esquema
- qdescrs = qdescr / (whsp "(" qdescrlist ")" whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp "'" descr "'" whsp

O atributo objectclass

O atributo objectclasses mostra uma lista das classes de objecto suportadas pelo servidor. Cada valor deste atributo representa uma definição de classe de objecto separada. As definições de classes de objecto podem ser adicionadas, eliminadas ou alteradas por modificações apropriadas do atributo objectclasses da entrada cn=esquema. Os valores do atributo objectclasses têm a seguinte gramática, tal como definido pelo RFC 2252:

```
ObjectClassDescription = "(" whsp
        numericoid whsp ; identificador de Objectclass
        [ "NAME" qdescrs ]
        [ "DESC" qdstring ]
```

```
        [ "OBSOLETE" whsp ]
        [ "SUP" oids ] ; objectclasses superiores
        [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; o valor assumido é estrutural
        [ "MUST" oids ] ; AttributeTypes
        [ "MAY" oids ] ; AttributeTypes
      whsp ")"
```

Por exemplo, a definição da objectclass person é:

```
( 2.5.6.6 NAME 'person' DESC 'Define entradas que genericamente representam pessoas.' STRUCTURAL
SUP top MUST ( cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

- O OID desta classe é 2.5.6.6
- O nome é ″person″
- Esta é uma classe de objecto estrutural
- Herda atributos da classe de objecto ″superior″
- Os seguintes atributos são obrigatórios: cn, sn
- Os seguintes atributos são opcionais: userPassword, telephoneNumber, seeAlso, description

Para obter mais informações sobre como alterar as classes de objecto suportadas pelo servidor, consulte “Gerir o esquema” na página 134.

O atributo attributetypes

O atributo attributetypes mostra, numa lista, o atributo suportado pelo servidor. Cada valor deste atributo representa uma definição de atributo separada. As definições de atributo podem ser adicionadas, eliminadas ou alteradas por modificações apropriadas do atributo attributetypes da entrada cn=esquema. Os valores do atributo attributetypes têm a seguinte gramática, tal como definido pelo RFC 2252:

```
AttributeTypeDescription = "(" whsp
        numericoid whsp ; identificador de AttributeType
        [ "NAME" qdescrs ] ; nome utilizado em AttributeType
        [ "DESC" qdstring ] ; descrição
        [ "OBSOLETE" whsp ]
        [ "SUP" woid ] ; deriva deste outro AttributeType
        [ "EQUALITY" woid ; nome de Regra de Correspondência
        [ "ORDERING" woid ; nome de Regra de Correspondência
        [ "SUBSTR" woid ] ; nome de Regra de Correspondência
        [ "SYNTAX" whsp noidlen whsp ]
        [ "SINGLE-VALUE" whsp ] ; valor assumido, com vários valores
        [ "COLLECTIVE" whsp ] ; valor assumido não colectivo
        [ "NO-USER-MODIFICATION" whsp ]; valor assumido modificável pelo utilizador
        [ "USAGE" whsp AttributeUsage ]; userApplications assumido
      whsp ")"

AttributeUsage =
        "userApplications" /
        "directoryOperation" /
        "distributedOperation" / ; partilhado por DSA
        "dSAOperation" ; específico de DSA, o valor depende do servidor
```

As regras de correspondência e os valores de sintaxe têm de ser um dos valores definidos por:

- “Regras de correspondência” na página 24
- “Sintaxe de atributos” na página 26

Apenas os atributos ″userApplications″ podem ser definidos ou modificados no esquema. Os atributos ″directoryOperation″, ″distributedOperation″ e ″dSAOperation″ são definidos pelo servidor e têm um significado específico para o funcionamento do servidor.

Por exemplo, o atributo ″description″ tem a seguinte definição:

```
( 2.5.4.13 NAME 'description' DESC 'Atributo comum ao esquema CIM e LDAP para fornecer uma
descrição detalhada de uma entrada de objecto directório.' EQUALITY caseIgnoreMatch SUBSTR
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
```

- O respectivo OID é 2.5.4.13
- O respectivo nome é ″description″
- A respectiva sintaxe é 1.3.6.1.4.1.1466.115.121.1.15 (Cadeia de Directórios)

Para obter mais informações sobre como alterar os tipos de atributo suportados pelo servidor, consulte “Gerir o esquema” na página 134.

O atributo IBMAttributeTypes

O atributo IBMAttributeTypes pode ser utilizado para definir informações sobre esquemas não abrangidas pela norma de LDAP Versão 3 para atributos. Os valores de IBMAttributeTypes têm de estar em conformidade com a seguinte gramática:

```
IBMAttributeTypesDescription = "(" whsp
        numericoid whsp
      [ "DBNAME"   qdescrs ]            ; no máximo, 2 nomes (tabela, coluna)
      [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
      [ "LENGTH" wlen whsp ]            ; comprimento máximo do atributo
      [ "EQUALITY" [ IBMwlen ] whsp ]   ; criar índice remissivo para regra de correspondência
      [ "ORDERING" [ IBMwlen ] whsp ]   ; criar índice remissivo para regra de correspondência
      [ "APPROX"   [ IBMwlen ] whsp ]   ; criar índice remissivo para regra de correspondência
      [ "SUBSTR"   [ IBMwlen ] whsp ]   ; criar índice remissivo para regra de correspondência
      [ "REVERSE"  [ IBMwlen ] whsp ]   ; inverter índice remissivo para subcadeia
      whsp ")"

   IBMAccessClass =
      "NORMAL"            / ; este é o valor assumido
      "SENSITIVE"         /
      "CRITICAL"          /
      "RESTRICTED"        /
      "SYSTEM"            /
      "OBJECT"

   IBMwlen = whsp len
```

Numericoid
Utilizado para correlacionar o valor de attributetypes com o valor de IBMAttributeTypes.

DBNAME
Pode fornecer 2 nomes no máximo, se forem fornecidos 2 nomes na realidade. O primeiro é o nome da tabela utilizado para este atributo. O segundo é o nome da coluna utilizado para o valor totalmente normalizado do atributo na tabela. Se só fornecer um nome, este será utilizado como o nome da tabela e também como o nome da coluna. Se não fornecer nenhum DBNAME, será utilizado o nome de atributo abreviado (de attributetypes).

ACCESS-CLASS
A classificação de acesso para este tipo de atributo. Se ACCESS-CLASS for omitido, terá como valor assumido normal.

LENGTH
O comprimento máximo deste atributo. O comprimento é expresso como o número de bytes. O Directory Server tem uma provisão para especificar o comprimento de um atributo. No valor attributetypes, a cadeia:

```
( attr-oid ... SYNTAX syntax-oid{len} ... )
```

pode ser utilizada para indicar que attributetype com oid attr-oid tem um comprimento máximo.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE
Se qualquer um destes atributos for utilizado, será criado um índice remissivo para a regra de correspondência equivalente. O comprimento opcional especifica a largura da coluna indexada. É

utilizado um único índice remissivo para implementar várias regras de correspondência. O Directory Server atribui um comprimento de 500, quando não indicado pelo utilizador. O servidor também pode utilizar um comprimento menor do que aquele que o utilizador pediu, quando for apropriado. Por exemplo, quando o comprimento do índice remissivo excede o comprimento máximo do atributo, o comprimento do índice remissivo é ignorado.

Regras de correspondência

Uma regra de correspondência fornece directrizes para a comparação entre cadeias durante uma operação de procura. Estas regras estão divididas em três categorias:

- Equality (Igualdade)
- Ordering (Ordenação)
- Substring (Subcadeia)

Regras de correspondência de igualdade		
Regra de Correspondência	**OID**	**Sintaxe**
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Sintaxe da Cadeia de Directórios
caseExactMatch	2.5.13.5 IA5	Sintaxe da cadeia
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Sintaxe da Cadeia IA5
caseIgnoreMatch	2.5.13.2	Sintaxe da Cadeia de Directórios
distinguishedNameMatch	2.5.13.1	DN - nome exclusivo
generalizedTimeMatch	2.5.13.27	Sintaxe da Hora Generalizada
ibm-entryUuidMatch	1.3.18.0.2.22.2	Sintaxe da Cadeia de Directórios
integerFirstComponentMatch	2.5.13.29	Sintaxe de números inteiros - número inteiro
integerMatch	2.5.13.14	Sintaxe de números inteiros - número inteiro
objectIdentifierFirstComponentMatch	2.5.13.30	Cadeia para conter OIDs. O OID é uma cadeia que contém dígitos (0-9) e vírgulas decimais (,).
objectIdentifierMatch	2.5.13.0	Cadeia para conter OIDs. O OID é uma cadeia que contém dígitos (0-9) e vírgulas decimais (,)
octetStringMatch	2.5.13.17	Sintaxe da Cadeia de Directórios
telephoneNumberMatch	2.5.13.20	Sintaxe do Número de Telefone
uTCTimeMatch	2.5.13.25	Sintaxe de hora UTC

Regras de correspondência de ordenação		
Regra de correspondência	**OID**	**Sintaxe**
caseExactOrderingMatch	2.5.13.6	Sintaxe da Cadeia de Directórios
caseIgnoreOrderingMatch	2.5.13.3	Sintaxe da Cadeia de Directórios

Regras de correspondência de ordenação		
Regra de correspondência	**OID**	**Sintaxe**
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - nome exclusivo
generalizedTimeOrderingMatch	2.5.13.28	Sintaxe da Hora Generalizada

Regras de correspondência de subcadeia		
Regra de correspondência	**OID**	**Sintaxe**
caseExactSubstringsMatch	2.5.13.7	Sintaxe da Cadeia de Directórios
caseIgnoreSubstringsMatch	2.5.13.4	Sintaxe da Cadeia de Directórios
telephoneNumberSubstringsMatch	2.5.13.21	Sintaxe do Número de Telefone

Nota: Hora UTC é o formato da cadeia de hora definido pelas normas ASN.1. Consulte a ISO 8601 e X680. Utilize esta sintaxe para armazenar o valor de hora no formato de Hora UTC. Consulte "Hora Generalizada e UTC" na página 34.

Regras de indexação

As regras de indexação associadas aos atributos possibilitam uma obtenção mais rápida de informações. Se apenas for fornecido o atributo, não serão mantidos quaisquer índices remissivos. O Directory Server fornece as seguintes regras de indexação:

- Equality (Igualdade)
- Ordering (Ordenação)
- Approximate (Aproximado)
- Substring (Subcadeia)
- Reverse (Inversão)

Especificações de regras de indexação para atributos: A especificação de uma regra de indexação para um atributo controla a criação e manutenção de índices remissivos especiais nos valores do atributo. Esta possibilidade reduz significativamente o tempo de resposta em procuras efectuadas com filtros que incluam esses atributos. Os cinco tipos de regras de indexação possíveis estão relacionados com as operações aplicadas ao filtro de procura.

Equality

Aplica-se nas seguintes operações de procura:

- equalityMatch '='

Por exemplo:

```
"cn = João Sousa"
```

Ordering

Aplica-se na seguinte operação de procura:

- greaterOrEqual '>='
- lessOrEqual '<='

Por exemplo:

```
"sn >= Sousa"
```

Approximate

Aplica-se na seguinte operação de procura:

- approxMatch '~='

Por exemplo:

```
"sn ~= sousa"
```

Substring

Aplica-se na operação de procura que utiliza a sintaxe de subcadeia:

- substring '*'

Por exemplo:

```
"sn = McC*"
"cn = J*Sousa"
```

Reverse

Aplica-se na seguinte operação de procura:

- '*' substring

Por exemplo:

```
"sn = *baugh"
```

No mínimo, recomenda-se que seja especificada uma indexação igual em todos os atributos que deverão ser utilizados em filtros de procura.

Sintaxe de atributos

A sintaxe de um atributo define os valores permitidos para esse atributo. O servidor utiliza a definição de sintaxe de um atributo para validar dados e determinar como encontrar correspondências para valores. Por exemplo, um atributo ″Booleano″ só pode ter os valores ″TRUE″ e ″FALSE″.

Sintaxe	OID
Sintaxe da Descrição de Tipo de Atributo	1.3.6.1.4.1.1466.115.121.1.3
Binário - cadeia de octetos	1.3.6.1.4.1.1466.115.121.1.5
Booleano - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Sintaxe da Cadeia de Directórios	1.3.6.1.4.1.1466.115.121.1.15
Sintaxe da Descrição de Regra de Contentores de DIT	1.3.6.1.4.1.1466.115.121.1.16
Sintaxe da Descrição de Regra de DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - nome exclusivo	1.3.6.1.4.1.1466.115.121.1.12
Sintaxe da Hora Generalizada	1.3.6.1.4.1.1466.115.121.1.24
Sintaxe da Cadeia IA5	1.3.6.1.4.1.1466.115.121.1.26
Descrição de Tipo de Atributo da IBM	1.3.18.0.2.8.1
Sintaxe de números inteiros - número inteiro	1.3.6.1.4.1.1466.115.121.1.27
Sintaxe da Descrição de Sintaxe de LDAP	1.3.6.1.4.1.1466.115.121.1.54
Descrição de Regra de Correspondência	1.3.6.1.4.1.1466.115.121.1.30
Descrição de Utilização de Regra de Correspondência	1.3.6.1.4.1.1466.115.121.1.31
Descrição de Formato de Nome	1.3.6.1.4.1.1466.115.121.1.35
Sintaxe de Descrição de Classe de Objecto	1.3.6.1.4.1.1466.115.121.1.37
Cadeia para conter OIDs. O OID é uma cadeia que contém dígitos (0-9) e vírgulas decimais (,). Consulte “Identificador de objecto (OID)” na página 27.	1.3.6.1.4.1.1466.115.121.1.38
Sintaxe do Número de Telefone	1.3.6.1.4.1.1466.115.121.1.50
Sintaxe de Hora UTC. Hora UTC é o formato da cadeia de hora definido pelas normas ASN.1. Consulte a ISO 8601 e X680. Utilize esta sintaxe para armazenar o valor de hora no formato de Hora UTC. Consulte “Hora Generalizada e UTC” na página 34.	1.3.6.1.4.1.1466.115.121.1.53

Identificador de objecto (OID)

Um identificador de objecto (OID) é uma cadeia, de números decimais, que identifica, de forma exclusiva, um objecto. Normalmente, estes objectos são uma classe de objecto ou um atributo.

Se não tiver um OID, pode especificar a classe de objecto ou nome de atributo associado a **-oid**. Por exemplo, se criar o atributo tempID, pode especificar o OID como **tempID-oid**.

É absolutamente fundamental que os OIDs privados sejam obtidos a partir de autoridades legítimas. Existem duas estratégias base para a obtenção de OIDs legítimos:

- Registar os objectos com uma autoridade. Esta estratégia pode ser conveniente, por exemplo, se necessitar de um número menor de OIDs.
- Obter um arco (um arco é uma sub-árvore individual da árvore do OID) a partir de uma autoridade e atribuir os seus próprios OIDs, de acordo com as necessidades. Esta estratégia pode ser preferível se forem necessários muitos OIDs ou se as atribuições de OIDs não forem estáveis.

O American National Standards Institute (ANSI) é a autoridade de registo de nomes de organizações nos Estados Unidos, ao abrigo do processo de registo global estabelecido pela International Standards Organization (ISO) e pela International Telecommunication Union (ITU). Poderá encontrar mais informações sobre o registo de nomes de organizações no sítio da Web da ANSI (www.ansi.org). O arco do OID ANSI para organizações é 2.16.840.1. A ANSI atribuirá um número (NEWNUM), criando um novo arco de OID: 2.16.840.1.NEWNUM.

Na maioria dos países ou regiões, a associação nacional de normas mantém um registo de OIDs. Tal como acontece com o arco da ANSI, estes são, geralmente, arcos atribuídos ao abrigo do OID 2.16. Poderá ser necessária alguma investigação para determinar a autoridade do OID para um país ou região específicos. A organização nacional de normas do seu país ou região pode ser membro da ISO. É possível encontrar os nomes e informações de contacto dos membros da ISO no sítio da Web da ISO (www.iso.ch).

A Internet Assigned Numbers Authority (IANA) atribui números privados de empresas, que são OIDs, no arco 1.3.6.1.4.1. A IANA atribuirá um número (NEWNUM) de modo a que o novo arco de OIDs seja 1.3.6.1.4.1.NEWNUM. Estes números podem ser obtidos no sítio da Web da IANA (www.iana.org).

Assim que tenha sido atribuído um OID à sua organização, poderá definir os seus próprios OIDs anexando ao fim do OID. Por exemplo, suponha que foi atribuído o OID fictício 1.1.1 à sua organização. Não será atribuído a nenhuma outra organização um OID que comece por ″1.1.1″. Pode criar um intervalo para o LDAP anexando ″.1″ para formar 1.1.1.1. Pode ainda subdividir este OID em intervalos para objectclasses (1.1.1.1.1), tipos de atributo (1.1.1.1.2) etc. e atribuir o OID 1.1.1.1.2.34 ao atributo ″foo″.

As entradas de sub-esquema

Existe uma entrada de sub-esquema por servidor. Todas as entradas do directório têm um tipo de atributo subschemaSubentry implícito. O valor do tipo de atributo subschemaSubentry é o DN da entrada do sub-esquema que corresponde à entrada. Todas as entradas sob o mesmo servidor partilham a mesma entrada de sub-esquema e o respectivo tipo de atributo subschemaSubentry tem o mesmo valor. A entrada de sub-esquema tem o DN 'cn=esquema' incluído no código.

A entrada de sub-esquema pertence às classes de objecto 'superior', 'subschema' e 'IBMsubschema'. A classe de objecto 'IBMsubschema' não tem atributos MUST e tem um tipo de atributo MAY ('IBMattributeTypes').

A classe de objecto IBMsubschema

A classe de objecto IBMsubschema só é utilizada na entrada de sub-esquema, do seguinte modo:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'Classe de objecto específica da IBM que armazena todos os atributos e classes de objecto de um
 determinado servidor de directórios.'
SUP 'subschema'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Consultas de esquema

A API ldap_search() pode ser utilizada para consultar a entrada de sub-esquema, tal como é mostrado no seguinte exemplo:

```
DN           : "cn=esquema"
search scope : base
filter       : objectclass=subschema ou objectclass=*
```

Este exemplo obtém o esquema completo. Para obter todos os valores de tipos de atributo seleccionados, utilize o parâmetro attrs em ldap_search. Não pode obter apenas um valor específico de um tipo de atributo específico.

Consulte o tópico "APIs do Directory Server" para obter mais informações sobre a API ldap_search.

Esquema dinâmico

Para executar uma alteração dinâmica num esquema, utilize a API ldap_modify com um DN ″cn=esquema″. Só é permitido adicionar, eliminar ou substituir uma entidade de esquema (por exemplo, um tipo de atributo ou uma classe de objecto) de cada vez.

Para eliminar uma entrada de esquema, especifique o atributo de esquema que define a entrada de esquema (objectclasses ou attributetypes) e, para o respectivo valor, o OID entre parênteses. Por exemplo, para eliminar o atributo com o OID <attr-oid>:

```
dn: cn=esquema
changetype: modify
delete: attributetypes
attributetypes: ( <attr-oid> )
```

Também pode fornecer uma descrição completa. Em qualquer um dos casos, a regra de correspondência utilizada para localizar a entidade de esquema a eliminar é objectIdentifierFirstComponentMatch.

Para adicionar ou substituir uma entidade de esquema, TEM (MUST) de fornecer uma definição de LDAP Versão 3 e PODE (MAY) fornecer a definição da IBM. Em todos os casos, só pode fornecer a definição ou definições da entidade de esquema que pretende afectar.

Por exemplo, para eliminar o tipo de atributo 'cn' (o respectivo OID é 2.5.4.3), utilize ldap_modify() com:

```
LDAPMod  attr;
LDAPMod *attrs[] = { &attr, NULL };
char    *vals [] = { "( 2.5.4.3 )", NULL };
attr.mod_op      = LDAP_MOD_DELETE;
attr.mod_type    = "attributeTypes";
attr.mod_values  = vals;
ldap_modify_s(ldap_session_handle, "cn=esquema", attrs);
```

Para adicionar uma nova barra de tipo de atributo com o OID 20.20.20 que herda do atributo ″name″ e tem 20 caracteres de comprimento:

```
char    *vals1[] = { "( 20.20.20 NAME 'bar' SUP name )" NULL };
char    *vals2[] = { "( 20.20.20 LENGTH 20 )", NULL };
LDAPMod  attr1;
LDAPMod  attr2;
LDAPMod *attrs[] = { &attr1, &attr2, NULL };
attr1.mod_op = LDAP_MOD_ADD;
attr1.mod_type = "attributeTypes";
```

```
attr1.mod_values = vals1;
attr2.mod_op = LDAP_MOD_ADD;
attr2.mod_type = "IBMattributeTypes";
attr2.mod_values = vals2;
ldap_modify_s(ldap_session_handle, "cn=esquema", attrs);
```

A versão de LDIF do acima descrito seria:

```
dn: cn=esquema
changetype: modify
add: attributetypes
attributetypes: ( 20.20.20 NAME 'bar' SUP name )
-
add:ibmattributetypes
ibmattributetypes: (20.20.20 LENGTH 20)
```

Controlos de acesso

As alterações dinâmicas a esquemas só podem ser executadas por um fornecedor de replicações ou DN do administrador.

Replicação

Quando é executada uma alteração dinâmica a um esquema, ela é replicada.

Alterações a esquemas não permitidas

Nem todas as alterações ao esquema são permitidas. As restrições às alterações incluem:

- Qualquer alteração ao esquema tem de deixar o esquema num estado consistente.
- Não é possível eliminar um tipo de atributo que seja um supertipo de outro tipo de atributo. Não é possível eliminar um tipo de atributo que seja ″MAY″ ou ″MUST″ de uma classe de objecto.
- Não é possível eliminar uma classe de objecto que seja uma superclasse de outra.
- Não é possível adicionar os tipos de atributo ou classes de objecto que se refiram a entidades não existentes (por exemplo, sintaxes ou classes de objecto).
- Os tipos de atributo ou classes de objecto não podem ser modificados de modo a que se refiram a entradas não existentes (por exemplo, sintaxes ou classes de objecto).

Não são permitidas alterações ao esquema que afectem o funcionamento do servidor. As definições de esquema que se seguem são necessárias ao Directory Server. Estas não podem ser alteradas.

Classes de objecto:

- accessGroup
- accessRole
- alias
- os400-usrprf
- referral
- replicaObject
- superior

Atributos:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName

- createTimestamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale

- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Sintaxes:
Todas

Regras de correspondência:
Todas

Verificação do esquema

Quando o servidor é inicializado, os ficheiros de esquema são lidos e submetidos a uma verificação de consistência e exactidão. Se as verificações falharem, o servidor não conseguirá proceder à inicialização e emitirá uma mensagem de erro. Durante qualquer alteração dinâmica a um esquema, o esquema resultante também será submetido a uma verificação de consistência e exactidão. Se as verificações falharem, será devolvido um erro e a alteração falha. Determinadas verificações fazem parte da gramática (por exemplo, um tipo de atributo pode ter, no máximo, um supertipo e uma classe de objecto pode ter qualquer número de superclasses).

Os seguintes itens são verificados para os tipos de atributo:

- Dois tipos de atributo diferentes não podem ter o mesmo nome ou OID.
- A hierarquia de herança dos tipos de atributo não tem ciclos.
- O supertipo de um tipo de atributo também tem de ser definido, embora a respectiva definição possa ser apresentada mais tarde ou num ficheiro separado.
- Se um tipo de atributo for um subtipo de outro, ambos terão a mesma UTILIZAÇÃO (USAGE).
- Todos os tipos de atributo têm uma sintaxe que é directamente definida ou herdada.
- Só os atributos operacionais podem ser marcados como NÃO-MODIFICÁVEIS-PELO-UTILIZADOR (NON-USER-MODIFICATION).

Os itens seguintes são verificados para as classes de objecto:

- Duas classes de objecto diferentes não podem ter o mesmo nome ou OID.
- A hierarquia de herança das classes de objecto não tem ciclos.
- A superclasse de uma classe de objecto também deve ser definida, embora a respectiva definição possa ser apresentada mais tarde ou num ficheiro separado.
- Os tipos de atributo ″MUST″ e ″MAY″ de uma classe de objecto também têm de ser definidos, embora a respectiva definição possa ser apresentada mais tarde ou num ficheiro separado.
- Cada classe de objecto estrutural é uma subclasse directa ou indirecta da superior.
- Se uma classe de objecto abstracta tiver superclasses, estas também devem ser abstractas.

Comparar uma entrada com o esquema

Quando uma entrada é adicionada ou modificada através de uma operação de LDAP, a entrada é comparada com o esquema. Por valor assumido, são executadas todas as verificações mostradas nesta secção. Contudo, pode desactivar selectivamente algumas das verificações do esquema, alterando o respectivo nível de verificação. Esta operação é executada através do iSeries Navigator pela alteração do valor do campo **Verificação do esquema** da página **Base de Dados/Sufixos** das propriedades do Directory Server. Consulte “Esquema de configuração do Directory Server” na página 205, para obter informações sobre atributos de configuração de esquemas.

Para estar em conformidade com um esquema, são verificadas as seguintes condições numa entrada:

Relativamente a classes de objecto:

- Devem ter, pelo menos, um valor de tipo de atributo ″objectClass″.
- Podem ter qualquer número de classes de objecto auxiliares, incluindo zero. Não se trata de uma verificação, mas de um esclarecimento. Não existem opções para desactivar esta acção.
- Podem ter qualquer número de classes de objecto abstractas, mas apenas como resultado da herança de classes. Isto significa que, para cada classe de objecto abstracta da entrada, ela também tem uma classe de objecto estrutural ou auxiliar que herda atributos directa ou indirectamente dessa classe de objecto abstracta.
- Devem ter, pelo menos, uma classe de objecto estrutural.
- Devem ter exactamente uma classe de objecto estrutural imediata ou base. Isto significa que todas as classes de objecto estruturais fornecidas com a entrada devem ser todas superclasses

de, exactamente, uma delas. A classe de objecto mais derivada é designada por classe de objecto ″immediate″ ou ″base structural″ da entrada ou, simplesmente, a classe de objecto ″structural″ da entrada.

- Não é possível alterar a respectiva classe de objecto estrutural imediata (em ldap_modify).
- Para cada classe de objecto fornecida com a entrada, é calculado o conjunto de todas as respectivas superclasses directas e indirectas; se alguma dessas superclasses não for fornecida com a entrada, será automaticamente adicionada.
- Se o nível de verificação do esquema for definido como **Versão 3 (estrita)**, terão de ser fornecidas todas as superclasses estruturais. Por exemplo, para criar uma entrada com a objectclass inetorgperson, têm de ser especificadas as seguintes objectclasses: person, organizationalperson e inetorgperson.

A validade dos tipos de atributo de uma entrada é determinada do seguinte modo:

- O conjunto de tipos de atributo MUST da entrada é calculado como a união dos conjuntos de tipos de atributo MUST de todas as respectivas classes de objecto, incluindo as classes de objecto herdadas implícitas. Se o conjunto de tipos de atributo MUST da entrada não for um subconjunto do conjunto de tipos de atributo contidos pela entrada, a entrada será rejeitada.
- O conjunto de tipos de atributo MAY da entrada é calculado como a união dos conjuntos de tipos de atributo MAY de todas as respectivas classes de objecto, incluindo as classes de objecto herdadas implícitas. Se o conjunto de tipos de atributo contidos pela entrada não for um subconjunto da união dos conjuntos de tipos de atributo MUST e MAY da entrada, a entrada será rejeitada.
- Se algum dos tipos de atributo definidos para a entrada estiver marcado como NO-USER-MODIFICATION, a entrada será rejeitada.

A validade dos valores de tipo de atributo de uma entrada é determinada do seguinte modo:

- Para cada tipo de atributo contido pela entrada, se o tipo de atributo só tiver um valor e a entrada tiver vários valores, a entrada será rejeitada.
- Para cada valor de atributo de cada tipo de atributo contido pela entrada, se a respectiva sintaxe não estiver em conformidade com a rotina de verificação da sintaxe desse atributo, a entrada será rejeitada.
- Para cada valor de atributo de cada tipo de atributo contido pela entrada, se o respectivo comprimento for maior que o comprimento máximo atribuído a esse tipo de atributo, a entrada será rejeitada.

A validade do DN é verificada do seguinte modo:

- Verifica-se se a sintaxe está em conformidade com o BNF para DistinguishedNames. Se não estiver em conformidade, a entrada será rejeitada.
- Verifica-se se o RDN é composto apenas por tipos de atributo que sejam válidos para essa entrada.
- Verifica-se se os valores dos tipos de atributo utilizados no RDN aparecem na entrada.

Compatibilidade com o iPlanet

O analisador utilizado pelo Directory Server permite a especificação dos valores de atributo de tipos de atributo de esquema (objectClasses e attributeTypes) com a utilização da gramática do iPlanet. Por exemplo, as descrições e oids numéricos podem ser especificados entre aspas (como se fossem qdescrs), contudo, as informações do esquema são sempre disponibilizadas através de ldap_search. Assim que seja efectuada uma única alteração dinâmica (através de ldap_modify) num valor de atributo de um ficheiro, todo o ficheiro será substituído por um em que todos os valores de atributo seguem as especificações do Directory Server. Uma vez que o analisador utilizado nos ficheiros e nos pedidos de ldap_modify é o mesmo, um ldap_modify que utilize a gramática do iPlanet para valores de atributo será também tratado correctamente.

Quando é efectuada uma consulta na entrada de sub-esquema de um servidor iPlanet, a entrada resultante pode ter vários valores para um determinado OID. Por exemplo, se um certo tipo de atributo tiver dois nomes (como 'cn' e 'commonName'), a descrição desse tipo de atributo será fornecida duas vezes, uma para cada nome. O Directory Server pode analisar um esquema em que a descrição de um único tipo de atributo ou classe de objecto aparece várias vezes (excepto para NAME e DESCR). No entanto, quando o Directory Server publica o esquema, fornece uma única descrição deste tipo de atributo com todos os nomes apresentados (o nome abreviado aparece primeiro). Por exemplo, segue-se o modo como o iPlanet descreve o atributo de nomes comum:

```
( 2.5.4.3 NAME 'cn'
  DESC 'Atributo Padrão'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
( 2.5.4.3 NAME 'commonName'
  DESC 'Atributo Standard, nome alternativo de cn'
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

É assim que o Directory Server o descreve:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' ) SUP name )
```

O Directory Server suporta subtipos. Se não pretender que 'cn' seja um subtipo do nome (o que difere do padrão), pode declarar o seguinte:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )
    DESC 'Atributo Padrão'
    SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

O primeiro nome ('cn') é aceite como o nome preferencial ou abreviado e todos os outros nomes após 'cn' como nomes alternativos. A partir deste ponto, as cadeias'2.3.4.3', 'cn' e 'commonName' (bem como as respectivas equivalentes não sensíveis a maiúsculas e minúsculas) podem ser utilizadas aleatoriamente no esquema ou nas entradas adicionadas ao directório.

Hora Generalizada e UTC

Existem notações diferentes utilizadas para designar informações relacionadas com a data e hora. Por exemplo, o quarto dia de Fevereiro do ano 1999 pode ser escrito como:

```
2/4/99
4/2/99
99/2/4
4.2.1999
04-FEV-1999
```

bem como muitas outras notações.

O Directory Server normaliza a representação de marca de hora ao requerer que os servidores de LDAP suportem duas sintaxes:

- A sintaxe da Hora Generalizada, que assume o seguinte formato:

  ```
  AAAAMMDDHHMMSS[.|,fracção][(+|-HHMM)|Z]
  ```

  São especificados 4 dígitos para o ano, 2 dígitos para o mês, dia, hora, minutos e segundos e uma fracção de segundo opcional. Sem mais adições, uma data e hora são assumidas como estando no fuso horário local. Para indicar que uma hora é especificada com a utilização do Tempo Universal Coordenado, anexe a letra Z maiúscula a uma hora ou a um diferencial de hora local. Por exemplo:

  ```
  "19991106210627.3"
  ```

  que, na hora local, representa 6 minutos, 27,3 segundos após as 21:00 do dia 6 de Novembro de 1999.

  ```
  "19991106210627.3Z"
  ```

  que é o tempo universal coordenado.

  ```
  "19991106210627.3-0500"
  ```

que é a hora local tal como no primeiro exemplo, com uma diferença de 5 horas em relação ao tempo universal coordenado.

Se designar uma fracção de segundo opcional, é necessário um ponto ou uma vírgula. Para um diferencial de hora local, o valor de hora-minutos terá de ser precedido de um sinal '+' ou '-'

- A sintaxe do Tempo universal, que assume o seguinte formato:

  ```
  AAMMDDHHMM[SS][(+ | -)HHMM)|Z]
  ```

  São especificados 2 dígitos para os campos ano, mês, dia, hora, minutos e segundos opcionais. Tal como em GeneralizedTime, pode ser especificado um diferencial de hora opcional. Por exemplo, se a hora local for 00:00 do dia 2 de Janeiro de 1999 e o tempo universal coordenado for 12:00 do dia 2 de Janeiro de 1999, o valor de UTCTime pode ser:

  ```
  "9901021200Z"
  ou "9901020700-0500"
  ```

  Se a hora local for 00:00 do dia 2 de Janeiro de 2001 e o tempo universal coordenado for 12:00 do dia 2 de Janeiro de 2001, o valor de UTCTime pode ser:

  ```
  "0101021200Z"
  ou "0101020700-0500"
  ```

  Uma vez que UTCTime permite apenas 2 dígitos para o valor de ano, não é recomendada a sua utilização.

As regras de correspondência suportadas são generalizedTimeMatch para igualdade e generalizedTimeOrderingMatch para desigualdade. A procura por subcadeia não é permitida. Por exemplo, os seguintes filtros são válidos:

```
 generalized-timestamp-attribute=199910061030
=atributo-marca-hora-utc>=991006
=atributo-marca-hora-generalizada=*
```

Os seguintes filtros não são válidos:

```
=atributo-marca-hora-generalizada=1999*
=atributo-marca-hora-utc>=*1010
```

Publicação

O i5/OS fornece a capacidade que permite ao sistema publicar determinados tipos de informações num directório de LDAP. Ou seja, o sistema criará e actualizará entradas de LDAP que representem vários tipos de dados.

O i5/OS dispõe de suporte incorporado para publicar as seguintes informações num servidor de LDAP:

Utilizadores

Quando configura o i5/OS para publicar o tipo de informações Users (Utilizadores) no Directory Server, ele exporta automaticamente entradas do directório de distribuição do sistema para o Directory Server. Para tal, utiliza a interface de programação de aplicações (API) QGLDSSDD. Este processo também mantém o directório de LDAP sincronizado com as alterações feitas no directório de distribuição do sistema. Para obter informações sobre a API QGLDSSDD, consulte "APIs do Directory Server" no tópico Programação.

A publicação de utilizadores é útil para fornecer acesso de pesquisa LDAP às informações do directório de distribuição do sistema (por exemplo, fornecer acesso de livro de endereços LDAP a clientes de correio POP3 que suportem LDAP, como o Netscape Communicator ou o Microsoft Outlook Express).

Os utilizadores publicados também podem ser utilizados para suportar a autenticação de LDAP com alguns utilizadores publicados a partir do directório de distribuição do sistema e outros utilizadores adicionados ao directório através de outros meios. Um utilizador publicado tem um atributo uid que designa o perfil do utilizador e não tem qualquer atributo userPassword. Quando é recebido um pedido de ligação para uma entrada como esta, o servidor pede à segurança do i5/OS que valide o ID do utilizador e a palavra-passe como um perfil e palavra-passe de utilizador válidos para esse perfil. Se pretender utilizar a autenticação de LDAP e pretender que os utilizadores existentes no i5/OS possam autenticar-se através das respectivas palavras-passe do i5/OS, enquanto os utilizadores sem ser do i5/OS são adicionados manualmente ao directório, deverá considerar este componente.

Informações do sistema

Quando configura o i5/OS para publicar o tipo de informação System (Sistema) no Directory Server, são publicados os seguintes tipos de informações:

- Informações base sobre esta máquina e a edição do sistema operativo.
- Opcionalmente, pode seleccionar uma ou mais impressoras para publicar, caso em que o sistema manterá automaticamente o directório de LDAP sincronizado com alterações que sejam efectuadas a essas impressoras no sistema.

As informações sobre impressoras que podem ser publicadas incluem:

- Localização
- Velocidade de impressão de páginas por minuto
- Suporte para modo dúplex e cor
- Tipo e modelo
- Descrição

Estas informações são provenientes da descrição de dispositivo do sistema a ser publicada. Num ambiente de rede, os utilizadores podem utilizar estas informações para os ajudar a seleccionar uma impressora. As informações são, primeiro, publicadas quando uma impressora é seleccionada para publicação, e actualizadas quando um escritor de impressora é parado ou iniciado, ou quando a descrição da impressora é alterada.

Partilhas de impressão

Quando configura o i5/OS para publicar partilhas de impressora, as informações sobre as partilhas de impressora seleccionadas do iSeries Netserver são publicadas no servidor do Active Directory configurado. A publicação de partilhas de impressão num Active Directory permite que os utilizadores adicionem impressoras do iSeries à respectiva área de trabalho do Windows 2000 com o Assistente para adicionar impressoras do Windows 2000. Para executar esta operação no Assistente para adicionar impressoras, especifique que pretende localizar uma impressora no Active Directory do Windows 2000. Tem de publicar partilhas de impressão num servidor de directórios que suporte o esquema do Active Directory da Microsoft.

TCP/IP Quality of Service

O servidor TCP/IP Quality of Service (QOS) pode ser configurado para utilizar uma política de QOS partilhada definida num directório de LDAP através de um esquema definido pela IBM. O agente de publicação de TCP/IP QOS é utilizado pelo servidor QOS para ler as informações de políticas; ele define o servidor, as informações de autenticação e o local no directório onde são armazenadas as informações de políticas.

Também pode criar uma aplicação para publicar ou procurar outros tipos de informações num directório de LDAP que utilize esta estrutura através da definição de agentes de publicação adicionais e utilizando as APIs de publicação de directórios. Para obter mais informações, consulte "APIs do Directory Server" no tópico Programação.

Replicação

A replicação é uma técnica utilizada pelos servidores de directórios para melhorar o rendimento e a fiabilidade. O processo de replicação mantém os dados de vários directórios sincronizados.

Para obter informações sobre como gerir a replicação, consulte "Gerir a replicação" na página 114. Para obter mais informações sobre replicação, consulte o seguinte:

- "Descrição geral de replicação"
- "Terminologia da replicação" na página 38
- "Acordos de replicação" na página 40
- "Modo de armazenamento das informações de replicação no servidor" na página 40
- "Considerações de segurança para informações de replicação" na página 41

Descrição geral de replicação

A replicação fornece dois benefícios fundamentais:

- Redundância das informações - as réplicas constituem uma cópia de segurança do conteúdo dos respectivos servidores fornecedores.
- Procuras mais rápidas - os pedidos de procura podem ser alargados a vários servidores diferentes, todos com o mesmo conteúdo, em vez de se limitarem a um só servidor. Esta possibilidade reduz o tempo de resposta para conclusão dos pedidos.

Entradas específicas do directório são identificadas como raízes de sub-árvores replicadas, através da adição da objectclass ibm-replicationContext às mesmas. Cada sub-árvore é replicada independentemente. A sub-árvore continua para baixo na árvore de informações de directórios (DIT), até atingir as entradas ao nível das folhas ou outras sub-árvores replicadas. As entradas são adicionadas abaixo da raiz da sub-árvore replicada para conterem as informações sobre a topologia da replicação. Estas entradas são uma ou mais entradas de grupo de réplicas, sob as quais são criadas sub-entradas de réplica. Associados a cada sub-entrada de réplica estão acordos de replicação que identificam os servidores que são fornecidos por (replicados para) cada servidor, para além de definirem as credenciais e informações de marcação.

Através da replicação, qualquer alteração efectuada a um directório é propagada por um ou mais directórios adicionais. Com efeito, uma alteração a um directório aparece em vários directórios diferentes. O IBM Directory suporta um modelo de replicação expandido do tipo principal-subordinado. As topologias de replicação são expandidas, de forma a incluírem:

- A replicação de sub-árvores da Árvore de Informações de Directórios (DIT) para servidores específicos
- Uma topologia multi-nível referida como replicação em cascata
- Atribuição da função do servidor (principal ou réplica) pela sub-árvore.
- Vários servidores principais, referidos como replicação unidade a unidade.

A vantagem da replicação por sub-árvores é o facto de não ser necessário que uma réplica copie todo o directório. Pode ser uma réplica de uma parte, ou sub-árvore, do directório.

O modelo expandido altera o conceito de principal e réplica. Estes termos já não se aplicam a servidores, mas antes às funções que um servidor tem relativamente a uma sub-árvore replicada específica. Um servidor pode funcionar como principal para umas sub-árvores e como réplica para outras. O termo principal é utilizado para um servidor que aceita actualizações de clientes para uma sub-árvore replicada.

O termo réplica é utilizado para um servidor que apenas aceita actualizações de outros servidores designados como fornecedores da sub-árvore replicada.

Existem três tipos de directórios, tal como definido pela respectiva função: *principal/unidade*, *cascata* e *só de leitura*.

Tabela 1. Funções do servidor

Directório	Descrição
Principal/unidade	O servidor principal/unidade contém as informações sobre o directório principal do qual são propagadas actualizações pelas réplicas. Todas as alterações são efectuadas e ocorrem no servidor principal, sendo este responsável pela propagação destas alterações pelas réplicas. Podem existir vários servidores a funcionar como principais relativamente às informações de directórios, sendo cada servidor principal responsável pela actualização de outros servidores principais e de réplica. Esta capacidade é referida como replicação de unidade. A replicação de unidade pode aumentar o rendimento e a fiabilidade. O rendimento é melhorado através do fornecimento de um servidor local para gerir actualizações numa rede vastamente distribuída. A fiabilidade é melhorada através do fornecimento de um servidor principal de cópias de segurança, pronto para funcionar caso o servidor principal falhe. **Notas:** 1. Os servidores principais replicam todas as actualizações de clientes, mas não replicam as actualizações recebidas de outros servidores principais. 2. As actualizações à mesma entrada efectuadas por vários servidores podem causar inconsistências nos dados dos directórios porque não existe resolução de conflitos.
Cascata (reencaminhamento)	Um servidor de cascata é um servidor de réplica que replica todas as alterações que lhe são enviadas. Este servidor distingue-se de um servidor principal/unidade na medida em que um servidor principal/unidade só replica as alterações que sejam efectuadas por clientes ligados a esse servidor. Um servidor de cascata pode aliviar o volume de trabalho de replicação dos servidores principais numa rede que contenha muitas réplicas vastamente dispersas.
Réplica (só de leitura)	Um servidor adicional que contém uma cópia das informações de directórios. As réplicas são cópias do principal (ou da sub-árvore da qual elas são uma réplica). A réplica fornece uma cópia de segurança da sub-árvore replicada.

Se a replicação falhar, esta será repetida mesmo que o servidor principal seja reiniciado. A janela Gerir Filas da ferramenta de administração da Web pode ser utilizada para verificar se ocorreu uma falha de replicação.

Pode pedir actualizações num servidor de réplica, mas as actualizações serão, na realidade, reencaminhadas para o servidor principal através da devolução de uma referência ao cliente. Se a actualização tiver êxito, o servidor principal envia-a para as réplicas. Enquanto o servidor principal não tiver concluído a replicação da actualização, a alteração não será reflectida no servidor de réplica onde foi inicialmente pedida. As alterações são replicadas pela ordem em que são efectuadas no servidor principal.

Se já não estiver a utilizar uma réplica, terá de remover o acordo de replicação do fornecedor. Se deixar a definição, fará com que o servidor coloque em fila todas as actualizações e utilize espaço desnecessário no directório. Além disso, o fornecedor continuará a tentar contactar o consumidor em falta para repetir o envio dos dados.

Terminologia da replicação

Segue-se alguma da terminologia utilizada na descrição da replicação:

Replicação em cascata
Uma topologia de replicação em que existem vários níveis de servidores. Um servidor unidade/principal executa a replicação para um conjunto de servidores só de leitura (reencaminhamento) que, por sua vez, replicam para outros servidores. Este tipo de topologia de replicação retira volume de trabalho de replicação dos servidores principais.

Servidor consumidor
Um servidor que recebe alterações através de replicação de outro servidor (fornecedor).

Credenciais
Identificam o método e as informações necessárias utilizadas pelo fornecedor na ligação ao consumidor. Para ligações simples, estas incluem o DN e palavra-passe. As credenciais são armazenadas numa entrada cujo DN está especificado no acordo de replicação.

Servidor de reencaminhamento
Um servidor só de leitura que replica todas as alterações que lhe são enviadas por um servidor principal ou de unidade. Os pedidos de actualização de clientes são referidos para o servidor principal ou de unidade.

Servidor principal
Um servidor que é passível de escrita (pode ser actualizado) para uma sub-árvore específica.

Sub-árvore imbricada
Uma sub-árvore numa sub-árvore replicada do directório.

Servidor de unidade
O termo utilizado para um servidor principal, quando existem vários servidores principais para uma determinada sub-árvore.

Acordo de replicação
As informações contidas no directório que definem a 'ligação' ou 'caminho de replicação' entre dois servidores. Um servidor chama-se fornecedor (aquele que envia as alterações) e o outro chama-se consumidor (aquele que recebe as alterações). O acordo contém todas as informações necessárias para o estabelecimento de uma ligação do fornecedor ao consumidor e para a marcação da replicação.

Contexto de replicação
Identifica a raiz de uma sub-árvore replicada. A classe de objecto auxiliar ibm-replicationContext pode ser adicionada a uma entrada para marcá-la como raiz de uma área replicada. As informações relacionadas com a topologia de replicação são mantidas num conjunto de entradas criadas abaixo de um contexto de replicação.

Grupo de réplicas
A primeira entrada criada sob um contexto de replicação tem a objectclass ibm-replicaGroup e representa um conjunto de servidores que participam na replicação. Fornece uma localização conveniente para a definição de ACLs para proteger as informações sobre a topologia da replicação. As ferramentas de administração suportam actualmente um grupo de réplicas sob cada contexto de replicação, denominado **ibm-replicagroup=default**.

Sub-entrada de réplica
Abaixo de uma entrada de grupo de réplicas, pode ser criada uma ou mais entradas com a objectclass ibm-replicaSubentry; uma para cada servidor que participe na replicação como fornecedor. A sub-entrada de réplica identifica a função que o servidor desempenha na replicação: principal ou só de leitura. Um servidor só de leitura pode, por sua vez, ter acordos de replicação para suportar a replicação em cascata.

Sub-árvore replicada
Uma parte do DIT que é replicada de um servidor para outro. Com esta concepção, uma determinada sub-árvore pode ser replicada para certos servidores e não para outros. Uma sub-árvore pode ser passível de escrita num determinado servidor, enquanto que outras sub-árvores podem ser só de leitura.

Marcação
A replicação pode ser marcada para ocorrer a determinadas horas, com alterações ao fornecedor acumuladas e enviadas num ficheiro batch. O acordo de réplica contém o DN para a entrada que fornece a marcação.

Servidor fornecedor
Um servidor que envia alterações para outro servidor (consumidor).

Acordos de replicação

Um acordo de replicação é uma entrada do directório com a classe de objecto **ibm-replicationAgreement** criada abaixo de uma sub-entrada de réplica para definir a replicação do servidor representado pela sub-entrada para outro servidor. Estes objectos são semelhantes às entradas replicaObject utilizadas por versões anteriores do Directory Server. O acordo de replicação consiste nos seguintes itens:

- Um nome familiar ao utilizador, usado como o atributo de nomenclatura para o acordo.
- Um URL de LDAP especificando o servidor, número da porta e se deverá ser utilizado SSL.
- O id do servidor consumidor, se conhecido. Os servidores de directório anteriores à V5R3 não têm um id de servidor.
- O DN de um objecto que contenha as credenciais utilizadas pelo fornecedor para ligação ao consumidor.
- Um indicador de DN opcional para um objecto que contenha as informações de marcação para a replicação. Se o atributo não estiver presente, as alterações serão replicadas imediatamente.

O nome familiar ao utilizador pode ser o nome do servidor consumidor ou outra cadeia descritiva à escolha.

O id do servidor consumidor é utilizado pela GUI administrativa para examinar a topologia. Indicado o ID do servidor consumidor, a GUI poderá localizar a sub-entrada correspondente e os respectivos acordos. Para ajudar a reforçar a exactidão dos dados, quando o fornecedor é ligado ao consumidor, obtém o ID do servidor do DSE raiz e compara-o com o valor existente no acordo. É registado um aviso se os IDs do servidor não corresponderem.

Uma vez que é possível replicar o acordo de replicação, é utilizado um DN para um objecto credencial. Isto permite que as credenciais sejam armazenadas numa área não replicada do directório. A replicação dos objectos credenciais (dos quais têm de ser passíveis de obtenção credenciais de ″texto simples″) representa um risco de segurança potencial. O sufixo cn=sistcentrallocal é uma localização assumida apropriada para criar objectos credenciais.

São definidas classes de objectos para cada um dos métodos de autenticação suportados:

- Ligação simples
- SASL
- Mecanismo EXTERNO com SSL
- Autenticação de Kerberos

Pode determinar que uma parte de uma sub-árvore replicada não seja replicada adicionando a classe auxiliar ibm-replicationContext à raiz da sub-árvore, sem definir quaisquer entradas de réplica.

Nota: A ferramenta de administração da Web também se refere aos acordos como ″filas″ ao mencionar o conjunto de alterações que aguardam replicação ao abrigo de um determinado acordo.

Modo de armazenamento das informações de replicação no servidor

As informações de replicação são armazenadas no directório, em três locais:

- A configuração do servidor, que contém informações sobre como outros servidores podem ser autenticados neste servidor para executarem a replicação (por exemplo, que o servidor é autorizado por este a servir de fornecedor).
- Na parte superior de uma sub-árvore replicada do directório. Se ″o=minha empresa″ for a parte superior de uma sub-árvore replicada, será criado um objecto denominado ″ibm-replicagroup=default″ directamente sob a mesma (ibm-replicagroup=default,o=minha empresa). Abaixo do objecto ″ibm-replicagroup=default″, serão colocados objectos adicionais que descrevem os servidores que têm réplicas da sub-árvore e os acordos entre os servidores.
- É utilizado um objecto denominado ″cn=replicação,cn=sistcentrallocal″ para conter informações de réplicas que só são utilizadas por um servidor. Por exemplo, o objecto que contém as credenciais utilizadas por um servidor fornecedor só é necessário ao servidor fornecedor. As credenciais podem ser colocadas sob ″cn=replicação,cn=sistcentrallocal″, o que as tornará acessíveis apenas a esse servidor.

Considerações de segurança para informações de replicação

Reveja as considerações de segurança relativas aos seguintes objectos:

- ibm-replicagroup=default: Os controlos de acesso deste objecto determinam quem pode ver ou alterar as informações de replicação nele armazenadas. Por valor assumido, este objecto herda o controlo de acesso do respectivo ascendente. Deverá considerar a definição do controlo de acesso neste objecto para restringir o acesso às informações de replicação. Por exemplo, pode definir um grupo de utilizadores que irão gerir a replicação. Este grupo pode passar a ser o proprietário do objecto ″ibm-replicagroup=default″ e pode não ser concedido acesso a outros utilizadores para o objecto.
- cn=replicação,cn=sistcentrallocal: Existem duas considerações de segurança relativas a este objecto:
  - O controlo de acesso neste objecto determina quem está autorizado a ver ou a actualizar os objectos nele contidos. O controlo de acesso assumido permite que utilizadores anónimos leiam a maioria das informações, excepto as palavras-passe, e requer autoridade de administrador para adicionar, alterar ou eliminar objectos.
  - Os objectos armazenados em ″cn=sistcentrallocal″ nunca são replicados para outros servidores. Pode colocar credenciais de replicação neste contentor no servidor que utiliza a credencial e estas não ficarão acessíveis para outros servidores. Como alternativa, pode optar por colocar credenciais sob o objecto ″ibm-replicagroup=default″ para que vários servidores partilhem as mesmas credenciais.

Domínios e modelos de utilizador

Os objectos domínio e modelo encontrados na ferramenta de administração da Web são utilizados para eliminar a necessidade, por parte do utilizador, de compreender algumas das questões subjacentes do LDAP.

Um domínio identifica um conjunto de utilizadores e grupos. Especifica informações, numa estrutura de directórios plana, como, por exemplo, onde estão localizados utilizadores e grupos. Um domínio define uma localização para utilizadores (por exemplo, ″cn=utilizadores,o=empresa,c=po″) e cria utilizadores como subordinados imediatos dessa entrada (por exemplo, Joaquim Dias é criado como ″cn=Joaquim Dias,cn=utilizadores,o=empresa,c=po″). Pode definir vários domínios e atribuir-lhes nomes familiares (por exemplo, Utilizadores da Web). O nome familiar pode ser utilizado pelas pessoas que criam e mantêm os utilizadores.

Um modelo descreve o aspecto de um utilizador. Especifica as objectclasses que são utilizadas na criação de utilizadores (quer a objectclass estrutural, quer quaisquer classes auxiliares à sua escolha). Um modelo também especifica o esquema dos painéis utilizados para criar ou editar utilizadores (por exemplo, nomes de separadores, valores assumidos e os atributos a incluir em cada separador).

Quando adiciona um novo domínio, está a criar um objecto ibm-realm no directório. O objecto ibm-realm controla a localização das propriedades do domínio, como onde são definidos utilizadores e grupos e qual o modelo a utilizar. O objecto ibm-realm pode indicar uma entrada de directório existente que seja o ascendente de utilizadores ou pode indicar-se a si própria (o valor assumido), o que a torna no contentor

para novos utilizadores. Por exemplo, pode ter um contentor cn=utilizadores,o=empresa,c=po e criar um domínio denominado `utilizadores` noutro local do directório (pode ser um objecto contentor denominado cn=domínios,cn=material admin,o=empresa,c=po) que identifique cn=utilizadores,o=empresa,c=po como uma localização de utilizadores e grupos. Esta acção cria um objecto ibm-realm:

```
dn: cn=utilizadores,cn=domínios,cn=material admin,o=empresa,c=po
objectclass: superior
objectclass: ibm-realm
objectclass: ibm-staticGroup
ibm-realmUserTemplate: cn=modelo utilizadores,cn=domínios,cn=material admin,o=empresa,c=po
ibm-realmUserContainer: cn=utilizadores,o=empresa,c=po
ibm-realmGroupContainer: cn=utilizadores,o=empresa,c=po
ibm-realmAdminGroup: cn=utilizadores,cn=domínios,cn=material admin,o=empresa,c=po
ibm-realmUserSearchFilter:
cn: users
```

Ou, se não existir um objecto cn=utilizadores,o=empresa,c=po, pode criar o domínio `utilizadores` em o=empresa,c=po e fazer com que este se indicasse a si próprio.

O administrador do directório é responsável pela gestão de modelos de utilizador, domínios e grupos de administradores de domínios. Após a criação de um domínio, os membros do grupo de administradores desse domínio são responsáveis pela gestão dos utilizadores e grupos pertencentes a esse domínio.

Para obter mais informações sobre como gerir domínios e modelos de utilizador, consulte “Gerir domínios e modelos de utilizador” na página 154.

Considerações sobre o suporte de idioma nacional (NLS)

Tenha em atenção as seguintes considerações sobre o NLS:
- Os dados são transferidos entre os servidores e clientes de LDAP no formato UTF-8. São permitidos todos os caracteres ISO 10646.
- O Directory Server utiliza o método de definição de UTF-16 para armazenar dados na base de dados.
- O servidor e o cliente efectuam comparações entre cadeias não sensíveis a maiúsculas/minúsculas. Os algoritmos em maiúsculas não serão correctos para todos os idiomas (locales).

Para obter mais informações sobre UCS-2, consulte “Globalização” no tópico Planeamento.

Consultas do directório de LDAP

As referências permitem que os Directory Servers trabalhem em equipas. Se o DN pedido por um cliente não estiver num directório, o servidor pode enviar (ou referir) automaticamente o pedido para qualquer outro servidor de LDAP.

O Directory Server permite utilizar tipos de referências diferentes. É possível especificar servidores de referência assumidos, em que o servidor de LDAP informará os clientes sempre que um DN não se encontre no directório. Também pode utilizar o seu cliente de LDAP e adicionar entradas ao Directory Server que tenha a referência de objectClass. Isto permite especificar referências baseadas no DN específico pedido por um cliente.

Nota: Com o Directory Server, os objectos de referência têm de conter apenas um nome exclusivo (`dn`), uma `objectClass` e um atributo de referência (`ref`). Consulte “ldapsearch” na página 188 para obter um exemplo ilustrativo desta restrição.

Os servidores de referência estão directamente relacionados com os servidores de réplica. Uma vez que os dados nos servidores de réplica não podem ser alterados a partir dos clientes, a réplica refere todos os pedidos para alterar dados do directório ao servidor principal.

Transacções

Pode configurar o seu Directory Server de modo a permitir que os clientes utilizem transacções. Para obter mais informações sobre a configuração de definições de transacção, consulte “Especificar definições de transacção” na página 107.) Uma transacção é um grupo de operações de directório de LDAP que é tratada como uma unidade. Nenhuma das operações de LDAP individuais que constituem uma transacção são permanentes até todas as operações da transacção terem sido concluídas por completo e a transacção ter sido consolidada. Se alguma das operações falhar ou se a transacção for cancelada, as restantes operações serão desfeitas. Esta capacidade poderá ajudar os utilizadores a manter as operações de LDAP organizadas. Por exemplo, um utilizador poderá definir uma transacção no cliente que eliminará várias entradas de directório. Se o cliente perder a ligação ao servidor a meio da transacção, nenhuma das entradas será eliminada. Como tal, o utilizador apenas terá de reiniciar a transacção, em vez de ter de verificar as entradas que tenham sido eliminadas com sucesso.

As seguintes operações de LDAP podem fazer parte de uma transacção:

- adicionar
- modificar
- modificar RDN
- eliminar

Nota: Não inclua alterações ao esquema do directório (o sufixo cn=esquema) nas transacções. Apesar de ser possível incluí-las, elas não podem ser desfeitas na eventualidade de a transacção falhar. Isto poderá evitar possíveis problemas de resultados imprevisíveis no Directory Server.

Segurança do Directory Server

Consulte o seguinte para obter mas informações sobre a segurança do Directory Server:

- “Auditoria”
- “Secure Sockets Layer (SSL) e Transport Layer Security com o Directory Server” na página 44
- “Autenticação de Kerberos com o Directory Server” na página 44)
- “Grupos e funções” na página 45
- “Listas de controlo de acesso” na página 51
- “Propriedade de objectos do directório de LDAP” na página 63
- “Política de palavras-passe” na página 63
- “Autenticação” na página 67

Auditoria

O Directory Server suporta a auditoria de segurança de OS/400. Os itens passíveis de auditoria incluem:

- Ligações e separações do Directory Server.
- Alterações e permissões dos objectos do directório de LDAP.
- Alterações na propriedade dos objectos de directório de LDAP.
- Criação, eliminação, procuras e alterações a objectos do directório de LDAP.
- Alterações da palavra-passe do administrador e actualização de nomes distintos (DNs)
- Alterações de palavras-passe de utilizadores.
- Importações e exportações de ficheiros.

Poderá ser necessário efectuar alterações às definições de auditoria do i5/OS para a auditoria às entradas de directório funcionar. Se o valor de sistema QAUDCTL tiver *OBJAUD especificado, poderá activar a auditoria de objectos através do iSeries Navigator. Para obter mais informações sobre auditoria, consulte

Security - Reference  ou o tópico “Auditoria de segurança”.

Secure Sockets Layer (SSL) e Transport Layer Security com o Directory Server

Para tornar as comunicações com o seu Directory Server mais seguras, o Directory Server pode utilizar a segurança de Secure Sockets Layer (SSL).

Para utilizar o SSL com o Directory Server, tem de ter um dos produtos do Cryptographic Access Provider (5722-ACx) instalado no sistema. Se pretende utilizar o SSL do iSeries Navigator, terá de ter instalado no seu PC um dos produtos Client Encryption (5722-CEx). Este software é necessário se pretender efectuar:

- Configurar e administrar o Directory Server a partir da estação de trabalho utilizando uma ligação com SSL. Isto inclui tarefas que pode efectuar a partir do iSeries Navigator.
- Utilizar uma ligação de SSL com aplicações criadas pelo utilizador com as interfaces de programação de aplicações (APIs) do cliente de LDAP.

O SSL é a norma de segurança da Internet. Pode utilizar o SSL para comunicar com clientes de LDAP, assim como com servidores de LDAP de réplicas. Pode utilizar a autenticação de cliente para além da autenticação do servidor para fornecer segurança adicional às suas ligações de SSL. A autenticação de cliente requer que o cliente de LDAP apresente um certificado digital que confirme a identidade do cliente ao servidor antes de ser estabelecida uma ligação.

Para utilizar SSL, tem de ter o Gestor de Certificados Digitais (DCM - Digital Certificate Manager), opção 34 do i5/OS, instalado no sistema. O DCM fornece uma interface para criar e gerir certificados digitais e arquivos de certificados. Consulte o tópico ""Gestor de Certificados Digitais"", para obter mais informações sobre certificados digitais e a utilização do DCM. Para obter informações sobre SSL no iSeries, consulte o tópico "Secure Sockets Layer (SSL)". Para obter informações sobre TLS no servidor iSeries, consulte os Protocolos SSL e Transport Layer Security (TLS) suportados.

Autenticação de Kerberos com o Directory Server

O Directory Server permite utilizar a autenticação de Kerberos. O Kerberos é um protocolo de autenticação de rede que utiliza uma criptografia de chave secreta para fornecer uma eficaz autenticação às aplicações de cliente/servidor.

Para activar a autenticação de Kerberos, terá de ter um dos produtos do Cryptographic Access Provider (5722AC2 ou 5722AC3) instalado no sistema. Também terá de ter configurado o serviço de autenticação de rede.

O suporte de Kerberos do Directory Server fornece suporte ao mecanismo GSSAPI SASL. Permite que ambos os clientes de LDAP do Directory Server e do Windows 2000 utilizem a autenticação de Kerberos com o Directory Server.

O **nome principal de Kerberos** que o servidor utiliza tem o seguinte formato:

```
nome-serviço/nome-sistemacentral@domínio
```

O `nome-serviço` é ldap (ldap tem de estar em minúsculas), `nome-sistemacentral` é o nome completo de TCP/IP do sistema e `domínio` é o domínio assumido especificado na configuração de sistemas do Kerberos.

Por exemplo, para um sistema denominado `meu-as400` no domínio de TCP/IP `empresa.com`, com um domínio de Kerberos assumido `EMPRESA.COM`, o nome de principal de Kerberos do servidor de LDAP `serialdap/meu-as400.empresa.com@EMPRESA.COM`. O domínio de Kerberos assumido é especificado no ficheiro de configuração do Kerberos (por valor assumido, /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) com a directiva default_realm (default_realm = EMPRESA.COM). O Directory Server não pode ser configurado para utilizar a autenticação de Kerberos se o domínio assumido não tiver sido configurado.

Quando é utilizada a autenticação de Kerberos, o Directory Server associa um nome exclusivo (DN) à ligação que determina o acesso aos dados do directório.Poderá seleccionar ter um DN do servidor associado a um dos seguintes métodos:

- O servidor poderá criar um DN baseado no ID de Kerberos. Quando seleccionar esta opção, uma entidade de Kerberos no formato ″director@domínio″ gera um DN no formato ″ibm-kn=director@domínio″. ibm-kn= é equivalente a ibm-kerberosName=.
- O servidor poderá procurar, no directório, um nome exclusivo (DN) que contenha uma entrada de principal e domínio de Kerberos. Quando escolhe esta opção, o servidor procura, no directório, uma entrada que especifique esta identidade de Kerberos.

Tem de ter um ficheiro de tabela de chaves (keytab) que contenha uma chave para o serviço principal de LDAP. Consulte o tópico Serviço de autenticação de rede do Information Center em Segurança, para obter mais informações sobre o Kerberos no servidor iSeries. A secção Configurar serviço de autenticação de rede contém informações sobre a adição de informações a ficheiros de tabelas de chaves.

Grupos e funções

Um grupo é uma lista, um conjunto de nomes. Um grupo pode ser utilizado nos atributos **aclentry**, **ibm-fliterAclEntry** e **entryowner**, para controlar o acesso, ou em utilizações específicas de aplicações, como numa lista de correio a enviar; consulte “Listas de controlo de acesso” na página 51. Os grupos podem ser definidos como estáticos, dinâmicos ou imbricados. Para obter informações sobre como trabalhar com grupos, consulte “Gerir utilizadores e grupos” na página 151.

As funções são semelhantes aos grupos na medida em que são representadas no directório por um objecto. Além disso, as funções contêm um grupo de DNs.

Consulte o seguinte para obter mais informações:

Grupos estáticos

Um grupo estático define cada membro individualmente com a utilização da objectclass **groupOfNames**, **groupOfUniqueNames**, **accessGroup** ou **accessRole** ou a objectclass auxiliar **ibm-staticgroup**. Estas objectclasses requerem o atributo **member** (ou uniqueMember no caso de groupOfUniqueNames). Um grupo estático que utilize as objectclasses estruturais **groupOfNames** ou **groupOfUniqueNames** tem de ter, pelo menos, um membro. Um grupo que utilize as objectclasses estruturais **accessGroup** ou **accessRole** pode estar vazio. Um grupo estático também pode ser definido com a utilização da objectclass auxiliar **ibm-staticGroup**, que não requer o atributo **member** e que, por esse motivo, pode estar vazia.

Uma entrada de grupo comum é:

```
DN: cn=Pessoal Dev.,ou=Almada,c=PO
objectclass: accessGroup
 cn: Pessoal Dev.
 member: cn=Joaquim Dias,o=IBM,c=PO
 member: cn=Joana Silva,o=IBM,c=PO
 member: cn=Jorge Silva,o=IBM,c=PO
```

Cada objecto de grupo contém um atributo com vários valores que consistem em DNs de membros.

Após a eliminação de um grupo de acesso, este também é eliminado de todas as ACLs às quais foi aplicado.

Grupos dinâmicos

Um grupo dinâmico define os respectivos membros de maneira diferente de um grupo estático. Em vez de os apresentar individualmente, o grupo dinâmico define os respectivos membros utilizando uma procura de LDAP. O grupo dinâmico utiliza a objectclass estrutural **groupOfURLs** (ou objectclass auxiliar **ibm-dynamicGroup**) e o atributo **memberURL** para definir a procura utilizando uma sintaxe de URL de LDAP simplificada.

```
ldap:///<DN base da procura> ? ? <âmbito da procura> ? <filtro de procura>
```

Nota: Tal como o exemplo ilustra, o nome do sistema central não pode estar presente na sintaxe. Os parâmetros restantes correspondem à sintaxe de URL de ldap normal. Cada campo de parâmetro tem de ser separado por um ?, mesmo que não seja especificado nenhum parâmetro. Normalmente, é incluída uma lista de atributos a devolver entre o DN base e o âmbito da procura. Este parâmetro também não é utilizado pelo servidor na determinação dos membros de grupo dinâmicos e, por isso, pode ser omitido. No entanto, o separador **?** tem de estar presente,

em que:

DN base da procura
É o ponto a partir do qual começa a procura no directório. Pode ser o sufixo ou raiz do directório como, por exemplo, **ou=Almada**. Este parâmetro é obrigatório.

âmbito da procura
Especifica a extensão da procura. O âmbito assumido é base.

base Devolve informações apenas sobre o DN base especificado no URL

um Devolve informações sobre as entradas num nível abaixo do DN base especificado no URL. Não inclui a entrada base.

sub Devolve informações sobre as entradas em todos os níveis abaixo e inclui o DN base.

filtro de procura
É o filtro que o utilizador pretende aplicar às entradas dentro do âmbito da procura. Consulte "a opção de filtro de ldapsearch" na página 192 para obter informações sobre a sintaxe de searchfilter. O valor assumido é objectclass=*

A procura de membros dinâmicos é sempre interna relativamente ao servidor, de modo que, ao contrário de um URL de ldap completo, nunca é especificado um nome de sistema central e um número de porta e o protocolo é sempre **ldap** (nunca **ldaps**). O atributo **memberURL** pode conter qualquer tipo de URL, mas o servidor só utiliza **memberURL**s que comecem por **ldap:///** para determinar os membros de grupo dinâmicos.

Exemplos

Uma entrada única em que o âmbito assume o valor base e o filtro assume o valor objectclass=*:

```
ldap:///cn=Joaquim Dias, cn=Empregados, o=Empresa, c=PO
```

Todas as entradas que estejam 1 nível abaixo de cn=Empregados e o filtro assumem o valor objectclass=*:

```
ldap:///cn=Empregados, o=Empresa, c=PO??um
```

Todas as entradas sob o-Empresa com a objectclass=person:

```
ldap:///o=Empresa, c=PO??sub?objectclass=person
```

Dependendo das classes de objecto que utilizar para definir entradas de utilizador, estas entradas podem não conter atributos que sejam apropriados para determinar os membros incluídos no grupo. Pode utilizar a classe de objecto auxiliar **ibm-dynamicMember** para alargar as suas entradas de utilizador de

modo a incluírem o atributo **ibm-group**. Este atributo permite adicionar valores arbitrários às entradas de utilizador para funcionarem como destinos para os filtros dos grupos dinâmicos. Por exemplo:

Os membros deste grupo dinâmico são entradas directamente sob a entrada cn=utilizadores,ou=Almada que têm um atributo ibm-group igual a GRUPO1:

```
dn: cn=GRUPO1,ou=Almada
 objectclass: groupOfURLs
 cn: GROUP1
 memberURL: ldap:///cn=utilizadores,ou=Almada??um?(ibm-group=GRUPO1)
```

Segue-se um membro exemplo de cn=GRUPO1,ou=Almada:

```
dn: cn=membro do Grupo 1, cn=utilizadores, ou=almada
 objectclass: person
 objectclass: ibm-dynamicMember
 sn: member
 userpassword: memberpassword
 ibm-group: GRUPO1
```

Grupos imbricados

A imbricação de grupos permite a criação de relações hierárquicas que podem ser utilizadas para definir a filiação de membros em grupos herdada. Um grupo imbricado é definido como uma entrada de grupo descendente cujo DN é referenciado por um atributo contido numa entrada de grupo ascendente. Um grupo ascendente é criado pelo alargamento de uma das classes de objecto de grupo estruturais **groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** ou **groupOfURLs**) com a adição da classe de objecto auxiliar **ibm-nestedGroup**. Após o alargamento de um grupo imbricado, podem ser adicionados zero ou mais atributos **ibm-memberGroup**, cujos valores deverão ser definidos como os DNs de grupos imbricados descendentes. Por exemplo:

```
dn: cn=Grupo 2, cn=Grupos, o=IBM, c=PO
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: superior
 cn: Grupo 2
 description: Grupo composto por membros estáticos e imbricados.
 member: cn=Pessoa 2.1, cn=Dept 2, cn=Empregados, o=IBM, c=PO
 member: cn=Pessoa 2.2, cn=Dept 2, cn=Empregados, o=IBM, c=PO
 ibm-memberGroup: cn=Grupo 8, cn=Imbricado Estático, cn=Grupos, o=IBM, c=PO
```

Não é permitida a introdução de ciclos na hierarquia de grupos imbricados. Se ficar determinado que uma operação com grupos imbricados resulta numa referência cíclica, quer directamente, quer por herança, isso será considerado como uma violação de restrição, provocando a falha da actualização.

Grupos híbridos

Qualquer uma das classes de objecto de grupo estrutural pode ser alargada de maneira a que os membros desse grupo sejam descritos por uma combinação de tipos de membros estáticos, dinâmicos e imbricados. Por exemplo:

```
dn: cn=Grupo 10, cn=Grupos, o=IBM, c=PO
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: superior
 cn: Grupo 10
 description: Grupo composto de membros estáticos, dinâmicos e imbricados.
 memberURL: ldap:///cn=Almada, cn=Empregados, o=IBM, c=PO??um?objectClass=person
 ibm-memberGroup: cn=Grupo 9, cn=Imbricado Dinâmico, cn=Grupos, o=IBM, c=PO
 member: cn=Pessoa 10.1, cn=Dept 2, cn=Empregados, o=IBM, c=PO
 member: cn=Pessoa 10.2, cn=Dept 2, cn=Empregados, o=IBM, c=PO
```

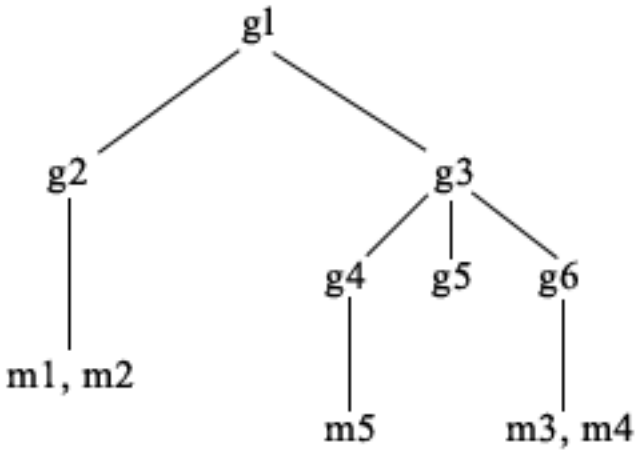
Determinar a filiação de membros em grupos

Podem ser utilizados dois atributos operacionais para consultar a filiação de membros em grupos. Para uma determinada entrada de grupo, o atributo operacional **ibm-allMembers** enumera o conjunto

agregado da filiação de membros em grupos, incluindo os membros estáticos, dinâmicos e imbricados, tal como descrito pela hierarquia de grupos imbricados. Para uma determinada entrada de utilizador, o atributo operacional **ibm-allGroups** enumera o conjunto agregado de grupos, incluindo grupos anteriores, nos quais esse utilizador está filiado.

Um solicitador só poderá receber um subconjunto do total de dados pedidos, dependendo do modo como as ACLs foram definidas nos dados. Qualquer utilizador poderá pedir os atributos operacionais **ibm-allMembers** e **ibm-allGroups**, mas o conjunto de dados devolvido só contém dados referentes às entradas e atributos de LDAP para os quais o solicitador tenha direitos de acesso. O utilizador que solicitar o atributo **ibm-allMembers** ou **ibm-allGroups** terá de ter acesso aos valores de atributo **member** ou **uniquemember** do grupo e dos grupos imbricados para poder ver membros estáticos e também tem de poder executar as procuras especificadas nos valores de atributo **memberURL** para poder ver membros dinâmicos. Por exemplo:

Exemplos de hierarquias



Neste exemplo, **m1** e **m2** são o atributo member de **g2**. A ACL para **g2** permite que o **utilizador1** leia o atributo member, mas o **utilizador 2** não tem acesso ao atributo member. O LDIF da entrada **g2** é o seguinte:

```
dn: cn=g2,cn=grupos,o=ibm,c=po
objectclass: accessGroup
cn: g2
member: cn=m1,cn=utilizadores,o=ibm,c=po
member: cn=m2,cn=utilizadores,o=ibm,c=po
aclentry: id-acesso:cn=utilizador1,cn=utilizadores,o=ibm,c=po:normal:rsc
aclentry: id-acesso:cn=utilizador2,cn=utilizadores,o=ibm,c=po:normal:rsc:at.member:recusar:rsc
```

A entrada **g4** utiliza a entrada de acl assumida, que permite que o **utilizador1** e o **utilizador2** leiam o respectivo atributo member. O LDIF da entrada **g4** é o seguinte:

```
dn: cn=g4, cn=grupos,o=ibm,c=po
objectclass: accessGroup
cn: g4
member: cn=m5, cn=utilizadores,o=ibm,c=po
```

A entrada **g5** é um grupo dinâmico, que obtém os respectivos dois membros do atributo memberURL. O LDIF da entrada **g5** é o seguinte:

```
dn: cn=g5, cn=grupos,o=ibm,c=po
objectclass: container
objectclass: ibm-dynamicGroup
cn: g5
memberURL: ldap:///cn=utilizadores,o=ibm,c=po??sub?(|(cn=m3)(cn=m4))
```

As entradas **m3** e **m4** são membros do grupo **g5** porque correspondem ao **memberURL**. A ACL da entrada **m3** permite que tanto o **utilizador1**, como o **utilizador2**, a procurem. A ACL das entradas **m4** não permite que o **utilizador2** a procure. O LDIF de **m4** é o seguinte:

```
dn: cn=m4, cn=utilizadores,o=ibm,c=po
objectclass:person
cn: m4
sn: quatro
aclentry: id-acesso:cn=utilizador1,cn=utilizadores,o=ibm,c=po:normal:rsc
aclentry: id-acesso:cn=utilizador2,cn=utilizadores,o=ibm,c=po
```

Exemplo 1:

O utilizador 1 efectua uma pesquisa para obter todos os membros do grupo **g1**. Como o utilizador 1 tem acesso a todos os membros, são todos apresentados.

```
ldapsearch -D cn=utilizador1,cn=utilizadores,o=ibm,c=po -w ppsutilizador1 -s base -b cn=g1,
           cn=grupos,o=ibm,c=po objectclass=* ibm-allmembers


cn=g1,cn=grupos,o=ibm,c=po
ibm-allmembers: CN=M1,CN=UTILIZADORES,O=IBM,C=PO
ibm-allmembers: CN=M2,CN=UTILIZADORES,O=IBM,C=PO
ibm-allmembers: CN=M3,CN=UTILIZADORES,O=IBM,C=PO
ibm-allmembers: CN=M4,CN=UTILIZADORES,O=IBM,C=PO
ibm-allmembers: CN=M5,CN=UTILIZADORES,O=IBM,C=PO
```

Exemplo 2:

O utilizador 2 executa uma procura para obter todos os membros do grupo **g1**. O utilizador 2 não tem acesso aos membros **m1** ou **m2** porque estes não têm acesso ao atributo member referente ao grupo **g2**. O utilizador 2 tem acesso ao atributo member de **g4** e, por isso, tem acesso ao membro **m5**. O utilizador 2 pode executar a procura no memberURL do **g5** relativo à entrada **m3**, de modo que esse membro está apresentado, mas não pode executar a procura de **m4**.

```
ldapsearch -D cn=utilizador2,cn=utilizadores,o=ibm,c=po -w ppsutilizador2 -s base -b cn=g1,
           cn=grupos,o=ibm,c=po objectclass=* ibm-allmembers


cn=g1,cn=grupos,o=ibm,c=po
ibm-allmembers: CN=M3,CN=UTILIZADORES,O=IBM,C=PO
ibm-allmembers: CN=M5,CN=UTILIZADORES,O=IBM,C=PO
```

Exemplo 3:

O utilizador 2 executa uma procura para verificar se **m3** é membro do grupo **g1**. O utilizador 2 tem acesso a esta procura, pelo que a procura mostra que **m3** é membro do grupo **g1**.

```
ldapsearch -D cn=utilizador2,cn=utilizadores,o=ibm,c=po -w ppsutilizador2  -s base -b cn=m3,
           cn=utilizadores,o=ibm,c=po objectclass=* ibm-allgroups


cn=m3,cn=utilizadores,o=ibm,c=po
ibm-allgroups: CN=G1,CN=GRUPOS,O=IBM,C=PO
```

Exemplo 4:

O utilizador 2 executa uma procura para verificar se **m1** é membro do grupo **g1**. O utilizador 2 não tem acesso ao atributo member, pelo que a procura não mostra se **m1** é membro do grupo **g1**.

```
ldapsearch -D cn=utilizador2,cn=utilizadores,o=ibm,c=po -w ppsutilizador2 -s base -b
           cn=m1,cn=utilizadores,o=ibm,c=po objectclass=* ibm-allgroups


cn=m1,cn=utilizadores,o=ibm,c=po
```

Classes de objecto de grupo para grupos imbricados e dinâmicos

ibm-dynamicGroup

Esta classe auxiliar permite o atributo opcional **memberURL**. Utilize-a com uma classe estrutural, como **groupOfNames**, para criar um grupo híbrido com membros estáticos e dinâmicos.

ibm-dynamicMember
Esta classe auxiliar permite o atributo opcional **ibm-group**. Utilize-a como atributo filtro para grupos dinâmicos.

ibm-nestedGroup
Esta classe auxiliar permite o atributo opcional **ibm-memberGroup**. Utilize-a com uma classe estrutural, como **groupOfNames**, para permitir a imbricação de subgrupos no grupo ascendente.

ibm-staticGroup
Esta classe auxiliar permite o atributo opcional **member**. Utilize-a com uma classe estrutural, como **groupOfURLs**, para criar um grupo híbrido com membros estáticos e dinâmicos.

Nota: O **ibm-staticGroup** é a única classe para a qual **member** é *opcional*; todas as outras classes que aceitem **member** requerem, pelo menos, um membro.

Tipos de atributo de grupos

ibm-allGroups
Mostra todos os grupos aos quais pertence uma entrada. Uma entrada pode ser um membro directamente pelos atributos **member**, **uniqueMember** ou **memberURL**, ou indirectamente pelo atributo **ibm-memberGroup**. Este atributo operacional **Só de leitura** não é permitido num filtro de procura. O atributo **ibm-allGroups** pode ser utilizado num pedido de comparação para determinar se uma entrada é membro de um grupo específico. Por exemplo, para determinar se ″cn=joão silva,cn=utilizadores,o=minha empresa″ é membro do grupo ″cn=administradores de sistema, o=minha empresa″:

```
rc = ldap_compare_s(ld, "cn=joão silva,cn=utilizadores,o=minha empresa,"ibm-allgroups",
    "cn=administradores de sistema,.o=minha empresa");
```

ibm-allMembers
Mostra todos os membros de um grupo. Uma entrada pode ser um membro directamente pelos atributos **member**, **uniqueMember** ou**memberURL**, ou indirectamente pelo atributo **ibm-memberGroup**. Este atributo operacional **Só de leitura** não é permitido num filtro de procura. O atributo **ibm-allMembers** pode ser utilizado num pedido de comparação para determinar se um DN é membro de um determinado grupo. Por exemplo, para determinar se ″cn=joão silva,cn=utilizadores,o=minha empresa″ é membro do grupo ″cn=administradores de sistema, o=minha empresa″:

```
rc = ldap_compare_s(ld, "cn=administradores de sistema,o=minha empresa, "ibm-allmembers",
    "cn=joão silva,cn=utilizadores,o=minha empresa");
```

ibm-group
É um atributo aceite pela classe auxiliar **ibm-dynamicMember**. Utilize-o para definir valores arbitrários para controlar a filiação de membros da entrada em grupos dinâmicos. Por exemplo, adicione o valor ″Equipa de Bowling″ para incluir a entrada em qualquer **memberURL** que tenha o filtro″ibm-group=Equipa de Bowling″.

ibm-memberGroup
É um atributo aceite pela classe auxiliar **ibm-nestedGroup**. Identifica subgrupos de uma entrada de grupo ascendente. Os membros de todos estes subgrupos são considerados como membros do grupo ascendente durante o processamento de ACLs ou os atributos operacionais **ibm-allMembers** e **ibm-allGroups**. As entradas de sub-grupo propriamente ditas *não* são membros. A filiação de membros imbricados é recorrente.

member
Identifica os nomes distintos para cada membro do grupo. Por exemplo: `member: cn=João Silva, dc=ibm, dc=com`.

memberURL
Identifica um URL associado a cada membro de um grupo. Pode ser utilizado qualquer tipo de URL identificado. Por exemplo: `memberURL: ldap:///cn=jsilva,dc=ibm,dc=com`.

uniquemember

Identifica um grupo de nomes associado a uma entrada em que, a cada nome, foi atribuído um uniqueIdentifier, para assegurar a exclusividade. Um valor para o atributo uniqueMember é um DN seguido do uniqueIdentifier. Por exemplo: `uniqueMember: cn=João Silva, dc=ibm, dc=com 17`.

Funções

A autorização baseada em funções é um complemento conceptual da autorização baseada em grupos e é útil em certos casos. Como membro de uma função, o utilizador tem autoridade para fazer o que for necessário para a função de modo a executar um trabalho. Ao contrário de um grupo, uma função está associada a um conjunto de permissões implícito. Não existe uma noção exacta das permissões que são obtidas (ou recusadas) por se ser membro de um grupo.

As funções são semelhantes aos grupos na medida em que são representadas no directório por um objecto. Além disso, as funções contêm um grupo de DNs. As funções que se destinarem a ser utilizadas no controlo de acesso têm de ter uma objectclass de 'AccessRole'. A objectclass 'Accessrole' é uma subclasse da objectclass 'GroupOfNames'.

Por exemplo, se existisse um conjunto de DNs como 'admin sis', a primeira reacção do utilizador poderia ser considerá-los como o 'grupo admin sis' (uma vez que grupos e utilizadores são os tipos mais comuns de atributos de privilégio). No entanto, como existe um conjunto de permissões que o utilizador esperaria receber como membro de 'admin sis', o conjunto de DNs pode ser definido mais precisamente como 'função admin sis'.

Listas de controlo de acesso

As listas de controlo de acesso (ACLs) fornecem um meio para proteger informações armazenadas num directório de LDAP. Os administradores utilizam ACLs para restringir o acesso a partes diferentes do directório ou a entradas específicas do directório. As alterações a cada entrada e atributo do directório podem ser controladas através da utilização de ACLs. Uma ACL para uma determinada entrada ou atributo pode ser herdada da respectiva entrada ascendente ou pode ser definida explicitamente.

É mais aconselhável criar a sua estratégia de controlo de acesso através da criação de grupos de utilizadores a serem utilizados durante a definição do acesso a objectos e atributos. Defina a propriedade e o acesso ao nível mais elevado possível na árvore e permita que os controlos sejam herdados no sentido descendente na árvore.

Os atributos operacionais associados ao controlo de acesso, como entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource e aclPropagate, não são comuns, uma vez que estão associados de forma lógica a cada objecto, mas podem ter valores que dependem de outros objectos mais acima na árvore. Dependendo do modo como forem estabelecidos, estes valores de atributo podem ser explícitos para um objecto ou herdados de um objecto anterior.

O modelo de controlo de acesso define dois conjuntos de atributos:as Informações de Controlo de Acesso (ACI) e as informações de entryOwner. As ACI definem os direitos de acesso concedidos a um objecto especificado relativamente às operações que executam nos objectos aos quais se aplicam. Os atributos aclEntry e aclPropagate aplicam-se à definição de ACI. As informações de entryOwner definem os sujeitos que podem definir as ACIs para o objecto entrada associado. Os atributos entryOwner e ownerPropagate aplicam-se à definição de entryOwner.

Existem dois tipos de listas de controlo de acesso à escolha: ACLs baseadas em filtros e ACLs não filtradas. As ACLs não filtradas aplicam-se explicitamente à entrada de directório que as contém, mas podem ser propagadas a nenhuma ou a todas as respectivas entradas descendentes. As ACLs baseadas em filtros distinguem-se das outras na medida em que empregam uma comparação baseada em filtros, utilizando um filtro de objecto especificado, para fazer corresponder objectos específicos com o acesso efectivo aplicável aos mesmos.

Com a utilização de ACLs, os administradores podem restringir o acesso a partes diferentes do directório, a entradas de directório específicas e, com base no nome ou classe de acesso do atributo, aos atributos contidos nas entradas. Cada entrada do directório de LDAP tem um conjunto de ACIs associadas. Em conformidade com o modelo de LDAP, as informações de ACI e de entryOwner são representadas como pares atributo-valor. Além disso, a sintaxe de LDIF é utilizada para administrar estes valores. Os atributos são:

- aclEntry
- aclPropagate
- ibm-filterAclEntry
- ibm-filterAclInherit
- entryOwner
- ownerPropagate

Para obter informações sobre como trabalhar com ACLs, consulte "Gerir listas de controlo de acesso (ACLs)" na página 162. Para obter informações adicionais, consulte:

- "ACLs Filtradas"
- "A sintaxe do atributo de controlo de acesso" na página 53
- "AclEntry e ibm-filterAclEntry" na página 54
- "EntryOwner" na página 56
- "Propagação" na página 56
- "Avaliação do acesso" na página 57
- "Definir as ACIs e os proprietários de entradas" na página 59
- "Modificar as ACIs e os valores de proprietários de entradas" na página 60
- "Eliminar os valores de ACIs/proprietário de entrada" na página 62
- "Obter os valores de ACIs/proprietário de entrada" na página 63
- "Considerações sobre replicação de sub-árvores" na página 63

ACLs Filtradas

As ACLs baseadas em filtros empregam uma comparação baseada em filtros, utilizando um filtro de objecto especificado, para fazer corresponder objectos específicos com o acesso efectivo aplicável aos mesmos.

As ACLs baseadas em filtros propagam-se inerentemente para quaisquer objectos para os quais a comparação encontrou correspondência na sub-árvore associada. Por este motivo, o atributo aclPropagate, que é utilizado para parar a propagação de ACLs não filtradas, não se aplica às novas ACLs baseadas em filtros.

O comportamento assumido das ACLs baseadas em filtros é serem acumuladas, desde a entrada de conteúdo inferior, no sentido ascendente e paralelamente à cadeia de entrada anterior, até à entrada de conteúdo superior da DIT. O acesso efectivo é calculado como a união dos direitos de acesso concedidos, ou recusados, pelas entradas anteriores constituintes. Existe uma excepção a este comportamento. Por uma questão de compatibilidade com a função de replicação da sub-árvore, e para permitir um maior controlo administrativo, é utilizado um atributo de limite máximo como meio para parar a acumulação na entrada em que está contido.

É utilizado um novo conjunto de atributos de controlo de acesso especificamente para o suporte de ACLs baseadas em filtros, como alternativa à intercalação de características baseadas em filtros nas ACLs não baseadas em filtros existentes. Os atributos são:

- ibm-filterAclEntry
- ibm-filterAclInherit

O atributo ibm-filterAclEntry tem o mesmo formato que aclEntry, com a adição de um componente de filtro de objectos. O atributo de limite máximo associado é ibm-filterAclInherit. Por valor assumido, é definido como true (verdadeiro). Quando é definido como false (falso), termina a acumulação.

A sintaxe do atributo de controlo de acesso

Cada um destes atributos pode ser gerido com a notação de LDIF. A sintaxe para os novos atributos de ACLs baseadas em filtros é composta por versões modificadas dos atributos actuais de ACLs não baseadas em filtros. Segue-se uma definição da sintaxe dos atributos ACI e entryOwner com a utilização de baccus naur form (BNF).

```
<aclEntry> ::=  <sujeito> [ ":"  <direitos> ]

<aclPropagate> ::=  "true" | "false"
<ibm-filterAclEntry> ::=  <sujeito>  ":" <filtro de objecto>  [ ":"     <direitos> ]

<ibm-filterAclInherit> ::=  "true" | "false"
<entryOwner> ::=  <sujeito>

<ownerPropagate> ::= "true" | "false"

<sujeito> ::= <subjectDnType> ':' <subjectDn> |
                      <pseudoDn>

<subjectDnType> ::= "função" | "grupo" | "id-acesso"

<subjectDn> ::= <DN>

<DN> ::= nome exclusivo como descrito no RFC 2251, secção 4.1.3.

<pseudoDn> ::= "grupo:cn=todos" | "grupo:cn=autenticado" |
                       "id-acesso:cn=este"
<filtro objecto> ::= filtro de procura de cadeia como definido no RFC 2254, secção 4
                              (a correspondência extensível não é suportada).
<direitos> ::= <accessList> [":" <direitos> ]

<accessList> ::=  <objectAccess> | <attributeAccess> |
                          <attributeClassAccess>

<objectAccess> ::= "objecto:" [<acção> ":"]  <objectPermissions>

<acção> ::= "conceder" | "recusar"

<objectPermisssions> ::=  <objectPermission> [ <objectPermissions> ]

<objectPermission> ::= "a" | "d" |  ""

<attributeAccess> ::= "at." <attributeName> ":" [<acção> ":"]
                                    <attributePermissions>

<attributeName> ::= nome de attributeType como descrito no RFC 2251, secção 4.1.4.
                      (OID ou cadeia alfanumérica com alfabeto à esquerda,
                       "-" e ";" permitidos)

<attributePermissions> ::=  <attributePermission>
                                  [<attributePermissions>]

<attributePermission> ::=  "r" | "w" | "s" | "c" |  ""

<attributeClassAccess> ::= <classe> ":" [<acção> ":"]
                                    <attributePermissions>

<classe> ::= "normal" | "sensível" | "crítica"
```

AclEntry e ibm-filterAclEntry

Sujeito: Um sujeito (a entidade que pede o acesso para operar num objecto) consiste na combinação de um tipo de DN (Nome exclusivo) e um DN. Os tipos de DN válidos são: id-acesso, Grupo e Função.

O DN identifica um id-acesso, função ou grupo específicos. Por exemplo, um sujeito poderia ser id-acesso: cn=pessoaA, o=IBM ou grupo: cn=deptXYZ, o=IBM.

Como o delimitador de campo é o sinal de dois pontos (:), um DN que contenha dois pontos pode estar entre aspas (“”). Se um DN já contiver caracteres entre aspas, estes caracteres terão de ser separados por uma barra invertida (\).

Todos os grupos de directórios podem ser utilizados no controlo de acesso.

Nota: Qualquer grupo de objectclasses estruturais **AccessGroup**, **GroupOfNames**, **GroupofUniqueNames** ou **groupOfURLs**, ou as classes de objectos auxiliares**ibm-dynamicGroup** e **ibm-staticGroup**, podem ser utilizados para controlo de acesso.

Outro tipo de DN utilizado no modelo de controlo é acesso é a função. Embora funções e grupos sejam semelhantes em termos de implementação, eles diferem sob o ponto de vista conceptual. Quando é atribuída uma função a um utilizador, parte-se do princípio de que já foi configurada a autoridade necessária para o utilizador desempenhar a tarefa associada a essa função. Com a filiação de membros em grupos, não existem certezas das permissões concedidas (ou recusadas) por se ser membro desse grupo.

As funções são semelhantes aos grupos na medida em que são representadas no directório por um objecto. Além disso, as funções contêm um grupo de DNs. As funções que forem utilizadas no controlo de acesso têm de ter uma objectclass **AccessRole**.

Pseudo-DN: O directório de LDAP contém vários pseudo-DNs. Estes são utilizados para referir grandes números de DNs que, no momento da ligação, partilham uma característica comum em relação quer à operação que está a ser executada, quer ao objecto destino em que a operação está a ser executada.

Actualmente, estão definidos três pseudo-DNs:

grupo:cn=todos
: Refere-se a todos os sujeitos, incluindo os que não estão autenticados. Todos os utilizadores pertencem automaticamente a este grupo.

grupo:cn=autenticado
: Refere-se a qualquer DN que tenha sido autenticado para o directório. O método de autenticação não é tomado em consideração.

id-acesso:cn=este
: Refere-se ao DN de ligação que corresponde ao DN do objecto destino em que a operação está a ser executada.

Filtros de objectos: Este parâmetro só se aplica a ACLs filtradas. O filtro de procura de cadeia, tal como é definido no RFC 2254, é utilizado como o formato de filtro de objectos. Como o objecto destino já é conhecido, a cadeia não é utilizada para executar uma procura real. Em vez disso, é executada uma comparação baseada em filtros no objecto destino em questão para se determinar se um determinado conjunto de valores de ibm-filterAclEntry lhe é aplicável.

Direitos: Os direitos de acesso podem aplicar-se a um objecto inteiro ou a atributos do objecto. Os direitos de acesso de LDAP são discretos. Um direito não implica outro. Os direitos podem ser combinados para fornecer a lista de direitos pretendidos a seguir a um conjunto de regras que serão abordadas mais à frente. Os direitos podem ter um valor não especificado, que indica que não foram concedidos direitos de acesso ao sujeito no objecto destino. Os direitos consistem em três partes:

Acção:

Os valores definidos são **grant** ou **deny**. Se este campo não estiver presente, o valor assumido será definido como **grant**.

Permissão:

Existem seis operações base que podem ser executadas num objecto directório. Destas operações, retira-se o conjunto base de permissões de ACIs. Estas são: adicionar uma entrada, eliminar uma entrada, ler um valor de atributo, escrever um valor de atributo, procurar um atributo e comparar um valor de atributo.

As permissões de atributos possíveis são: ler (r), escrever (w), procurar (s) e comparar (c). Além disso, as permissões de objectos aplicam-se à entrada como um todo. Estas permissões são adicionar entradas descendentes (a) e eliminar esta entrada (d).

A tabela que se segue resume as permissões necessárias para executar cada uma das operações de LDAP.

Operação	Permissão Necessária
ldapadd	adição (no ascendente)
ldapdelete	eliminação (no objecto)
ldapmodify	escrita (nos atributos a serem modificados)
ldapsearch	• procura, leitura (nos atributos do RDN) • procura (nos atributos especificados no filtro de procura) • procura (nos atributos devolvidos só com nomes) • procura, leitura (nos atributos devolvidos com valores)
ldapmodrdn	escrita (nos atributos do RDN)
ldapcompare	comparação (no atributo comparado)

Nota: Para operações de procura, é necessário que o sujeito possua acesso de procura (s) para todos os atributos existentes no filtro de procura, ou não serão devolvidas entradas. Para as entradas devolvidas por uma procura, é necessário que o sujeito tenha acesso de procura (s) e leitura (r) para todos os atributos existentes no RDN das entradas devolvidas, ou estas entradas não serão devolvidas.

Destino do Acesso:

Estas permissões podem ser aplicadas a todo o objecto (adicionar entrada descendente, eliminar entrada), a um atributo individual da entrada ou a grupos de atributos (Classes de Acesso a Atributos), tal como é descrito abaixo.

Os atributos que requerem permissões semelhantes para acesso são agrupados em classes. Os atributos são definidos de acordo com as respectivas classes de atributo no ficheiro de esquemas do directório. Estas classes são discretas: o acesso a uma classe não implica o acesso a outra. As permissões são definidas tendo em consideração a classe de acesso de atributo como um todo. As permissões definidas numa classe de atributo específica aplicam-se a todos os atributos dentro dessa classe de acesso, a menos que sejam especificadas as permissões de acesso de atributo individuais.

A IBM define três classes de atributo que são utilizadas na avaliação do acesso a atributos de utilizador: **normal**, **sensitive** e **critical**. Por exemplo, o atributo **commonName** pertence à classe ″normal″ e o atributo ppsutilizador pertence à classe ″critical″. Os atributos definidos pelo utilizador pertencem à classe de acesso ″normal″, salvo indicação em contrário.

Também estão definidas duas outras classes: ″system″ e ″restricted″. Os atributos da classe sistema são:

- **creatorsName**

- **modifiersName**
- **createTimestamp**
- **modifyTimestamp**
- **ownerSource**
- **aclSource**

Estes são atributos mantidos pelo servidor de LDAP e são só de leitura para os utilizadores do directório. **OwnerSource** e **aclSource** estão descritas na secção Propagação (consulte "Propagação").

As classes restritas de atributos que definem o controlo de acesso são:

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**
- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

Todos os utilizadores têm acesso de leitura para os atributos restritos, mas apenas os **entryOwners** podem criar, modificar e eliminar estes atributos.

Nota: O atributo **ibm-effectiveAcl** é só de leitura.

EntryOwner

Os proprietários de entradas têm permissões totais para executar qualquer operação no objecto, independentemente da respectiva entrada de ACL. Adicionalmente, os proprietários de entradas são os únicos utilizadores autorizados a administrar as entradas de ACL desse objecto. EntryOwner é um sujeito de controlo de acesso e pode ser definido como indivíduos, grupos ou funções.

Nota: O administrador do directório é um dos proprietários de entradas de todos os objectos do directório por valor assumido, e a propriedade de entradas do administrador do directório não pode ser removida de nenhum objecto.

Propagação

As entradas nas quais tenha sido colocada uma aclEntry são consideradas como tendo uma **aclEntry** explícita. De forma semelhante, se o **entryOwner** tiver sido definido numa entrada específica, essa entrada terá um proprietário explícito. As duas não são combinadas, isto é, uma entrada com um proprietário explícito pode ou não ter uma **aclEntry** explícita e uma entrada com uma **aclEntry** explícita pode ter um proprietário explícito. Se um destes valores não estiver explicitamente presente numa entrada, o valor em falta será herdado de um nó anterior existente na árvore de directórios.

Cada **aclEntry** ou **entryOwner** explícito aplica-se à entrada onde está definido. Além disso, o valor pode aplicar-se a todos os descendentes que não tenham um valor explicitamente definido. Estes valores são considerados como propagados; os respectivos valores são propagados através da árvore de directórios. A propagação de um valor específico continua até ser atingido outro valor propagável.

Nota: As ACLs baseadas em filtros não se propagam da mesma forma que as ACLs não baseadas em filtros. Propagam-se a quaisquer objectos para os quais a comparação tenha encontrado correspondência na sub-árvore associada. Consulte "ACLs Filtradas" na página 52, para obter mais informações sobre as diferenças.

AclEntry e **entryOwner** podem ser definidos de forma a aplicarem-se apenas a uma entrada específica com o valor de propagação definido como ″false″, ou a uma entrada e à respectiva sub-árvore com o

valor de propagação definido como ″true″. Embora tanto **aclEntry**, como **entryOwner** possam ser propagados, a respectiva propagação não é ligada de nenhuma forma.

Os atributos **aclEntry** e **entryOwner** permitem valores múltiplos, mas os atributos de propagação (**aclPropagate** e **ownerPropagate**) apenas podem ter um único valor para todos os valores dos atributos**aclEntry** ou **entryOwner** existentes na mesma entrada.

Os atributos de sistema **aclSource** e **ownerSource** contêm o DN do nó efectivo a partir do qual a **aclEntry** ou o **entryOwner** são avaliados, respectivamente. Se não existir um nó deste tipo, será atribuído o valor **assumido**.

As definições de controlo de acesso efectivas de um objecto podem ser derivadas pela seguinte lógica:

- Se existir um conjunto de atributos de controlo de acesso explícitos no objecto, esse conjunto será a definição de controlo de acesso do objecto.
- Se não existirem atributos de controlo de acesso explicitamente definidos, atravesse a árvore de directórios no sentido ascendente até encontrar um nó anterior com um conjunto de atributos de controlo de acesso propagáveis.
- Se não for encontrado nenhum nó anterior, será concedido ao sujeito o acesso assumido descrito abaixo.

O administrador do directório é o proprietário da entrada. É concedido, ao pseudo-grupo cn=todos (todos os utilizadores), acesso de leitura, procura e comparação, para os atributos existentes na classe de acesso `normal`.

Avaliação do acesso

O acesso para uma operação específica é concedido ou recusado com base no DN de ligação do sujeito para essa operação no objecto destino. O processamento pára assim que o acesso possa ser determinado.

As verificações do acesso são executadas, primeiro, pela procura da definição efectiva de **entryOwnership** e **ACI**, pela procura das propriedades da entrada e, em seguida, pela avaliação dos valores de ACI do objecto.

As ACLs baseadas em filtros acumulam-se desde a entrada de conteúdo inferior, no sentido ascendente e paralelamente à cadeia de entrada anterior, até à entrada de conteúdo superior na DIT. O acesso efectivo é calculado como a união dos direitos de acesso concedidos, ou recusados, pelas entradas anteriores constituintes. O conjunto existente de regras de especificidade e combinação é utilizado para avaliar o acesso efectivo para ACLs baseadas em filtros.

Os atributos baseados e não baseados em filtros são mutuamente exclusivos numa única entrada de directório de conteúdo. Não é permitido colocar ambos os tipos de atributos na mesma entrada, sendo uma violação de restrição. Se esta condição for detectada, as operações associadas à criação de, ou as actualizações a uma entrada de directório falharão.

No cálculo do acesso efectivo, o primeiro tipo de ACL a ser detectado na cadeia anterior da entrada de objecto destino define o modo do cálculo. No modo baseado em filtros, as ACLs não baseadas em filtros são ignoradas no cálculo do acesso efectivo. Da mesma forma, no modo não baseado em filtros, as ACLs baseadas em filtros são ignoradas no cálculo do acesso efectivo.

Para limitar a acumulação de ACLs baseadas em filtros no cálculo do acesso efectivo, pode ser colocado um atributo **ibm-filterAclInherit** definido como um valor ″false″ numa entrada entre as ocorrências máxima e mínima de **ibm-filterAclEntry** numa determinada sub-árvore. Esta acção faz com que o subconjunto de atributos **ibm-filterAclEntry** acima do mesmo na cadeia anterior do objecto destino seja ignorado.

No modo de ACL baseada em filtros, se não se aplicar nenhuma ACL baseada em filtros, aplica-se a ACL assumida (é concedido acesso de leitura, procura e comparação a cn=todos para os atributos constantes na classe de acesso `normal`). Esta situação pode ocorrer quando a entrada que está a ser acedida não corresponde a nenhum dos filtros especificados nos valores **ibm-filterAclEntry**. O utilizador pode desejar especificar uma ACL de filtros assumida como a seguinte se não pretender que este controlo de acesso assumido se aplique:

```
ibm-filterAclEntry: grupo:cn=todos:(objectclass=*):
```

Este exemplo não concede acesso. Altere-o para fornecer o acesso que pretende que seja aplicado.

Por valor assumido, o administrador do directório e o servidor principal ou o servidor de unidade (para replicação) obtêm direitos de acesso totais para todos os objectos do directório, excepto acesso de escrita para os atributos de sistema. Outros **entryOwners** obtém direitos de acesso totais para os objectos dos quis são proprietários, excepto acesso de escrita para os atributos de sistema. Todos os utilizadores têm direitos de acesso para atributos de sistema e restritos. Estes direitos predefinidos não podem ser alterados.Se o sujeito solicitador tiver **entryOwnership**, o acesso é determinado pelas definições assumidas acima referidas e o processamento do acesso pára.

Se o sujeito solicitador não for um entryOwner, os valores de ACI para as entradas de objecto serão verificados. Os direitos de acesso, tal como estão definidos nas ACIs para o objecto destino, são calculados pelas regras de especificidade e combinação.

Regra de especificidade

As definições de aclEntry mais específicas são as que são utilizadas na avaliação de permissões concedidas/recusadas a um utilizador. Os níveis de especificidade são:

- ID-acesso é mais específico que grupo ou função. Os grupos e funções estão ao mesmo nível.
- Ao mesmo nível de **dnType**, as permissões de nível de atributo individuais são mais específicas que as permissões de nível de classe de atributo.
- Ao mesmo nível de atributo ou de classe de atributo, **deny** é mais específico que **grant**.

Regra de combinação

As permissões concedidas a sujeitos de igual especificidade são combinadas. Se não for possível determinar o acesso no mesmo nível de especificidade, serão utilizadas as definições de acesso de um nível menos específico. Se o acesso não for determinado após serem aplicadas todas as ACIs definidas, o acesso será recusado.

Nota: Após ser encontrada uma **aclEntry** de um nível de id-acesso correspondente na avaliação do acesso, as aclEntries de nível de grupo não são incluídas no cálculo do acesso. A excepção é que, se as**aclEntries** de um nível de id-acesso correspondente forem todas definidas sob cn=este, todas as **aclEntries** do nível de grupo correspondente também serão combinadas na avaliação.

Por outras palavras, na entrada de objecto, se uma entrada de ACI definida contiver um DN de sujeito de id-acesso correspondente ao DN de ligação, as permissões serão, primeiro, avaliadas com base nessa aclEntry. Sob o mesmo DN de sujeito, se forem definidas permissões de nível de atributo correspondentes, estas substituirão quaisquer permissões definidas sob as classes de atributo. Sob a mesma definição de nível de atributo ou de classe de atributo, se existirem permissões em conflito, as permissões recusadas substituem as permissões concedidas.

Nota: Uma permissão de valor nulo definida impede a inclusão de definições de permissões menos específicas.

Se ainda não for possível determinar o acesso e se todas as aclEntries correspondentes encontradas estiverem definidas sob "cn=este", a filiação de membros em grupos é avaliada. Se um utilizador pertencer a mais de um grupo, o utilizador receberá as permissões combinadas destes grupos. Além disso, o utilizador pertence automaticamente ao grupo cn=Todos e, possivelmente, ao grupo

cn=Autenticado, caso tenha executado uma ligação autenticada. Se estiverem definidas permissões para esses grupos, o utilizador receberá as permissões especificadas.

Nota: A filiação de membros em Grupo e Função é determinada no momento da ligação e dura até ocorrer outra ligação, ou até ser recebido um pedido de desligação. Os grupos e funções imbricados, ou seja, um grupo ou função definido como membro de outro grupo ou função, não são resolvidos na determinação da filiação de membros em grupos, nem na avaliação do acesso.

Por exemplo, suponha que o atributo1 está na classe de atributo sensível e que o utilizador cn=PessoaA, o=IBM, pertence ao grupo1 e ao grupo2 com as seguintes aclEntries definidas:

1. aclEntry: id-acesso: cn=Pessoa A, o=IBM: at.atributol:conceder:rsc:sensível:recusar:rsc
2. aclEntry: grupo: cn=grupo1,o=IBM:crítico:recusar:rwsc
3. aclEntry: grupo: cn=grupo2,o=IBM:crítico:conceder:r:normal:conceder:rsc

Este utilizador obtém:

- Acesso 'rsc' para o atributo1, (a partir de 1. A definição de nível de atributo substitui a definição de nível de classe de atributo).
- Não existe acesso a outros atributos de classe sensíveis no objecto destino (a partir de 1).
- Não são concedidos outros direitos (2 e 3 NÃO estão incluídos na avaliação do acesso).

Veja outro exemplo, com as seguintes aclEntries:

1. aclEntry: id-acesso: cn=este: sensível
2. aclEntry: grupo: cn=grupo1,o=IBM:sensível:conceder:rsc:normal:conceder:rsc

O utilizador:

- não tem acesso a atributos de classe sensíveis (a partir de 1. Valor nulo definido sob id-acesso impede a inclusão de permissões em atributos de classe sensíveis a partir do grupo1).
- tem acesso 'rsc' a atributos de classe normais (a partir de 2).

Definir as ACIs e os proprietários de entradas

Os dois exemplos seguintes mostram o estabelecimento de um subdomínio administrativo. O primeiro exemplo mostra um único utilizador a ser atribuído como entryOwner de todo o domínio. O segundo exemplo mostra um grupo atribuído como entryOwner.

```
entryOwner: id-acesso:cn=Pessoa A,o=IBM
ownerPropagate: true

entryOwner: grupo:cn=Proprietários de Sistemas, o=IBM
ownerPropagate: true
```

O exemplo seguinte mostra como estão a ser concedidas, a um id-acesso"cn=Pessoa 1, o=IBM", permissões de leitura, procura e comparação relativas ao atributo1. A permissão aplica-se a qualquer nó de toda a sub-árvore no, ou abaixo do nó que contém estas ACIs, e que corresponda ao filtro de comparação "(objectclass=groupOfNames)". A acumulação de atributos ibm-filteraclentry correspondentes em quaisquer nós anteriores foi terminada nesta entrada através da definição do atributo ibm-filterAclInherit como "false".

```
ibm-filterAclEntry: id-acesso:cn=Pessoa 1,o=IBM:(objectclass=groupOfNames):
                    at.atributo1:conceder:rsc

ibm-filterAclInherit: false
```

O exemplo seguinte mostra como estão a ser concedidas, ao grupo "cn=Dept XYZ, o=IBM", permissões de leitura, procura e comparação relativas ao atributo1. A permissão aplica-se a toda a sub-árvore abaixo do nó que contém estas ACIs.

```
aclEntry: grupo:cn=Dept XYZ,o=IBM:at.atributo1:conceder:rsc
aclPropagate: true
```

O exemplo seguinte mostra como está a ser concedida, à função ″cn=Admins Sistema,o=IBM″, permissão para adicionar objectos abaixo deste nó e permissões de leitura, procura e comparação relativas ao atributo1 e à classe de atributo crítica. A permissão só se aplica ao nó que contém estas ACIs.

```
aclEntry: função:cn=Admins Sistema,o=IBM:objecto:conceder:a:at.
         atributo2:conceder:rsc:crítico:conceder:rsc
aclPropagate: false
```

Modificar as ACIs e os valores de proprietários de entradas

Modify-replace

Modify-replace funciona da mesma forma que todos os outros atributos. Se o valor do atributo não existir, crie-o. Se o valor do atributo existir, substitua-o.

Considere as seguintes ACIs para uma entrada:

```
aclEntry: grupo:cn=Dept ABC,o=IBM:normal:conceder:rsc
aclPropagate: true
```

execute a seguinte alteração:

```
dn: cn=uma entrada
changetype: modify
replace: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

As ACIs resultantes são:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclPropagate: true
```

Os valores de ACIs para o Dept ABC perdem-se com a substituição.

Considere as seguintes ACIs para uma entrada:

```
ibm-filterAclEntry: grupo:cn=Dept ABC,o=IBM:(cn=Gestor do ABC):normal
                  :conceder:rsc
ibm-filterAclInherit: true
```

execute as seguintes alterações:

```
dn: cn=uma entrada
changetype: modify
replace: ibm-filterAclEntry
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):normal
                  :conceder:rsc
dn: cn=uma entrada
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

As ACIs resultantes são:

```
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):normal
                  :conceder:rsc
ibm-filterAclInherit: false
```

Os valores de ACIs para o Dept ABC perdem-se com a substituição.

Modify-add

Durante uma operação ldapmodify-add, se não existirem as ACIs ou o entryOwner, serão criadas as ACIs ou entryOwner com os valores específicos. Se existirem as ACIs ou o entryOwner, adicione os valores especificados às ACIs ou entryOwner fornecidos. Por exemplo, considere as ACIs:

```
 aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
```

com uma modificação:

```
dn: cn=uma entrada
changetype: modify
add: aclEntry
aclEntry: grupo:cn=Dept ABC,o=IBM:at.atributo1:conceder:rsc
```

resultaria na seguinte aclEntry com vários valores:

```
aclEntry: group:cn=Dept XYZ,o=IBM:normal:grant:rsc
aclEntry: grupo:cn=Dept ABC,o=IBM:at.atributo1:conceder:rsc
```

Por exemplo, considere as ACIs:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :conceder:rsc
```

com uma modificação:

```
dn: cn=uma entrada
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: grupo:cn=Dept ABC,o=IBM:(cn=Gestor do ABC)
                  :at.atributo1:conceder:rsc
```

resultaria na seguinte aclEntry com vários valores:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :conceder:rsc
ibm-filterAclEntry: grupo:cn=Dept ABC,o=IBM:(cn=Gestor do ABC):at.atributo1
                  :conceder:rsc
```

As permissões sob o mesmo atributo ou classe de atributo são consideradas como os blocos de construção base e as acções são consideradas como os qualificadores. Se o mesmo valor de permissão for adicionado mais do que uma vez, só será armazenado um valor. Se o mesmo valor de permissão for adicionado mais do que uma vez com valores de acção diferentes, será utilizado o último valor de acção. Se o campo de permissão resultante estiver vazio (""), este valor de permissão será definido como nulo e o valor de acção será definido como **conceder**.

Por exemplo, considere as seguintes ACIs:

```
 aclEntry: grupo:cn=Dept XYZ,O=IBM:normal:conceder:rsc
```

com uma modificação:

```
dn: cn=uma entrada
changetype: modify
add: aclEntry
aclEntry: grupo:cn=Dept XYZ,o=IBM:normal:recusar:r:crítico:recusar::sensível
                  :conceder:r
```

resulta na seguinte aclEntry:

```
aclEntry: grupo:cn=Dept XYZ,O=IBM:normal:conceder:sc:normal:recusar:r:crítico
        :conceder::sensível:conceder:r
```

Por exemplo, considere as seguintes ACIs:

```
Ibm-filterAclEntry: grupo:cn=Dept XYZ,O=IBM:(cn=Gestor do XYZ):normal
                  :conceder:rsc
```

com uma modificação:

```
dn: cn=uma entrada
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):normal
                  :recusar:r:crítico:recusar::sensível:conceder:r
```

resulta na seguinte aclEntry:

```
ibm-filterAclEntry: group:cn=Dept XYZ,O=IBM:(cn=Manager XYZ):normal
                  :conceder:sc:normal:recusar:r:crítico:conceder::sensível
                  :conceder:r
```

Modify-delete

Para eliminar um valor de ACIs específico, utilize a sintaxe regular ldapmodify-delete.

Considere as seguintes ACIs:

```
aclEntry: grupo:cn=Dept XYZ,o=IBM:objecto:conceder:ad
aclEntry: grupo:cn=Dept XYZ,o=IBM:normal:conceder:rwsc

dn: cn = uma entrada
changetype: modify
delete: aclEntry aclEntry: grupo:cn=Dept XYZ,o=IBM:objecto:conceder:ad
```

resulta nas seguintes ACIs que permanecem no servidor:

```
aclEntry: grupo:cn=Dept XYZ,o=IBM:normal:conceder:rwsc
```

Considere as seguintes ACIs:

```
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):object
                  :conceder:ad
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):normal
                  :conceder:rwsc
dn: cn = uma entrada
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):object
                  :conceder:ad
```

resulta nas seguintes ACIs que permanecem no servidor:

```
ibm-filterAclEntry: grupo:cn=Dept XYZ,o=IBM:(cn=Gestor do XYZ):normal
                  :conceder:rwsc
```

A eliminação de um valor de ACIs ou entryOwner que não exista resulta em ACIs ou num entryOwner não alterados e num código de retorno a especificar que o valor de atributo não existe.

Eliminar os valores de ACIs/proprietário de entrada

Com a operação ldapmodify-delete, o entryOwner pode ser eliminado através da especificação de

```
dn: cn = uma entrada
changetype: modify
delete: entryOwner
```

Neste caso, a entrada não teria um entryOwner explícito. O ownerPropagate também é removido automaticamente. Esta entrada herdaria o respectivo entryOwner do nó anterior na árvore de directórios que segue a regra de propagação.

Pode ser executada a mesma operação para eliminar completamente a aclEntry:

```
dn: cn = uma entrada
changetype: modify
delete: aclEntry
```

Eliminar o último valor de ACIs ou de entryOwner de uma entrada não é o mesmo que eliminar as ACIs ou o entryOwner. É possível uma entrada conter ACIs ou um entryOwner sem valores. Neste caso, não é devolvido nenhum valor ao cliente quando consultar as ACIs ou o entryOwner e a definição propagar-se-á pelos nós descendentes até ser substituída. Para evitar entradas complicadas de acesso difícil, o administrador do directório dispõe de acesso total para qualquer entrada mesmo que esta tenha um valor de ACIs ou entryOwner nulo.

Obter os valores de ACIs/proprietário de entrada

Os valores de ACIs ou entryOwner efectivos podem ser obtidos pela simples especificação dos atributos de ACL ou entryOwner pretendidos numa procura como, por exemplo,

```
ldapsearch -b "cn=objecto A, o=ibm" -s base "objectclass=*"
    aclentry aclpropagate aclsource entryowner ownerpropagate ownersource
    ibm-filterAclEntry ibm-filterAclInherit ibm-effectiveAcl
```

devolve todas as informações sobre ACLs ou entryOwners que são utilizadas na avaliação do acesso no objecto A. Note que os valores devolvidos podem ter mudado desde que foram definidos pela primeira vez. Os valores são o equivalente do formato original.

A procura apenas no atributo ibm-filterAclEntry só devolve os valores específico da entrada de conteúdo.

É utilizado um atributo operacional só de leitura, ibm-effectiveAcl, para mostrar o acesso efectivo acumulado. Um pedido de procura de ibm-effectiveAcl devolve o acesso efectivo que se aplica ao objecto destino, com base em: ACLs sem ser de filtros ou ACLs de filtros, dependendo do modo como foram distribuídas na DIT.

Uma vez que as ACLs baseadas em filtros podem ser provenientes de várias origens anteriores, uma procura no atributo aclSource produz uma lista das origens associadas.

Considerações sobre replicação de sub-árvores

Para que o acesso baseado em filtros seja incluído na replicação de sub-árvores, quaisquer atributos ibm-filterAclEntry terão de residir na, ou abaixo da entrada ibm-replicationContext associada.

Uma vez que o acesso efectivo não pode ser acumulado a partir de uma entrada anterior acima de uma sub-árvore replicada, o atributo ibm-filterAclInherit tem de ser definido como **false** e residir na entrada ibm-replicationContext associada.

Propriedade de objectos do directório de LDAP

Cada objecto existente no directório de LDAP tem, pelo menos, um proprietário. Os proprietários de objectos têm poder para os eliminar. Os proprietários e o administrador do servidor são os únicos utilizadores que podem alterar as propriedades e os atributos da lista de controlo de acesso (ACL) de um objecto. A propriedade de objectos pode ser herdada ou explícita. Isto é, para atribuir propriedade pode efectuar um dos seguintes procedimentos:

- Configurar explicitamente a propriedade de um objecto específico.
- Especificar que os objectos herdem os proprietários de objectos mais acima na hierarquia de directórios de LDAP.

O Directory Server permite especificar vários proprietários do mesmo objecto. Também pode especificar que um objecto é proprietário de si próprio. Para o fazer, tem de incluir o DN especial `cn=este` na lista de proprietários de objectos. Por exemplo, suponha que o objecto `cn=A` tem o proprietário `cn=este`. Qualquer utilizador terá acesso de proprietário ao objecto `cn=A` se este se ligar ao servidor como `cn=A`.

Para obter informações sobre como trabalhar com características de propriedade, consulte “Gerir entradas de directório” na página 145.

Política de palavras-passe

Com a utilização de servidores de LDAP para autenticação, é importante que o servidor de LDAP suporte políticas relacionadas com a expiração de palavras-passe, tentativas de início de sessão falhadas e regras de palavras-passe. O Directory Server fornece suporte configurável para estes três tipos de políticas. Esta política aplica-se a todas as entradas de directório que tenham um atributo userPassword. Não pode definir uma política para um conjunto de utilizadores e políticas diferentes para outros conjuntos de utilizadores. O Directory Server também fornece um mecanismo para informar os clientes acerca das condições relacionadas com a política de palavras-passe (a palavra-passe expira após três dias),

além de um conjunto de atributos operacionais que um administrador pode utilizar para procurar, por exemplo, utilizadores com palavras-passe expiradas ou contas bloqueadas.

Para obter mais informações sobre como trabalhar com propriedades da política de palavras-passe, consulte "Definir política de palavras-passe" na página 108.

Configuração

Pode configurar o comportamento do servidor relativamente às palavras-passe nas seguintes áreas:

- Um comutador global de ″ligar/desligar″ para activar ou desactivar a política de palavras-passe
- Regras para alterar palavras-passe, incluindo:
  - Os utilizadores podem alterar as suas próprias palavras-passe. Note que esta política se aplica em adição a qualquer controlo de acesso. Ou seja, o controlo de acesso tem de conceder a um utilizador autoridade para alterar o atributo userPassword e a política de palavras-passe deve permitir que os utilizadores alterem as suas próprias palavras-passe. Se esta política for desactivada, os utilizadores não poderão alterar as suas próprias palavras-passe. Só um administrador ou outro utilizador com autoridade para alterar o atributo userPassword poderá alterar a palavra-passe para uma entrada.
  - As palavras-passe têm de ser alteradas após a reposição. Se esta política for activada, quando uma palavra-passe é alterada por outro utilizador, ela é marcada como resposta e terá de ser alterada pelo utilizador antes de este poder executar outras operações no directório. Um pedido de ligação com uma palavra-passe reposta será bem sucedido. Para ser notificada de que a palavra-passe tem de ser reposta, a aplicação tem de ter conhecimento da política de palavras-passe.
  - Os utilizadores têm de enviar a palavra-passe antiga quando alterarem a palavra-passe. Se esta política for activada, uma palavra-passe só poderá ser alterada por um pedido de modificação que inclua tanto a eliminação do atributo userPassword (com o valor antigo), como a adição do novo valor de userPassword. Esta acção assegura que apenas um utilizador que conheça a palavra-passe a pode alterar. O administrador, ou outros utilizadores autorizados a alterar o atributo userPassword, podem sempre definir a palavra-passe.
- Regras para a expiração de palavras-passe incluindo:
  - As palavras-passe nunca expiram, ou as palavras-passe expiram após um período de tempo configurável, depois de terem sido alteradas pela última vez.
  - Não avisar os utilizadores quando uma palavra-passe expira ou avisar os utilizadores um período de tempo configurável antes de a respectiva palavra-passe expirar. Para ser notificada de que se aproxima o momento da expiração da palavra-passe, a aplicação tem de ter conhecimento da política de palavras-passe.
  - Permitir um número configurável de inícios de sessão de tolerância após a expiração da palavra-passe do utilizador. Uma aplicação com conhecimento da política de palavras-passe será notificada do número de inícios de sessão de tolerância restantes. Se não forem permitidos inícios de sessão de tolerância, um utilizador não poderá autenticar-se ou alterar a respectiva palavra-passe depois de ter expirado.
- Regras para validação da palavra-passe, incluindo:
  - Um tamanho configurável do histórico de palavras-passe, que pede ao servidor para manter um histórico das últimas N palavras-passe e rejeita as palavras-passe anteriormente utilizadas.
  - Verificação da sintaxe das palavras-passe, incluindo uma definição do modo como o servidor se deverá comportar quando as palavras-passe estão incorrectas. Esta definição determina se o servidor deverá ou não ignorar a política com uma das seguintes condições:
    - O servidor estiver a armazenar palavras-passe incorrectas.
    - Um cliente apresentar uma palavra-passe incorrecta ao servidor (o que pode acontece durante a transferência de entradas entre servidores através de um ficheiro LDIF, caso o servidor origem armazene palavras-passe incorrectas).

    Em qualquer um destes casos, o servidor pode não conseguir aplicar todas as regras de sintaxe. São suportadas as seguintes regras de sintaxe: comprimento mínimo, número mínimo de caracteres

alfabéticos, número mínimo de caracteres numéricos ou especiais, número de caracteres repetidos e número de caracteres em que a palavra-passe deve diferir da palavra-passe anterior.

- Regras para inícios de sessão falhados, incluindo:
  - Um período de tempo mínimo permitido entre alterações de palavras-passe, que impede que os utilizadores mudem repetidamente de palavra-passe, para voltarem à respectiva palavra-passe original.
  - Um número máximo de tentativas de início de sessão falhadas antes de a conta ser bloqueada.
  - Uma duração configurável para o bloqueio da palavra-passe. Decorrido este período, pode ser utilizada uma conta anteriormente bloqueada. Esta acção pode ajudar a impedir uma tentativa de um intruso de determinar uma palavra-passe, auxiliando, ao mesmo tempo, um utilizador que possa ter-se esquecido da palavra-passe.
  - Um tempo configurável durante o qual o servidor mantém o controlo das tentativas de início de sessão falhadas. Se o número máximo de tentativas de início de sessão falhadas ocorrer dentro deste período, a conta será bloqueada. Assim que este período de tempo expirar, o servidor elimina as informações sobre tentativas de início de sessão falhadas para esta conta.

As definições de políticas de palavra-passe para o Directory Server estão armazenadas no objecto "cn=políticappasse", que se assemelha ao seguinte:

```
cn=políticappasse objectclass=container objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=superior
cn=Políticappasse
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

Aplicações com conhecimento da política de palavras-passe

O suporte de política de palavras-passe do Directory Server para iSeries inclui um conjunto de controlos de LDAP que podem ser utilizados por uma aplicação com conhecimento da política de palavras-passe para receber uma notificação das condições adicionais relacionadas com a política de palavras-passe.

Uma aplicação pode ser informada das seguintes condições de alerta:

- Tempo restante antes da expiração da palavra-passe
- Número de inícios de sessão de tolerância após a expiração da palavra-passe

Uma aplicação também pode ser informada das seguintes condições de erro:

- A palavra-passe expirou
- A conta está bloqueada
- A palavra-passe foi reposta e tem de ser alterada

- O utilizador não está autorizado a alterar a respectiva palavra-passe
- A palavra-passe antiga tem de ser fornecida durante a alteração da palavra-passe
- A nova palavra-passe viola as regras de sintaxe de palavras-passe
- A nova palavra-passe é demasiado curta
- A alteração da palavra-passe é demasiado recente
- A nova palavra-passe encontra-se no histórico

São utilizados dois controlos. Um controlo de pedido de palavra-passe é utilizado para informar o servidor de que a aplicação pretende ser informada das condições relacionadas com a política de palavras-passe. Este controlo tem de ser especificado pela aplicação em todas as operações às quais se destina, que são, normalmente, o pedido de ligação inicial e quaisquer pedidos de alteração de palavras-passe. Se o controlo de pedidos de políticas de palavras-passe estiver presente, será devolvido pelo servidor um controlo de resposta de política de palavras-passe quando existir qualquer uma das condições de erro anteriores.

As APIs de cliente do Directory Server incluem um conjunto de APIs que podem ser utilizadas por aplicações C para funcionar com estes controlos. Estas APIs são:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

Para as aplicações que não utilizem estas APIs, os controlos estão definidos abaixo. Tem de utilizar as capacidades fornecidas pelas APIs de cliente de LDAP que estão a ser utilizadas para processar os controlos. Por exemplo, a Interface de Nomenclatura e Directórios de Java (JNDI - Java Naming and Directory Interface) dispõe de suporte incorporado para determinados controlos conhecidos, além de fornecer uma estrutura para suporte de controlos não reconhecidos pela JNDI.

Controlo de Pedidos da Política de Palavras-passe

```
Nome do controlo: 1.3.6.1.4.1.42.2.27.8.5.1
Nível de gravidade do controlo: FALSE
Valor do controlo: Nenhum
```

Controlo de Respostas da Política de Palavras-passe

```
Nome do controlo: 1.3.6.1.4.1.42.2.27.8.5.1 (igual ao controlo de pedidos)
Nível de gravidade do controlo: FALSE
Valor do controlo: Um valor codificado BER definido como ASN.1, do seguinte modo:
  PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
  timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
  graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error  [1] ENUMERATED OPTIONAL {
  passwordExpired   (0),
  accountLocked    (1),
  changeAfterReset   (2),
  passwordModNotAllowed (3),
  mustSupplyOldPassword (4),
  invalidPasswordSyntax (5),
  passwordTooShort   (6),
  passwordTooYoung   (7),
  passwordInHistory   (8) } }
```

Tal como outros elementos do protocolo de LDAP, a codificação BER utiliza a marcação implícita.

Atributos operacionais da política de palavras-passe

O Directory Server mantém um conjunto de atributos operacionais para cada entrada que tenha um atributo userPassword. Estes atributos podem ser procurados por utilizadores autorizados, usados em filtros de procura ou devolvidos pelo pedido de procura. Estes atributos são:

- pwdChangedTime - Um atributo GeneralizedTime que contém a hora a que a palavra-passe foi alterada pela última vez.
- pwdAccountLockedTime - Um atributo GeneralizedTime que contém a hora a que a conta foi bloqueada. Se a conta não tiver sido bloqueada, este atributo não estará presente.
- pwdExpirationWarned - Um atributo GeneralizedTime que contém a hora a que o aviso de expiração de palavra-passe foi enviado pela primeira vez ao cliente.
- pwdFailureTime - Um atributo GeneralizedTime com vários valores que contém as horas de inícios de sessão falhados consecutivos anteriores. Se o último início de sessão tiver tido êxito, este atributo não estará presente.
- pwdGraceUseTime - Um atributo GeneralizedTime com vários valores que contém as horas dos inícios de sessão de tolerância anteriores.
- pwdReset - Um atributo Booleano que contém o valor TRUE se a palavra-passe tiver sido reposta e que tem de ser alterado pelo utilizador.

Replicação da Política de Palavras-passe

As informações sobre a política de palavras-passe é replicada pelos servidores fornecedores para os consumidores. As alterações à entrada cn=políticappasse são replicadas como alterações globais, tal como as alterações ao esquema. As informações sobre o estado da política de palavras-passe para entradas individuais também são replicadas, de modo a que, por exemplo, se uma entrada estiver bloqueada num servidor fornecedor, essa acção será replicada para quaisquer consumidores. No entanto, as alterações ao estado da política de palavras-passe numa réplica só de leitura não são replicadas para outros servidores.

Autenticação

O controlo de acesso no Directory Server baseia-se no nome exclusivo (DN) associado a uma determinada ligação. Esse DN é estabelecido como resultado de uma ligação ao (início de sessão no) Directory Server.

Quando o Directory Server é configurado pela primeira vez, podem ser utilizadas as seguintes identidades para autenticação no servidor:

- anónima
- o administrador do directório (cn=administrador por valor assumido)
- um perfil de utilizador projectado do i5/OS (consulte o tópico “Sistema origem de projecção do sistema operativo” na página 70)

É recomendável criar utilizadores adicionais aos quais possa ser concedida autoridade para gerir partes diferentes do directório sem ser necessário partilhar a identidade do administrador do directório.

Numa perspectiva de LDAP, existem duas estruturas para autenticação no LDAP:

- Ligação simples, na qual uma aplicação fornece um DN e a palavra-passe de texto normal para esse DN.
- Simple Authentication and Security Layer (SASL), que fornece vários métodos de autenticação adicionais, incluindo CRAM-MD5, EXTERNAL, GSSAPI e OS400-PRFTKN.

Ligação simples (e CRAM-MD5)

Para utilizar uma ligação simples, o cliente tem de fornecer o DN de uma entrada de LDAP existente que corresponda ao atributo userPassword para essa entrada. Por exemplo, pode criar uma entrada para João Silva do seguinte modo:

```
sample.ldif:
dn: cn=João Silva,cn=utilizadores,o=empresa,c=po
objectclass: inetorgperson
cn: João Silva
```

```
        sn: silva
        userPassword: minhapalavrapasse

ldapadd -D cn=administrador -w secreta -f sample.ldif
```

Agora, pode utilizar o DN ″cn=João Silva,cn=utilizadores,o=empresa,c=po″ no controlo de acesso ou torná-lo membro de um grupo utilizado no controlo de acesso.

Várias objectclasses predefinidas permitem a especificação de userPassword, incluindo (mas não se limitando a): person, organizationalperson, inetorgperson, organization, organizationalunit e outras.

As palavras-passe do Directory Server são sensíveis a maiúsculas e minúsculas. Se criar uma entrada com o valor `secreta` de userPassword, uma ligação que especifique a palavra-passe `SECRETA` falhará.

Ao utilizar uma ligação simples, o cliente envia a palavra-passe de texto normal para o servidor como parte do pedido de ligação. Isto expõe a palavra-passe a um risco de segurança ao nível do protocolo. Pode ser utilizada uma ligação de SSL para proteger a palavra-passe (todas as informações enviadas através de uma ligação de SSL são codificadas). Também pode ser utilizado o método CRAM-MD5 SASL.

O método CRAM-MD5 requer que o servidor tenha acesso à palavra-passe de texto normal (a protecção por palavra-passe é definida como `nenhuma`, o que significa realmente que a palavra-passe é armazenada no formato descodificado e devolvida nas procuras como texto normal). O cliente envia o DN para o servidor. O servidor obtém o valor de userPassword para a entrada e gera uma cadeia aleatória. A cadeia aleatória é enviada para o cliente. Tanto o cliente, como o servidor decifram a cadeia aleatória utilizando a palavra-passe como chave e o cliente envia o resultado para o servidor. Se as duas cadeias aleatórias decifradas corresponderem, o pedido de ligação terá êxito e a palavra-passe nunca é enviada para o servidor.

Para poder utilizar CRAM-MD5, o servidor terá de ser configurado de modo a que a protecção por palavra-passe seja Nenhuma, e o valor de sistema QRETSVRSEC (Reter dados de segurança do servidor) tem de ser 1 (Reter dados).

Ligação como um utilizador publicado

O Directory Server fornece um meio de ter uma entrada de LDAP cuja palavra-passe é a mesma de um perfil de utilizador do i5/OS no mesmo sistema. Para tal, a entrada:

- tem de ter um atributo de ID do utilizador, cujo valor seja o nome de um perfil de utilizador do i5/OS
- não pode ter um atributo userPassword

Quando o servidor recebe um pedido de ligação para uma entrada que tenha um valor de ID do utilizador, mas que não tenha nenhuma userPassword, o servidor chama a segurança do i5/OS para determinar se o ID do utilizador é um nome de perfil de utilizador válido e se a palavra-passe especificada está correcta para esse perfil de utilizador. Uma entrada deste tipo é denominada ″utilizador publicado″, em referência à publicação do directório de distribuição do sistema (SDD) no LDAP, que cria estas entradas.

Ligação como um utilizador projectado

Uma entrada de LDAP que represente um perfil de utilizador do i5/OS é referida como um utilizador projectado. Pode utilizar o DN de um utilizador projectado juntamente com a palavra-passe correcta para esse perfil de utilizador numa ligação simples. Por exemplo, o DN para o utilizador JSILVA no sistema meu-sistema.empresa.com seria:

```
os400-profile=JSILVA,cn=contas,os400-sys=meu-sistema.empresa.com
```

Ligação SASL EXTERNAL

Se for utilizada uma ligação de SSL ou TLS com a autenticação de cliente (por exemplo, caso o cliente tenha um certificado privado), pode ser utilizado o método SASL EXTERNAL. Este método indica ao servidor que deverá obter a identidade do cliente através de uma origem externa, neste caso, da ligação de SSL. O servidor obtém a parte pública do certificado do cliente (enviado para o servidor como parte do estabelecimento da ligação de SSL) e extrai o DN do sujeito. Esse DN é atribuído pelo servidor de LDAP à ligação.

Por exemplo, considere um certificado atribuído a:

```
nome comum: João Silva
unidade organizacional: Engenharia
organização: EMPRESA
localidade: Almada
distrito: Setúbal
país: PO
```

O DN do sujeito seria:

```
cn=João Silva,ou=Engenharia,o=empresa,l=Almada,st=Setúbal,c=PO
```

Note que os elementos cn, ou, o, l, st e c são utilizados pela ordem apresentada para gerar o DN do sujeito.

Ligação de SASL GSSAPI

O mecanismo de ligação de SASL GSSAPI é utilizado para autenticação no servidor com a utilização de um bilhete de Kerberos. Este mecanismo é útil quando o cliente tiver executado um KINIT ou outra forma de autenticação de Kerberos (por exemplo, um início de sessão no domínio do Windows 2000). Neste caso, o servidor valida o bilhete do cliente e, em seguida, obtém os nomes de director e do domínio de Kerberos; por exemplo, o director jsilva no domínio empresa.com, normalmente, expresso como jsilva@empresa.com. O servidor pode ser configurado para fazer corresponder esta identidade com um DN de um de dois modos:

- Gerar um pseudo-DN no formato ibm-kn=jsilva@empresa.com
- Procurar uma entrada que tenha a classe auxiliar ibm-securityidentities e um valor altsecurityidenties no formato KERBEROS:<director>@<domínio>.

Uma entrada a ser utilizada para jsilva@empresa.com pode ser semelhante a:

```
dn: cn=João Silva,cn=utilizadores,o=empresa,c=po
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: João Silva
sn: Silva
altsecurityidentities: kerberos:jsilva@empresa.com
```

Para obter informações sobre como activar a autenticação de Kerberos, consulte “Activar a autenticação de Kerberos no Directory Server” na página 133.

Ligação de OS400-PRFTKN

O mecanismo de ligação de OS400-PRFTKN SASL é utilizado para autenticação no servidor com a utilização de um sinal de perfil (consulte a API Gerar Sinal de Perfil). Quando este mecanismo é utilizado, o servidor valida o sinal do perfil e associa o DN do perfil de utilizador projectado à ligação (por exemplo, os400-profile=JSILVA,cn=contas,os400-system=meu-as400.minhaempresa.com). Se a aplicação já tiver um sinal de perfil, este mecanismo evita a necessidade de obter o nome do perfil e palavra-passe do utilizador para executar uma ligação simples. Para utilizar este mecanismo, use a API ldap_sasl_bind s, especificando um DN nulo, `OS400-PRFTKN` para o mecanismo e um ″berval″ (dados binários que são codificados com a utilização de regras de codificação básicas) que contenha o sinal de perfil de 32 bytes para as credenciais.

LDAP como um serviço de autenticação

O LDAP é normalmente utilizado para fornecer um serviço de autenticação. Pode configurar um servidor da Web para autenticação no LDAP. Ao configurar vários servidores da Web (ou outras aplicações) para autenticação no LDAP, pode estabelecer um único registo de utilizadores para essas aplicações, em vez de definir utilizadores repetidamente para cada aplicação ou ocorrência do servidor da Web.

Como funciona este método? Em poucas palavras, o servidor da Web pede um nome de utilizador e palavra-passe ao utilizador. O servidor da Web recebe estas informações e, em seguida, efectua uma procura no directório de LDAP um entrada com esse nome de utilizador (por exemplo, pode configurar o servidor da Web para fazer corresponder o nome do utilizador com os atributos 'uid' ou 'mail' de LDAP). Se este encontrar exactamente uma entrada, o servidor da Web enviará um pedido de ligação para o servidor utilizando o DN da entrada que acabou de encontrar e a palavra-passe de utilizador fornecida. Se a ligação tiver êxito, o utilizador é autenticado nesta altura. Podem ser utilizadas ligações de SSL para proteger as informações de palavra-passe de riscos de segurança ao nível do protocolo.

O servidor da Web também pode controlar a localização do DN que foi utilizado de modo a que uma determinada aplicação possa utilizar esse DN, por exemplo, armazenando dados de personalização nessa entrada, noutra entrada associada ou numa base de dados separada com a utilização do DN como chave para encontrar as informações.

Uma alternativa comum à utilização de um pedido de ligação é utilizar a operação comparar do LDAP. Por exemplo, `ldap_compare(ldap_session, dn, "userPassword", enteredPassword)`. Isto permite a utilização pela aplicação de uma única sessão de LDAP, em vez de iniciar e terminar sessões para cada pedido de autenticação.

Sistema origem de projecção do sistema operativo

O programa emissor projectado do sistema tem a capacidade para mapear objectos do i5/OS como entradas na árvore de directórios acessível por LDAP. Os objectos projectados são representações de LDAP de objectos do i5/OS em vez de entradas reais armazenadas na base de dados do servidor de LDAP. Os perfis de utilizador são os únicos objectos a ser mapeados ou projectados como entradas na árvore de directórios. O mapeamento de objectos do perfil de utilizador é denominada programa emissor projectado pelo utilizador do i5/OS.

As operações de LDAP são mapeadas para os objectos subjacentes do i5/OS e executam funções do sistema operativo para poderem aceder a estes objectos. Todas as operações de LDAP executadas nos perfis de utilizador são executadas sob a autoridade do perfil de utilizador associado à ligação do cliente.

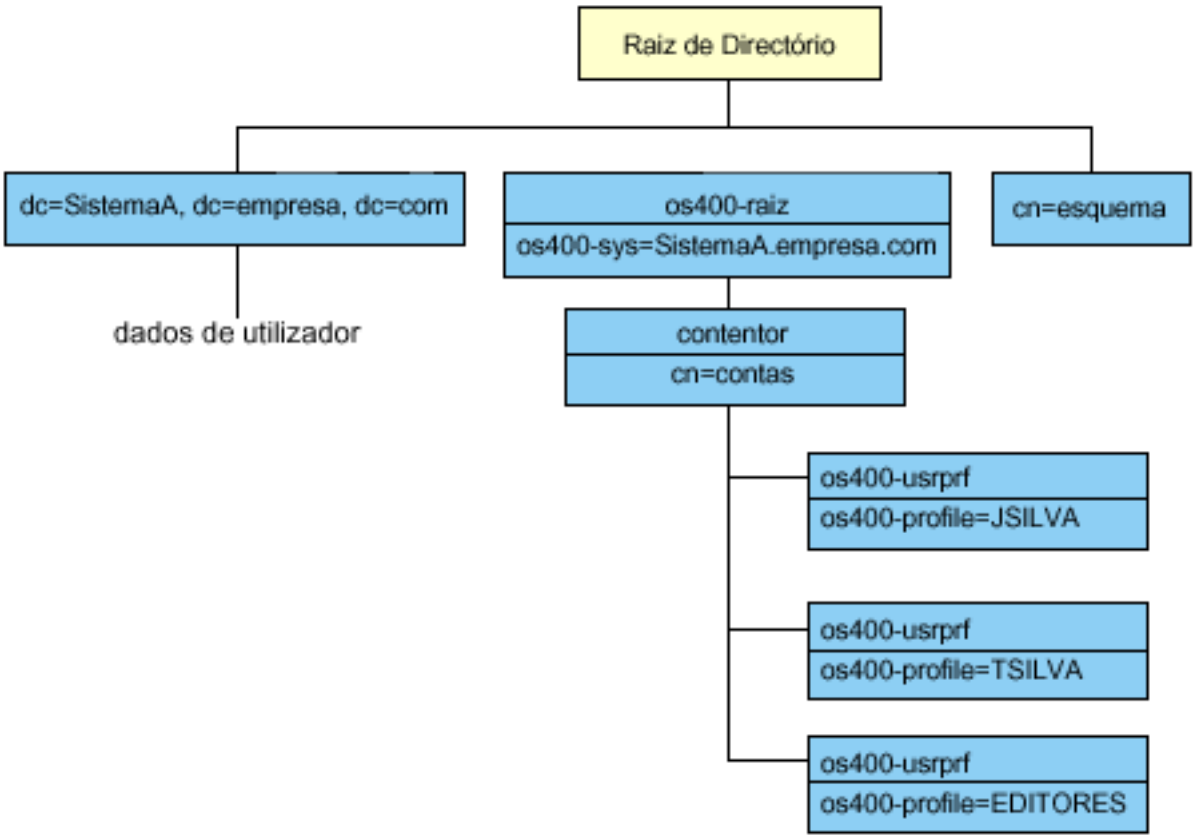
Para obter informações mais detalhadas sobre o sistema origem de projecção do sistema operativo, consulte:

- "Árvore de informações de directório projectada pelo utilizador do i5/OS"
- "Operações de LDAP" na página 71
- "DNs do administrador e de ligação de réplicas" na página 76
- "Esquema projectado pelo utilizador do i5/OS" na página 76

Árvore de informações de directório projectada pelo utilizador do i5/OS

A figura que se segue mostra uma árvore de informações de directório (DIT) exemplo para o sistema origem projectado pelo utilizador. A figura mostra perfis individuais e de grupo. Na figura, JSILVA e TSILVA são perfis de utilizador, indicados internamente pelo identificador de grupo (GID), GID=*NONE (ou 0); EDITORS é um perfil de grupo, que está indicado internamente por um GID diferente de zero.

O sufixo dc=SistemaA,dc=empresa,dc=com está incluído na figura para referência. Este sufixo representa o suporte de base de dados actual, que está a gerir outras entradas de LDAP. O sufixo cn=esquema é o esquema actual que está a ser utilizado em todo o servidor.



A raiz da árvore é um sufixo, cujo valor assumido é `os400-sys=`*`SistemaA.empresa.com`*, em que *`SistemaA.empresa.com`* é o nome do sistema. A objectclass é `os400-root`. Embora a DIT não possa ser modificada nem eliminada, poderá reconfigurar o sufixo dos objectos do sistema. No entanto, tem de assegurar que o sufixo actual não está a ser utilizado em ACLs ou noutro local do sistema em que possa ser necessário modificar entradas caso o sufixo seja alterado.

Na figura anterior, o contentor, cn=contas, é mostrado abaixo da raiz. Este objecto não pode ser modificado. É colocado um contentor neste nível, tendo em consideração outros tipos de informações ou objectos que poderão ser projectados pelo sistema operativo no futuro. Abaixo do contentor cn=contas, encontram-se os perfis de utilizador que são projectados como `objectclass=os400-usrprf`. Os perfis de utilizador são referidos como perfis de utilizador projectados e são conhecidos pelo LDAP no formato `os400-profile=JSILVA,cn=contas,os400-sys=SistemaA.empresa.com`.

Operações de LDAP

Seguem-se as operações de LDAP que podem ser executadas com a utilização dos perfis de utilizador projectados.

Ligar

Um cliente de LDAP pode ligar-se ao (autenticar-se no) servidor de LDAP utilizando o perfil de utilizador projectado. Para executar esta acção, especifique o nome exclusivo (DN - distinguished name) do perfil de utilizador projectado para o DN de associação e a palavra-passe correcta do perfil de utilizador do i5/OS para autenticação. Um exemplo de um DN utilizado num pedido de ligação seria `os400-profile=jsilva,cn=contas,os400-sys=sistemaA.empresa.com`.

Um cliente tem de ligar como um utilizador projectado para aceder às informações existentes no sistema origem de projecção do sistema.

Estão disponíveis dois mecanismos adicionais para autenticação no Directory Server como um utilizador do i5/OS:

- Ligação de GSSAPI SASL. Se o i5/OS estiver configurado para utilizar o mapeamento de identidades empresariais (EIM - Enterprise Identity Mapping), o Directory Server consulta o EIM para determinar se existe uma associação a um perfil de utilizador local do i5/OS, a partir da identidade Kerberos inicial. Se existir uma associação deste tipo, o servidor associará o perfil de utilizador à ligação e esta poderá ser utilizada para aceder ao sistema origem de projecção do sistema. Para obter mais informações sobre EIM, consulte o tópico EIM.
- Ligação de OS400-PRFTKN SASL. Pode ser utilizado um sinal de perfil para autenticação no Directory Server. O servidor associa o perfil de utilizador do sinal do perfil à ligação.

O servidor executa todas as operações utilizando a autoridade desse perfil de utilizador. O DN do perfil de utilizador projectado também pode ser utilizado em ACLs de LDAP tal como os DNs de outra entrada de LDAP. O método de ligação simples é o único método de ligação permitido quando é especificado um perfil de utilizador projectado num pedido de ligação.

Procura

O sistema origem de projecção do sistema suporta alguns filtros de procura base. Pode especificar os atributos objectclass, os400-profile e os400-gid em filtros de procura. O atributo os400-profile suporta caracteres globais. O atributo os400-gid está limitado à especificação de `(os400-gid=0)`, que é um perfil de utilizador individual, ou `!(os400-gid=0)`, que é um perfil de grupo. Pode obter todos os atributos de um perfil de utilizador, excepto a palavra-passe e atributos semelhantes.

Para certos filtros, só são devolvidos os valores de DN objectclass e os400-profile. No entanto, as procuras subsequentes poderão ser orientadas de modo a devolver informações mais detalhadas.

A tabela que se segue descreve o comportamento do sistema origem de projecção do sistema para operações de procura.

Tabela 2. Comportamento do sistema origem de projecção do sistema para operações de procura

Procura pedida	Base da procura	Âmbito da procura	Filtro de procura	Comentários
Devolver informações sobre os400-sys=SistemaA, (opcionalmente) para os contentores sob esse atributo e (opcionalmente) para os objectos nesses contentores.	os400-sys=SistemaA.empresa.com	base, sub ou um	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Devolver os atributos apropriados e os respectivos valores com base no âmbito e filtro especificados. Os atributos incorporados no código e os respectivos valores são devolvidos para o sufixo de objecto do sistema e para o contentor sob o mesmo.

Tabela 2. Comportamento do sistema origem de projecção do sistema para operações de procura (continuação)

Procura pedida	Base da procura	Âmbito da procura	Filtro de procura	Comentários
Devolver todos os perfis de utilizador.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	os400-gid=0	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.
Devolver todos os perfis de grupo.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	(!(os400-gid=0))	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.
Devolver todos os perfis de utilizador e de grupo.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	os400-profile=*	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.
Devolver informações sobre um perfil de utilizador ou de grupo específico, tal como o perfil de utilizador JSILVA.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	os400-profile=JSILVA	Podem ser especificados outros atributos a devolver.
Devolver informações sobre um perfil de utilizador ou de grupo específico, tal como o perfil de utilizador JSILVA.	os400-profile=JSILVA, cn=contas, os400-sys=SistemaA.empresa.com	bas, sub ou one	objectclass=os400-usrprf objectclass=* os400-profile=JSILVA	Podem ser especificados outros atributos a devolver. Embora possa ser especificado um âmbito de um nível, os resultados da procura não devolveriam valores porque não existe nada abaixo do perfil de utilizador JSILVA na DIT.

Tabela 2. Comportamento do sistema origem de projecção do sistema para operações de procura (continuação)

Procura pedida	Base da procura	Âmbito da procura	Filtro de procura	Comentários
Devolver todos os perfis de utilizador e de grupo começados por A.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	os400-profile=A*	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.
Devolver todos os perfis de grupo começados por G.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	(&(!(os400-gid=0)) (os400-profile=G*))	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.
Devolver todos os perfis de utilizador começados por A.	cn=contas, os400-sys=SistemaA.empresa.com	one ou sub	(&(os400-gid=0) (os400-profile=A*))	Só são devolvidos os valores de nome exclusivo (DN), classe objecto e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_TO_PERFORM.

Comparar

A operação comparar de LDAP pode ser utilizada para comparar um valor de atributo de um perfil de utilizador projectado. Os atributos os400-aut e os400-docpwd não podem ser comparados.

Adicionar e modificar

Pode criar perfis de utilizador utilizando a operação adicionar de LDAP e também pode modificar perfis de utilizador usando a operação modificar de LDAP.

Eliminar

Os perfis de utilizador podem ser eliminados através da operação eliminar de LDAP. Para especificar o comportamento dos parâmetros DLTUSRPRF OWNOBJOPT e PGPOPT, são agora fornecidos dois controlos do servidor de LDAP. Estes controlos podem ser especificados na operação eliminar de LDAP. Consulte o comando Eliminar Perfil de Utilizador (DLTUSRPRF) para obter mais informações sobre o comportamento destes parâmetros.

Seguem-se os controlos e os respectivos identificadores de objecto (OIDs) que podem ser especificados na operação eliminar cliente de LDAP.

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  O valor de controlo é uma cadeia no seguinte formato:

  – controlValue ::= ownObjOpt [newOwner]
  – ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  O valor de controlo ownObjOpt especifica a acção a executar se o perfil de utilizador for proprietário de quaisquer objectos. O valor *NODLT indica a não eliminação do perfil de utilizador, se for o proprietário de quaisquer objectos. O valor *DLT indica a eliminação de objectos com proprietário e o valor *CHGOWN indica a transferência da propriedade para outro perfil.

  O valor newOwner especifica o perfil para o qual a propriedade é transferida. Este valor é necessário quando ownObjOpt está definido como *CHGOWN.

  Seguem-se alguns exemplos do valor de controlo:

  – *NODLT: especifica que o perfil não pode ser eliminado se for proprietário de quaisquer objectos
  – *CHGOWN SILVA: especifica a transferência da propriedade de quaisquer objectos para o perfil de utilizador SILVA.

- O identificador de objecto (OID) é definido em ldap.h como LDAP_OS400_OWNOBJOPT_CONTROL_OID.

  – os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    O valor de controlo é definido como uma cadeia no seguinte formato:

    controlValue ::=pgpOpt [newPgp [newPgpAut]]
    pgpOpt ::= *NOCHG / *CHGPGP
    newPgp ::= *NONE / nome-perfil-utilizador
    newPgpAut ::= *OLDPGP / *PRIVATE / *ALL / *CHANGE / *USE / *EXCLUDE

    O valor pgpOpt especifica a acção a executar se o perfil que está a ser eliminado for o grupo principal de quaisquer objectos. Se for especificado *CHGPGP, também terá de ser especificado newPgp. O valor newPgp especifica o nome do perfil do grupo principal ou *NONE. Se for especificado um novo perfil de grupo principal, o valor newPgpAut também terá de ser especificado. O valor newPgpAut especifica a autoridade para os objectos que é concedida ao novo grupo principal.

  Seguem-se alguns exemplos do valor de controlo:

  – *NOCHG: especifica que o perfil não pode ser eliminado se for o grupo principal de quaisquer objectos.
  – *CHGPGP *NONE: especifica a remoção do grupo principal dos objectos.
  – *CHGPGP SILVA *USE: especifica a alteração do grupo principal para o perfil de utilizador SILVA e a atribuição da autoridade *USE ao grupo principal.

  Se um destes controlos não for especificado na eliminação, são utilizados, como alternativa, os valores assumidos actualmente em efeito para o comando QSYS/DLTUSRPRF.

ModRDN

Não pode mudar o nome dos perfis de utilizador projectados, uma vez que esta operação não é suportada pelo sistema operativo.

Importar e Exportar APIs

As APIs QgldImportLdif e QgldExportLdif não suportam a importação e exportação de dados no sistema origem de projecção do sistema.

DNs do administrador e de ligação de réplicas

Pode especificar um perfil de utilizador projectado como o DN do administrador ou de ligação de réplicas configurado. É usada a palavra-passe do perfil de utilizador. Os perfis de utilizador projectados também podem tornar-se administradores de LDAP se estiverem autorizados a aceder ao identificador da função Administrador do Directory Server (QIBM_DIRSRV_ADMIN). O acesso de administrador pode ser concedido a vários perfis de utilizador.

Para obter mais informações, consulte a secção "Trabalhar com o acesso administrativo para utilizadores autorizados" na página 111.

Esquema projectado pelo utilizador do i5/OS

Poderá encontrar as classes e atributos de objecto do sistema origem projectado no esquema utilizado em todo o servidor. Os nomes dos atributos de LDAP são especificados no formato `os400–nnn`, em que *nnn* é, normalmente, a palavra-chave do atributo nos comandos do perfil de utilizador. Por exemplo, o atributo os400-usrcls corresponde ao parâmetro USRCLS do comando CRTUSRPRF. Os valores dos atributos correspondem aos valores dos parâmetros aceites pelos comandos CRTUSRPRF e CHGUSRPRF ou aos valores apresentados quando é mostrado um perfil de utilizador. Utilize a ferramenta de administração da Web ou outra aplicação para ver as definições da objectclass os400-usrprf e os atributos de os400-xxx associados.

Suporte de registo de alterações do Directory Server e i5/OS

O Directory Server utiliza o suporte de base de dados do i5/OS, para armazenar informações de directório. O Directory Server utiliza o controlo de consolidações para arquivar entradas de directório na base de dados. Esta operação requer o suporte de registo de alterações do i5/OS.

Quando o servidor ou a ferramenta de importação de LDIF são iniciados pela primeira vez, são criados:

- Um diário
- Um receptor de diário
- Quaisquer tabelas de bases de dados necessárias inicialmente

O diário QSQJRN é construído na biblioteca da base de dados configurada pelo utilizador. O receptor de diário QSQJRN0001 é criado inicialmente na biblioteca de base de dados configurada pelo utilizador.

O ambiente, o tamanho e a estrutura do directório ou a estratégia de salvaguarda e restauro podem impor algumas diferenças, relativamente aos valores assumidos, incluindo o modo como estes objectos são geridos e o limiar de tamanho utilizado. Pode alterar os parâmetros dos comandos de registo em diários, se necessário. O registo em diário de LDAP é configurado, por valor assumido, de modo a eliminar receptores antigos. Se o registo de alterações estiver configurado e o utilizador pretender manter receptores antigos, execute o seguinte comando numa linha de comandos do i5/OS:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN) DLTRCV(*NO)
```

Se o registo de alterações for configurado, poderá eliminar os respectivos receptores de diário antigos com o seguinte comando:

```
CHGJRN JRN(QUSRDIRCL/QSQJRN)  DLTRCV(*YES)
```

Para obter informações sobre comandos de registo de alterações, consulte ""Comandos do OS/400"", no tópico ″Programação″.

Atributos operacionais

Existem vários atributos que têm um significado especial para o Directory Server e que são conhecidos como atributos operacionais. Estes são atributos mantidos pelo servidor e reflectem as informações que são geridas pelo servidor sobre uma entrada ou afectam o funcionamento do servidor. Estes atributos têm características especiais:

- Os atributos só são devolvidos por uma operação de procura se forem especificamente pedidos (por nome) no pedido de procura
- Os atributos não fazem parte de nenhuma classe de objecto. O servidor controla quais as entradas que têm os atributos.

São suportados pelo Directory Server os seguintes conjuntos de atributos operacionais:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp. Estes estão presentes em todas as entradas. Estes atributos mostram o DN de ligação e a hora a que uma entrada foi criada ou em que foi modificada pela última vez. Pode utilizar estes atributos em filtros de procura, por exemplo, para localizar todas as entradas modificadas após um período de tempo especificado. Estes atributos não podem ser modificados por nenhum utilizador.
- ibm-entryuuid. Este está presente em todas as entradas criadas quando o servidor tem a V5R3 ou posterior instalada. Este atributo é um identificador de cadeia universalmente exclusivo atribuído a cada entrada pelo servidor quando a entrada é criada. É útil para as aplicações que têm de distinguir entradas com nomes idênticos em servidores diferentes. O atributo utiliza o algoritmo DCE UUID para gerar um ID que seja exclusivo em todas as entradas de todos os servidores que utilizem uma marca de hora, um endereço de adaptador e outras informações.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Para obter mais informações, consulte a secção “Listas de controlo de acesso” na página 51.
- hasSubordinates. Este está presente em todas as entradas e tem o valor TRUE se a entrada tiver subordinados.
- numSubordinates. Este está presente em todas as entradas e contém o número de entradas que são descendentes desta entrada.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory (atributos da política de palavras-passe).
- subschemasubentry. Está presente em todas as entradas e identifica a localização do esquema para essa parte da árvore. É útil para os servidores com vários esquemas, caso se pretenda localizar o esquema que pode utilizar nessa parte da árvore.

Controlos e operações expandidas

Controlos

Os controlos fornecem informações adicionais ao servidor para determinar como este interpreta um determinado pedido. Por exemplo, um controlo `eliminar sub-árvore` pode ser especificado num pedido de eliminação de LDAP, indicando que o servidor deverá eliminar a entrada e todas as respectivas entradas subordinadas, em vez de eliminar apenas a entrada especificada. Um controlo consiste em três partes:

- O tipo de controlo, que é um OID que o identifica.
- Um indicador do nível de gravidade, que especifica qual deverá ser o comportamento do servidor caso não suporte o controlo. Este é um valor Booleano. FALSE indica que o controlo não é crítico e que o servidor o deverá ignorar caso não o suporte. TRUE indica que o controlo é crítico e que todo o pedido deverá falhar (com um erro de extensão crítico não suportado) caso o servidor possa respeitar o controlo.

- Um valor de controlo opcional, que contém outras informações específicas do controlo. O conteúdo do valor de controlo é especificado com a notação ASN.1. O valor propriamente dito é a codificação BER dos dados do controlo.

O Directory Server suporta os seguintes controlos:

Nome	**OID**	**Edição mais antiga do OS/400**	**Versão mais antiga do IBM Directory Server.**	**Descrição**
Gerir DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Gerir entradas de referência como entradas regulares.
Transacção	1.3.18.0.2.10.5	V4R5	V3.2	Marcar uma operação como parte de uma transacção.
OS/400 DLTUSRPRF OWNOBJOPT	1.3.18.0.2.10.8	V5R2		Opção eliminar perfil de utilizador do OS/400 referente ao proprietário do objecto. Consulte "Sistema origem de projecção do sistema operativo" na página 70, para obter detalhes.
OS/400 DLTUSRPRF PGPOPT	1.3.18.0.2.10.9	V5R2		Opção eliminar perfil de utilizador do OS/400 referente ao grupo principal. Consulte "Sistema origem de projecção do sistema operativo" na página 70, para obter detalhes.
Procura ordenada	1.2.840.113556.1.4.473 (pedido) e 1.2.840.113556.1.4.474 (resposta)	V5R2 com PTF	V4.1	Ordenar resultados da procura antes de devolver as entradas ao cliente.
Procura por página	1.2.840.113556.1.4.319	V5R2 com PTF	V4.1	Devolver os resultados da procura em páginas ao cliente, em vez de todos de uma vez.

Nome	OID	Edição mais antiga do OS/400	Versão mais antiga do IBM Directory Server.	Descrição
Controlo Eliminar Árvore	1.2.840.113556.1.4.805	V5R3	V5.1	Este controlo é anexado a um pedido Eliminar para indicar que a entrada especificada e todas as entradas descendentes deverão ser eliminadas. O utilizador tem de ser administrador de directório. A entrada a ser eliminada não pode ser um contexto de replicação.
Política de palavras-passe	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Devolver informações de erro adicionais sobre a política de palavras-passe ao cliente.
Administração do servidor	1.3.18.0.2.10.15	V5R3	V5.1	Permite que o administrador execute operações de reparação que, em condições normais, lhe seriam recusadas (por exemplo, actualizar uma réplica só de leitura, actualizar um servidor inactivo ou definir certos atributos operacionais).

Operações expandidas

As operações expandidas são utilizadas para iniciar operações adicionais para além das operações base do LDAP. Por exemplo, foram definidas operações expandidas para agrupar um conjunto de operações numa única transacção. Uma operação expandida consiste:

- No nome do pedido, um OID que identifique a operação específica.
- Num valor de pedido opcional, que contém outras informações específicas da operação. O conteúdo do valor do pedido é especificado com a utilização da notação ASN.1. O valor propriamente dito é a codificação BER dos dados do pedido.

Normalmente, as operações expandidas têm uma resposta expandida. A resposta consiste:

- Nos componentes do resultado de LDAP padrão (código de erro, DN correspondente e mensagem de erro)

- O nome da resposta, um OID que identifique o tipo de resposta
- Um valor opcional, que contém outras informações específicas da resposta. O conteúdo do valor de resposta é especificado com a utilização da notação ASN.1. O valor propriamente dito é a codificação BER dos dados da resposta.

O Directory Server suporte os seguintes pedidos expandidos:

Nome	OID	Edição mais antiga do OS/400	Versão mais antiga do IBM Directory Server.	Descrição
Registo de acontecimentos	1.3.18.0.2.12.1	V4R5	V3.2	
Cancelar registo de acontecimentos	1.3.18.0.2.12.3	V4R5	V3.2	
Iniciar transacção	1.3.18.0.2.12.5	V4R5	V3.2	
Terminar transacção	1.3.18.0.2.12.6	V4R5	V3.2	
Pedido de normalização do DN	1.3.18.0.2.12.30	V5R3	V5.1	

Estão definidas operações expandidas adicionais que não se destinam a ser iniciadas por um cliente. Estas operações são usadas através do utilitário ldapexop ou de operações executadas pela ferramenta de Administração da Web. Segue-se uma lista das operações, bem como a autoridade necessária para as iniciar:

Nome	OID	Edição mais antiga do OS/400	Versão mais antiga do IBM Directory Server.	Descrição
Replicação de controlos	1.3.18.0.2.12.16	V5R3	V5.1	Esta operação executa a acção pedida no servidor para o qual é emitida e dispõe em cascata a chamada a todos os consumidores abaixo da mesma na topologia de replicação. O cliente tem de ser o administrador do directório ou ter autoridade de escrita para o objecto ibm-replicagroup=default relativamente ao contexto de replicação associado.

Nome	OID	Edição mais antiga do OS/400	Versão mais antiga do IBM Directory Server.	Descrição
Fila de replicação de controlos	1.3.18.0.2.12.17	V5R3	V5.1	Esta operação marca itens como `já replicados` para um acordo especificado. Esta operação só é permitida quando o cliente tem autoridade de escrita para o acordo de replicação.
Tornar inactivo ou activo	1.3.18.0.2.12.17	V5R3	V5.1	Esta operação coloca a sub-árvore num estado que não aceita actualizações de clientes (ou termina este estado), à excepção das actualizações provenientes de clientes autenticados como administradores de directórios, em que está presente o controlo da Administração do Servidor. O cliente tem de estar autenticado como administrador do directório ou ter autoridade de escrita para o objecto ibm-replicagroup=default relativamente ao contexto de replicação associado.
Terminar transacção	1.3.18.0.2.12.19	V5R3	V5.1	

Nome	OID	Edição mais antiga do OS/400	Versão mais antiga do IBM Directory Server.	Descrição
Dispor replicação de controlos em cascata	1.3.18.0.2.12.15	V5R3	V5.1	Esta operação executa a acção pedida no servidor para o qual é emitida e dispõe em cascata a chamada a todos os consumidores abaixo da mesma na topologia de replicação. O cliente tem de ser o administrador do directório ou ter autoridade de escrita para o objecto ibm-replicagroup=default relativamente ao contexto de replicação associado.
Actualizar configuração	1.3.18.0.2.12.28	V5R3	V5.1	Esta operação é utilizada para fazer com que o servidor leia de novo definições específicas da respectiva configuração. A operação só é permitida quando o cliente é o administrador do directório.

Capítulo 5. Como começar com o Directory Server

O Directory Server é automaticamente instalado quando instala o i5/OS. O Directory Server inclui uma configuração assumida. Para começar com o Directory Server, proceda do seguinte modo:

1. Se estiver a instalar a V5R3 e a utilizar o Directory Server numa edição anterior, reveja as considerações sobre migração. Para obter mais informações, consulte "Considerações sobre migração".
2. Planeie o seu Directory Server. Para obter mais informações, consulte "Planear o Directory Server" na página 88.
3. Para personalizar definições do Directory Server, execute o assistente de Configuração do Directory Server. Para obter mais informações, consulte "Configurar o Directory Server" na página 89.
4. Inicie o servidor. Para obter mais informações, consulte a secção "Iniciar o Directory Server" na página 106
5. Utilize a ferramenta de administração da Web para criar ou editar directórios de LDAP. Para obter mais informações, consulte "Administração da Web" na página 90.
6. Consulte as informações do Capítulo 7, "Administrar o Directory Server", na página 105 para encontrar mais detalhes sobre como executar várias tarefas relacionadas com o Directory Server.

Considerações sobre migração

O Directory Server é automaticamente instalado quando instala o i5/OS. Da primeira vez que o servidor é iniciado, este migra automaticamente qualquer configuração e dados existentes. Este facto pode causar uma longa demora antes de o servidor ser iniciado da primeira vez.

Se tiver o Directory Server em execução com a V5R2 ou V5R1, consulte "Migrar para a V5R3 da V5R2 ou V5R1".

Se tiver o Directory Server em execução com a V4R3, V4R4 ou V4R5, pode migrar os seus dados para a V5R3. Para obter mais informações, consulte a secção "Migrar dados da V4R3, V4R4 ou V4R5 para a V5R3" na página 84.

Se tiver uma rede de servidores de replicação, consulte "Migrar uma rede de servidores de replicação" na página 86 para obter mais informações.

Se estiver a utilizar Kerberos, consulte "Alteração de nomes de serviço do Kerberos" na página 87.

Migrar para a V5R3 da V5R2 ou V5R1

A V5R3 do OS/400 introduz novas funções e capacidades no Directory Server. Estas alterações afectam tanto o Directory Server de LDAP como a interface gráfica do utilizador (GUI) do iSeries Navigator. Para beneficiar das novas funções da GUI, terá de instalar o iSeries Navigator num PC que possa comunicar por TCP/IP com o servidor iSeries. O iSeries Navigator é um componente do iSeries Access para Windows. Se tiver uma versão mais antiga do iSeries Navigator instalada, deverá actualizar para a V5R3.

A V5R3 do OS/400 suporta actualizações da V5R1 e V5R2. Quando actualiza para a V5R3 do OS/400, tanto os dados do directório de LDAP, como os ficheiros de esquema de directório, são automaticamente migrados para conformidade com os formatos da V5R3.

Quando actualizar para a V5R3 do OS/400, deverá ter em consideração algumas questões relacionadas com a migração:

- Quando actualiza para a V5R3, o Directory Server migra automaticamente os seus ficheiros de esquemas para a V5R3 e elimina os ficheiros de esquemas antigos. Contudo, se tiver eliminado ou

atribuído outro nome aos ficheiros de esquema, o Directory Server não pode migrá-los. Pode receber um erro ou o Directory Server pode assumir que os ficheiros já foram migrados.

- O Directory Server migra dados de directório para o formato da V5R3 da primeira vez que inicia o servidor ou importa um ficheiro LDIF. Reserve algum tempo para a conclusão da migração.

  Após actualizar para a V5R3, deverá iniciar o seu servidor uma vez para migrar os dados existentes antes de importar novos dados. Se tentar importar dados antes de iniciar o servidor uma vez e não tiver a autoridade necessária, a importação poderá falhar.
- Após a migração, o Directory Server de LDAP será automaticamente iniciado quando o TCP/IP for iniciado. Se não desejar que o Directory Server seja iniciado automaticamente, utilize o iSeries Navigator para alterar essa definição.

Migrar dados da V4R3, V4R4 ou V4R5 para a V5R3

A V5R3 do OS/400 não suporta actualizações directas da V4R3, V4R4 ou V4R5. Se pretende migrar um Directory Server com a V4R3, V4R4 ou V4R5, para a V5R3, pode executar um dos seguintes procedimentos:

- "Actualizar o OS/400 da V4R3, V4R4 ou V4R5 para uma edição intermédia" na página 85
- "Guardar a biblioteca de bases de dados e instalar a V5R3" na página 85

Antes de começar, leia o seguinte:

- Quando faz a actualização da V4R3 para qualquer versão posterior, deve ter em atenção os seguintes aspectos:
  - **Migrar o ficheiro do conjunto de chaves mistas para uma base de dados de chaves**

    O Directory Server de LDAP também utiliza um ficheiro do conjunto de chaves mistas para as respectivas ligações de SSL na V4R3. A partir da V4R4, utiliza o armazenamento de certificados do sistema. Se o servidor tiver sido configurado para utilizar SSL na versão V4R3, o conteúdo do ficheiro do conjunto de chaves mistas será migrado para o armazenamento de certificados do sistema.
  - **Foram removidos dois ficheiros de dados contínuos:**

    Os seguintes ficheiros de dados contínuos utilizados por Directory Server na V4R3 já não são necessários e são removidos automaticamente quando instala uma versão posterior:

    ```
    /QIBM/ProdData/OS400/DirSrv/qgldcert.kyr
    /QIBM/ProdData/OS400/DirSrv/qgldcert.sth
    ```

    Não é necessária qualquer acção relativamente a estes ficheiros. Este aspecto só é mencionado para que o utilizador não se preocupe se reparar que já não estão presentes no sistema.
- A V4R4 e as edições anteriores do Directory Server não tinham em consideração os fusos horários quando criavam entradas de marca de hora. A partir da V4R5, o fuso horário é utilizado em todas as adições e modificações feitas no directório. Por este motivo, se actualizar dados da V4R4 ou de uma versão anterior, o Directory Server ajusta os atributos `createtimestamp` e `modifytimestamp` existentes, de modo a reflectirem o fuso horário correcto. Realiza esta operação subtraindo o fuso horário actualmente definido no sistema iSeries às marcas de hora armazenadas no directório. Note que, se o fuso horário actual não for o mesmo que estava activo quando as entradas foram originalmente criadas ou modificadas, os novos valores da marca de hora não irão reflectir o fuso horário original.
- Se actualizar dados da V4R4 ou de uma versão anterior, tenha em atenção que os dados do directório vão requerer aproximadamente o dobro do espaço em memória que requeriam anteriormente. Isto acontece porque na V4R4, ou nas versões anteriores, o Directory Server apenas suportava o conjunto de caracteres IA5 e guardava dados em ccsid 37 (formato de byte único). O Directory Server suporta o conjunto de caracteres completo ISO 10646. Após a actualização, deverá iniciar o servidor uma vez para migrar os dados existentes antes de importar novos dados. Se tentar importar dados antes de iniciar o servidor uma vez e não tiver a autoridade necessária, a importação poderá falhar.
- Tenha também em atenção que podem existir questões adicionais associadas à actualização para a edição actual a partir de outras edições.

Actualizar o OS/400 da V4R3, V4R4 ou V4R5 para uma edição intermédia

Embora as actualizações da V4R3, V4R4 e V4R5 do OS/400 para a V5R3 não sejam suportadas, são suportadas as seguintes:

- Actualização da V4R3 e V4R4 para a V4R5
- Actualização da V4R4 e V4R5 para a V5R1
- Actualização da V4R5 e V5R1 para a V5R2
- Actualização da V5R1 e V5R2 para a V5R3

Uma forma de migrar o seu servidor com o Directory Server é actualizá-lo para uma edição intermédia (V5R1 ou V5R2) e, em seguida, para a V5R3. Para obter informações detalhadas sobre os procedimentos de instalação do OS/400, consulte o tópico *"Software Installation"*. Siga estes passos gerais para efectuar a migração:

1. Anote quaisquer alterações que tenha efectuado aos ficheiros de esquema no directório /QIBM/UserData/OS400/DirSrv. Os ficheiros de esquemas são migrados automaticamente.
2. Para a V5R3, proceda à instalação da V4R5.
3. Para a V4R4 ou V4R5, proceda à instalação da V5R1 ou V5R2.
4. Proceda à instalação para a V5R3.
5. Inicie o Directory Server, se ainda não o tiver feito.
6. Utilize a ferramenta de administração da Web para modificar os ficheiros de esquemas, de modo a incluírem quaisquer alterações de utilizador que tenha anotado no passo 1.
7. Reinicie o Directory Server.

Guardar a biblioteca de bases de dados e instalar a V5R3

Pode migrar o seu servidor com o Directory Server guardando a biblioteca de bases de dados que o Directory Server utiliza na V4R3, V4R4 ou V4R5 e, em seguida, restaurando-a após instalar a V5R3. Este procedimento evita a execução do passo da instalação de uma edição intermédia. Contudo, como as definições do servidor não são migradas, terá de as reconfigurar. Para obter informações detalhadas acerca dos procedimentos de instalação do OS/400, consulte *Instalação de Software* . Siga estes passos gerais para efectuar a migração:

1. Anote quaisquer alterações que tenha efectuado aos ficheiros de esquema no directório /QIBM/UserData/OS400/DirSrv. Os ficheiros de esquema não são migrados automaticamente, pelo que, se desejar manter as alterações, terá de as implementar de novo manualmente.
2. Anote as várias definições de configuração nas propriedades do Directory Server, incluindo o nome da biblioteca de bases de dados.
3. Guarde a biblioteca de bases de dados que está especificada na configuração do Directory Server. Se tiver configurado o registo de alterações, também terá de guardar a biblioteca QUSRDIRCL.
4. Anote a configuração de publicação.
5. Instale a V5R3 do OS/400 no sistema.
6. Utilize o EZ-Setup para configurar o Directory Server.
7. Restaure a biblioteca de bases de dados que tinha guardado no passo 3. Se tiver guardado a biblioteca QUSRDIRCL no passo 3, restaure-a agora.
8. Utilize a ferramenta de administração da Web para modificar os ficheiros de esquemas, de modo a incluírem quaisquer alterações de utilizador que tenha anotado no passo 1.
9. Utilize o iSeries Navigator para reconfigurar o Directory Server. Especifique a biblioteca de bases de dados que foi anteriormente configurada e que foi guardada e restaurada nos passos anteriores
10. Utilize o iSeries Navigator para reconfigurar a publicação.
11. Reinicie o Directory Server.

Migrar uma rede de servidores de replicação

Quando o servidor principal é iniciado pela primeira vez, migra as informações do directório que controlam a replicação. As entradas com a objectclass replicaObject em cn=sistcentrallocal são substituídas por entradas utilizadas pelo novo modelo de replicação (para obter mais informações, consulte "Replicação" na página 37). O servidor principal está configurado para replicar todos os sufixos do directório. As entradas de acordos são criadas com o atributo ibm-replicationOnHold definido como true (verdadeiro). Isto permite que as actualizações efectuadas ao servidor principal sejam acumuladas para a réplica até esta estar preparada.

Estas entradas são referidas como a topologia de replicação. O novo servidor principal pode ser utilizado com réplicas com versões anteriores instaladas; os dados relacionados com as novas funções não serão replicados para os servidores de versões anteriores. É necessário exportar as entradas de topologia de replicação do servidor principal e adicioná-las a cada réplica após o servidor de réplica ter sido migrado. Para exportar as entradas, utilize a ferramenta da linha de comandos Qshell "ldapsearch" na página 188 e guarde o output num ficheiro. O comando search é semelhante a:

```
ldapsearch -h nome-sistcentral-servidor-principal -p porta-servidor-principal \
 -D DN-admin-servidor-principal -w palavra-passe_admin-servidor-principal \
 -b ibm-replicagroup=default,DN-entrada-sufixo \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

Este comando cria um ficheiro LDIF de output denominado replication.topology.ldif no directório de trabalho actual. O ficheiro só contém as novas entradas.

Nota: Não inclua os seguintes sufixos:

- cn=registoalterações
- cn=sistcentrallocal
- cn=políticappasse
- cn=esquema
- cn=configuração

Inclua apenas os sufixos criados pelo utilizador.

Repita o comando para cada entrada de sufixo no servidor principal, mas substitua ">" por ">>" para anexar os dados ao ficheiro de output para procuras subsequentes. Concluído o ficheiro, copie-o para os servidores de réplica.

Adicione o ficheiro aos servidores de réplica após terem sido migrados com êxito; não adicione o ficheiro a servidores com versões anteriores do Directory Server instaladas. Tem de iniciar e parar o servidor antes de adicionar o ficheiro.

Para iniciar o servidor, utilize a opção **Iniciar** do iSeries Navigator. Para obter mais informações, consulte a secção "Iniciar o Directory Server" na página 106.

Para parar o servidor, utilize a opção **Parar** do iSeries Navigator. Para obter mais informações, consulte "Parar o Directory Server" na página 106.

Quando adicionar o ficheiro a um servidor de réplica, certifique-se de que este não foi iniciado. Para adicionar os dados, utilize a opção **Importar Ficheiro** do iSeries Navigator.

Carregadas as entradas da topologia de replicação, inicie o servidor de réplica e retome a replicação. Pode retomar a replicação de uma das seguintes formas:

- No servidor principal, utilize **Gerir Filas na Gestão de Replicação** da ferramenta de administração da Web.
- Use o utilitário de linha de comandos **ldapexop**. Por exemplo:

```
ldapexop -h nome-sistcentral-servidor-principal -p  porta-servidor-principal \
 -D DN-admin-servidor-principal -w palavra-passe_admin-servidor-principal \
 -op controlrepl -action retomar -ra DN-acordo-réplica
```

Este comando retoma a replicação do servidor definido na entrada com o DN especificado.

Para determinar qual o DN do acordo de réplica correspondente a um servidor de réplica, procure-o no ficheiro replication.topology.ldif. O servidor principal registará uma mensagem indicando que foi iniciada a replicação para essa réplica e um aviso de que o ID do servidor de réplica que consta no acordo não corresponde ao ID do servidor de réplica. Para actualizar o acordo de réplica de forma a utilizar o ID de servidor correcto, utilize **Gestão de Replicação** na ferramenta de administração da Web ou a ferramenta de linha de comandos **ldapmodify**. Por exemplo:

```
ldapmodify -c -h nome-sistcentral-servidor-principal -p porta-servidor-principal \
 -D DN-admin-servidor-principal -w  palavra-passe_admin-servidor-principal
dn: DN-acordo-réplica
changetype: modify
replace: ibm-replicaConsumerID
ibm-replicaConsumerID: ID-servidor-réplica
```

Pode introduzir estes comandos directamente na linha de comandos ou guardá-los num ficheiro LDIF e fornecê-los ao comando com a opção **-i** *ficheiro*. Utilize **Terminar Pedido Anterior** para parar o comando.

A migração desta réplica está concluída.

Para continuar a utilizar uma réplica com uma versão anterior instalada, continua a ser necessário retomar a replicação utilizando a ferramenta de linha de comandos **ldapexop** ou a **Gestão de Replicação** na ferramenta de administração da Web para essa réplica. Se for migrada posteriormente uma réplica com uma versão anterior instalada, utilize a ferramenta de linha de comandos **ldapdiff** para sincronizar os dados do directório. Deste modo, assegurará que as entradas ou atributos que não foram replicados são actualizados na réplica.

Alteração de nomes de serviço do Kerberos

Na V5R3, o nome de serviço utilizado pelo Directory Server e pelas APIs de cliente para autenticação de GSSAPI (Kerberos) foi alterado. Esta alteração é incompatível com o nome de serviço utilizado antes da V5R3 (a PTF 5722SS1-SI08487 da V5R2M0 inclui a mesma alteração).

Antes desta edição, o Directory Server e as APIs de cliente do i5/OS utilizavam um nome de serviço com o formato `LDAP/nome-sistcentral-dns@nicho do Kerberos` quando o mecanismo GSSAPI (Kerberos) era utilizado para autenticação. Este nome não está em conformidade com os padrões que definem a autenticação de GSSAPI, que indica que o nome do director deverá começar por ″ldap″ em minúsculas. Em resultado, tanto o Directory Server, como as APIs de cliente do i5/OS, podem não interagir com os produtos de outros fornecedores. Isto é particularmente verdade se o centro de distribuição de chaves de Kerberos (KDC) tiver nomes de directores sensíveis a maiúsculas e minúsculas. O fornecedor de serviços de LDAP para JNDI, uma API de cliente de LDAP de Java habitualmente utilizada, é um exemplo de um cliente incluído no i5/OS que utiliza o nome de serviço correcto.

A V5R3M0 altera o nome de serviço de modo a ficar em conformidade com as normas. No entanto, esta situação causa os seus próprios problemas de compatibilidade.

- Um Directory Server configurado para utilizar a autenticação de GSSAPI não começará a instalar esta edição. Isto acontece porque o ficheiro de separadores de chaves utilizado pelo servidor tem credenciais que usam o nome de serviço antigo (LDAP/mysys.ibm.com@IBM.COM), enquanto que o servidor procura credenciais que usem o novo nome de serviço (ldap/mysys.ibm.com@IBM.COM).
- Um Directory Server ou aplicação de LDAP que utilize as APIs de LDAP na V5R3M0 pode não conseguir a autenticação com servidores ou clientes de i5/OS mais antigos. Para corrigir esta situação, deverá proceder do seguinte modo:

1. Se o KDC utilizar nomes de directores sensíveis a maiúsculas e minúsculas, crie uma conta que utilize o nome de serviço correcto (ldap/mysys.ibm.com@IBM.COM).
2. Actualize o ficheiro de separadores de chaves utilizado pelo Directory Server do i5/OS de modo a conter credenciais para o novo nome de serviço. Também pode achar conveniente eliminar as credenciais antigas. Pode usar o utilitário de separadores de chaves Qshell para actualizar o ficheiro de separadores de chaves. Por valor assumido, o Directory Server utiliza o ficheiro /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. O assistente do Serviço de Autenticação da Rede V5R3M0 (Kerberos) do iSeries Navigator também cria entradas de separadores de chaves que utilizam o novo nome de serviço.
3. Actualize os sistemas de i5/OS V5R2M0, em que a GSSAPI é utilizada através da aplicação da PTF 5722SS1-SI08487.

Como alternativa, pode decidir que o Directory Server e as APIs de cliente continuem a utilizar o nome de serviço antigo. Esta situação pode ser conveniente quando estiver a utilizar a autenticação de Kerberos numa rede mista de sistemas a funcionar com e sem as PTFs. Para tal, defina a variável de ambiente LDAP_KRB_SERVICE_NAME. Pode defini-la para todo o sistema (obrigatório para definir o nome de serviço para o servidor) utilizando o seguinte comando:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

ou em QSH (para afectar os utilitários de LDAP executados a partir desta sessão de QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

Planear o Directory Server

Antes de instalar o Directory Server e antes de começar a configurar o directório de LDAP, disponha de algum tempo para planear o directório. Alguns aspectos importantes a considerar incluem:

- **Organizar o directório**. Planeie a estrutura do directório e determine quais os sufixos e atributos necessários ao servidor. Para obter mais informações, consulte “Directórios” na página 7, “Sufixo (contexto de nomenclatura)” na página 14 e “Atributos” na página 19.
- **Decidir o tamanho que pretende que o directório tenha**. Pode, em seguida, estimar a quantidade de memória necessária. O tamanho do directório depende do seguinte:
  - O número de atributos no esquema de servidores.
  - O número de entradas do servidor.
  - O tipo de informações que armazena no servidor.

  Por exemplo, um directório vazio que utiliza o esquema do Directory Server assumido necessita aproximadamente de 10 MB de espaço em memória. Um directório que utilize o esquema assumido e que contenha 1000 entradas de informações típicas sobre empregados requer cerca de 30 MB de espaço em memória. Este número varia de acordo com os atributos exactos que utilizou. Também aumentará significativamente se tiver armazenado no directório objectos grandes, como, por exemplo, imagens.
- **Decidir quais as medidas de segurança que irá tomar**.

  O Directory Server permite aplicar uma política de palavras-passe para assegurar que os utilizadores mudam periodicamente as respectivas palavras-passe e que estas cumprem os requisitos sintácticos de palavras-passe impostos pela empresa.

  O Directory Server suporta a utilização de Secure Sockets Layer (SSL) e Certificados Digitais, bem como a Transport Layer Security (TLS) para a segurança das comunicações. A autenticação de Kerberos também é suportada.

  O Directory Server permite controlar o acesso a objectos de directório com listas de controlo de acesso (ACLs). Também pode utilizar a auditoria de segurança do i5/OS para proteger o directório.

  Adicionalmente, escolha a política de palavras-passe a aplicar.
- **Escolher o DN e palavra-passe de um administrador**. O DN de administrador assumido é `cn=administrador`. Esta é a única identidade com autoridade para criar ou modificar entradas de

directório quando o servidor é configurado inicialmente. Pode utilizar o DN de administrador assumido ou seleccionar um DN diferente. Necessitará igualmente de criar uma palavra-passe para o DN do administrador.

- **Instalar software de pré-requisito para a ferramenta de administração da Web do Directory Server**. Para poder utilizar a ferramenta de administração da Web do Directory Server, terá de instalar os produtos de pré-requisito que se seguem no servidor iSeries.
  - IBM HTTP Server for iSeries (5722-DG1)
  - IBM WebSphere® Application Server - Express (5722-IWE Base and Option 2)

  Consulte o tópico IBM HTTP Server para obter mais informações sobre o IBM HTTP Server para iSeries e IBM WebSphere Application Server - Express.

Configurar o Directory Server

1. Se o seu sistema não tiver sido configurado para publicar informações noutro servidor de LDAP e não existirem outros servidores de LDAP conhecidos pelo servidor de DNS de TCP/IP, o Directory Server é automaticamente instalado com uma configuração assumida limitada. Consulte a secção "Configuração assumida do Directory Server" na página 90 para obter mais informações.O Directory Server fornece um assistente para o ajudar na configuração do Directory Server para as suas necessidades específicas. Pode executar este assistente como parte do EZ-Setup ou executá-lo mais tarde a partir do iSeries Navigator. Utilize este assistente quando configurar pela primeira vez o Directory Server. Pode igualmente utilizar o assistente para reconfigurar o Directory Server.

   Nota: Quando utiliza o assistente para reconfigurar o Directory Server, a configuração é iniciada de raiz. Em vez de ser alterada, a configuração original é eliminada. Contudo, os dados do directório não são eliminados, permanecendo armazenados na biblioteca que seleccionou na instalação (QUSRDIRDB, por valor assumido). O registo de alterações também permanece intacto, por valor assumido, na biblioteca QUSRDIRCL.

   Se pretende começar completamente do início, limpe aquelas duas bibliotecas antes de iniciar o assistente.

   Se pretender alterar a configuração do Directory Server, mas não limpá-la completamente, faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**. Este procedimento não elimina a configuração original.

   Para configurar o servidor, tem de ter as autoridades especiais *ALLOBJ e *IOSYSCFG. Se pretender configurar a auditoria de segurança do OS/400, também terá de ter a autoridade especial *AUDIT.
2. Para iniciar o Assistente de Configuração do Directory Server, efectue os seguintes passos:
   a. No iSeries Navigator, expanda **Rede**.
   b. Expanda **Servidores**.
   c. Faça clique sobre **TCP/IP**.
   d. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Configurar**.

      Nota: Se já tiver configurado o Directory Server, faça clique sobre **Reconfigurar** em vez de fazer clique sobre **Configurar**.
3. Siga as instruções do Assistente de Configuração do Directory Server para configurar o Directory Server.

   Nota: Pode também optar por colocar a biblioteca que armazena os dados de directórios num conjunto de memória auxiliar do utilizador (ASP), em vez do ASP do sistema. No entanto, esta biblioteca não pode ser armazenada num ASP Independente e qualquer tentativa de configurar, reconfigurar ou iniciar o servidor com uma biblioteca que exista num ASP Independente falhará.

4. Quando o assistente terminar, o Directory Server terá uma configuração base. Se estiver a utilizar o Lotus® Domino® no seu sistema, a porta 389 (a porta assumida para o servidor de LDAP) pode já estar a ser utilizada pela função de LDAP do Domino.Tem de executar uma das seguintes operações:
   - Alterar a porta utilizada pelo Lotus Domino. Consulte ""Hospedar o Domino LDAP e o Directory Server no mesmo iSeries"", no tópico "Correio electrónico", para obter mais informações.
   - Altere a porta utilizada pelo Directory Server. Consulte o tópico "Alterar a porta ou endereço de IP" na página 108, para obter mais informações.
   - Utilize endereços de IP específicos. Consulte a secção "Alterar a porta ou endereço de IP" na página 108 para obter mais informações.
5. Crie entradas correspondentes ao sufixo ou sufixos que tenha configurado. Para obter mais informações, consulte a secção "Adicionar e remover sufixos do Directory Server" na página 110.

Pode achar conveniente executar algumas ou todas as seguintes operações antes de continuar:
- Importar dados para o servidor; consulte "Importar um ficheiro de LDIF" na página 109.
- Activar a segurança de Secure Sockets Layer (SSL); consulte "Activar SSL no Directory Server" na página 131.
- Activar a autenticação de Kerberos, consulte "Activar a autenticação de Kerberos no Directory Server" na página 133.
- Configurar uma referência; consulte "Especificar um servidor para consultas de directório" na página 110.

Configuração assumida do Directory Server

O Directory Server é automaticamente instalado quando instala oOS/400. Esta instalação inclui uma configuração assumida. O Directory Server utilizar a configuração assumida quando todas as seguintes condições forem verdadeiras:

- Os administradores não executaram o Assistente de Configuração do Directory Server ou alterado as definições de directório com as páginas de propriedades.
- A publicação do Directory Server não está configurada.
- O Directory Server não consegue encontrar informações de DNS de LDAP.

Se o Directory Server utilizar a configuração assumida, ocorrerá o seguinte:

- O Directory Server será iniciado automaticamente quando o TCP/IP for iniciado.
- O sistema cria um administrador assumido, cn=Administrador. Para além disso, também gera uma palavra-passe que é utilizada internamente. Se necessitar de utilizar uma palavra-passe de administrador posteriormente, poderá definir uma nova na página de propriedades do Directory Server.
- É criado um sufixo assumido baseado no nome de IP do sistema. Também é criado um sufixo de objecto de sistema com base no nome do sistema. Por exemplo, se o nome de IP do seu sistema for maria.empresa.com, o sufixo será dc=maria,dc=empresa,dc=com.
- O Directory Server utiliza a biblioteca de dados assumida QUSRDIRDB. O sistema cria-a no ASP de sistema.
- O servidor utiliza a porta 389 para comunicações não seguras. Se tiver sido configurado um certificado digital para LDAP, o secure sockets layer (SSL) é activado e é utilizada a porta 636 para comunicações seguras.

Administração da Web

Podem ser administrados um ou mais Directory Servers através da consola de administração da Web. A consola de administração da Web permite:

- Adicionar ou alterar a lista de Directory Servers que podem ser administrados.
- Administrar um Directory Server utilizando a ferramenta de administração da Web.
- Alterar os atributos da consola de administração da Web.

Para utilizar a consola de administração da Web, proceda do seguinte modo:

1. Se esta for a primeira vez que está a utilizar a administração da Web do Directory Server, terá, primeiro de configurar a administração da Web (consulte "Configurar administração da Web pela primeira vez") e, em seguida, continuar com o passo seguinte.
2. Inicie sessão na administração da Web do Directory Server procedendo de um dos seguintes modos:
   - No iSeries Navigator, seleccione o seu servidor e faça clique sobre **Rede** > **Servidores** > **TCP/IP**, faça clique com o botão direito do rato sobre **Directório** e faça clique sobre **Administração do Servidor**.
   - Na página Tarefas do iSeries (http://*seu_servidor*:2001), faça clique sobre **IBM Directory Server**.
3. Se pretender administrar um Directory Server, proceda do seguinte modo:
   a. Seleccione o Directory Server que pretende administrar no campo **Nome de Sistema Central de LDAP**.
   b. Introduza o DN de início de sessão de administrador que utiliza para ligar ao Directory Server.
   c. Introduza a palavra-passe de administrador.
   d. Faça clique em **Iniciar Sessão**. É apresentada a página Ferramenta de Administração da Web do IBM Directory Server. Para obter mais informações sobre a página Ferramenta de Administração da Web do IBM Directory Server, consulte "Ferramenta de administração da Web" na página 93.
4. Se pretender adicionar ou alterar a lista de Directory Servers que podem ser administrados, ou alterar os atributos da consola de administração da Web, proceda do seguinte modo:
   a. Seleccione o campo **Admin da Consola** no campo **Nome de Sistema Central de LDAP**.
   b. Introduza o início de sessão de administrador da consola.
   c. Introduza a palavra-passe de administrador da consola.
   d. Faça clique em **Iniciar Sessão**. É apresentada a página Ferramenta de Administração da Web do IBM Directory Server. Para obter mais informações sobre a página Ferramenta de Administração da Web do IBM Directory Server, consulte "Ferramenta de administração da Web" na página 93.
   e. Faça clique sobre **Administração da consola** e, em seguida, seleccione uma das seguintes opções:
      - **Alterar início de sessão do administrador da consola**, para alterar o nome do início de sessão do administrador da consola.
      - **Alterar palavra-passe do administrador da consola**, para alterar a palavra-passe do administrador da consola.
      - **Gerir servidores da consola** para optar entre os Directory Servers que podem ser administrados pela consola de administração da Web.
      - **Gerir propriedades da consola** para alterar as propriedades da consola de administração da Web.

Configurar administração da Web pela primeira vez

Proceda do seguinte modo para configurar a Ferramenta de Administração da Web do Directory Server pela primeira vez.

1. Instale o IBM WebSphere Application Server - Express (5722-IWE Base e Opção 2) e o software de pré-requisito associado, se ainda não estiverem instalados. Consulte o tópico IBM HTTP Server para obter mais informações.
2. Active a instância-objecto do servidor de aplicações do sistema na instância-objecto do servidor HTTP ADMIN.
   a. Inicie a instância-objecto do servidor HTTP ADMIN procedendo do modo seguinte.
      - No iSeries Navigator, faça clique em **Network** -> **Servers** -> **TCP/IP** (Rede -> Servidores -> TCP/IP) e faça clique com o botão direito do rato em **HTTP Administration** (Administração de HTTP). Em seguida, faça clique em **Start** (Iniciar).
      - Numa linha de comandos do i5/OS, escreva `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

b. Inicie sessão no IBM Web Administration para iSeries. Utilize um perfil de utilizador e palavra-passe do i5/OS para iniciar sessão na página Tasks (Tarefas) do iSeries (http://*servidor*:2001), em seguida, faça clique em **IBM Web Administration for iSeries** (Administração da Web para iSeries da IBM).

c. Na página HTTP Server Administration *servidor* (Administração do servidor de HTTP em servidor), faça clique no separador **Manage** (Gerir) e, em seguida, faça clique no separador **HTTP Servers** (Servidores de HTTP). Certifique-se de que **ADMIN – Apache** está seleccionado na lista pendente Server (Servidor). Nas opções da área esquerda da janela da página, faça clique em **General Server Configuration** (Configuração geral do servidor).

   Nota: Poderá necessitar de expandir a secção **Server Properties** (Propriedades do servidor) para poder ver a opção **General Server Configuration** (Configuração geral do servidor).

d. Defina **Start the system application server instance when the 'Admin' server is started** (Iniciar a instância-objecto do servidor de aplicações do sistema quando o servidor 'Admin' for iniciado) como **Yes** (Sim).

e. Faça clique sobre **OK**.

3. Defina o WebSphere Application Server para utilizar o SYSINST.
   a. Faça clique em **WebSphere Application Server** nas opções da área esquerda da janela.
   b. Seleccione **WebSphere Application Server – Express 5.0**.
   c. Na lista pendente **WebSphere instance** (Instância-objecto do WebSphere), seleccione **SYSINST**.

      Nota: Se SYSINST não estiver presente na lista pendente, reinicie o servidor ADMIN.

   d. Na lista pendente **Start all WebSphere application server(s)...** (Iniciar todos os servidores da aplicação WebSphere), seleccione **Yes** (Sim).
   e. Na lista pendente **Stop all WebSphere application server(s)...** (Parar todos os servidores da aplicação WebSphere), seleccione **Yes** (Sim).
   f. Faça clique sobre **OK**.
4. Reinicie a instância-objecto do servidor HTTP ADMIN fazendo clique no botão de reinício (o segundo botão do separador **HTTP Servers** [Servidores de HTTP]). Também pode parar e iniciar a instância-objecto do servidor HTTP ADMIN utilizando o iSeries Navigator ou uma linha de comandos do i5/OS.

   Pode parar a instância-objecto do servidor HTTP ADMIN procedendo do modo seguinte.
   - No iSeries Navigator, faça clique em **Network -> Servers -> TCP/IP** (Rede -> Servidores -> TCP/IP) e faça clique com o botão direito do rato em **HTTP Administration** (Administração de HTTP). Em seguida, faça clique em **Stop** (Parar).
   - Numa linha de comandos do i5/OS, escreva `ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

   Pode iniciar a instância-objecto do servidor HTTP ADMIN procedendo do modo seguinte.
   - No iSeries, faça clique sobre **Rede -> Servidores -> TCP/IP** e faça clique com o botão direito do rato sobre **Administração de HTTP**. Em seguida, faça clique em **Start** (Iniciar).
   - Numa linha de comandos do i5/OS, escreva `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

   Consulte o tópico IBM HTTP Server para obter mais informações.
5. Inicie sessão em Directory Server Web Administration Tool (Ferramenta da Administração da Web do Directory Server).
   a. Invoque a **Login page** (Página de início de sessão) procedendo do modo seguinte.
      - No iSeries Navigator, seleccione o servidor e faça clique em **Network** -> **Servers** -> **TCP/IP** (Rede -> Servidores -> TCP/IP), faça clique com o botão direito do rato em **IBM Directory Server** e faça clique em **Server Administration** (Administração do servidor).
      - Na página Tasks (Tarefas) do iSeries (http://*servidor*:2001), faça clique em **IBM Directory Server for iSeries**.

b. Seleccione o campo **Console Admin** (Admin da Consola) no campo **LDAP Hostname** (Nome de sistema central de LDAP).
c. Escreva `superadmin` no campo **Username** (Nome de utilizador).
d. Escreva `secreta` no campo **Palavra-passe**.
e. Faça clique em **Iniciar Sessão**. É apresentada a página Ferramenta de Administração da Web do IBM Directory Server.

6. Mude o início de sessão de administração da consola.
   a. Faça clique em **Console administration** (Administração da consola) na área esquerda da janela para expandir a secção e, em seguida, faça clique em **Change console administrator login** (Alterar início de sessão do administrador da consola).
   b. Escreva um novo nome de início de sessão de administração da consola no campo **Administrador da consola**.
   c. Escreva a palavra-passe actual (`secreta`) no campo **Palavra-passe actual**.
   d. Faça clique sobre **OK**.
7. Altere a palavra-passe de administração da consola. Faça clique em **Change console administrator password** (Alterar palavra-passe do administrador da consola) na área esquerda da janela.
8. Adicione o Directory Server que pretende administrar. Faça clique em **Manage console servers** (Gerir servidores da consola) na área esquerda da janela.

   Nota: Ao adicionar um Directory Server do i5/OS, a **Administration port** (Porta de administração) não é utilizada e é ignorada.
9. Se pretender alterar as propriedades da consola, faça clique em **Manage console properties** (Gerir propriedades da consola) na área esquerda da janela.
10. Faça clique sobre **Terminar sessão**. Quando for apresentado o ecrã Logout successful (Concluir sessão com êxito), faça clique na ligação **aqui** para regressar à página de início de sessão da administração da Web.

Após ter configurado a consola pela primeira vez, poderá regressar à consola em qualquer momento, para:

- Alterar o início de sessão e palavra-passe do administrador da consola.
- Alterar os Directory Servers que podem ser administrados pela ferramenta de administração da Web.
- Alterar propriedades da consola.

Ferramenta de administração da Web

Depois de ter iniciado sessão na ferramenta de administração da Web, encontrará uma janela de aplicação composta por cinco partes:

Área da faixa
A área da faixa está localizada na parte superior do painel e contém o nome da aplicação e o logótipo da IBM.

Área de navegação
A área de navegação, localizada no lado esquerdo do painel, apresenta categorias expansíveis de várias tarefas de conteúdo relacionado com o servidor, tais como:

Propriedades do utilizador
Esta tarefa permite alterar a palavra-passe do utilizador actual.

Gestão de esquemas
Esta tarefa permite trabalhar com classes de objecto, atributos, regras de correspondência e sintaxes.

Gestão de directórios
Esta tarefa permite trabalhar com entradas de directório.

Gestão de replicação
Esta tarefa permite trabalhar com credenciais, topologia, marcações e filas.

Domínios e modelos
Esta tarefa permite trabalhar com modelos e domínios de utilizador.

Utilizadores e grupos
Esta tarefa permite trabalhar com utilizadores e grupos nos domínios definidos.Por exemplo, se pretender criar um novo utilizador da Web, a tarefa **Utilizadores e grupos** funciona com uma única objectclass de grupo, groupOfNames. Não é possível personalizar o suporte de grupo.

Espaço de trabalho
O espaço de trabalho mostra as tarefas associadas à tarefa seleccionada na área de navegação. Por exemplo, se estiver seleccionada a opção Gerir segurança do servidor na área de navegação, o espaço de trabalho apresentará a página Segurança do Servidor e os separadores que contêm as tarefas relacionadas com a configuração da segurança do servidor.

Área de estado do servidor
A área de estado do servidor, localizada na parte superior do espaço de trabalho. O símbolo do lado esquerdo da área de estado do servidor indica o estado actual do servidor. Ao lado do símbolo, está o nome do servidor que está a ser administrado. O símbolo do lado direito da área de estado do servidor fornece uma ligação à ajuda online.

Área de estado da tarefa
A área da tarefa, localizada abaixo do espaço de trabalho, apresenta o estado da tarefa actual.

Capítulo 6. Cenário: MinhaEmp, Lda. configura um Directory Server

Situação

Enquanto administrador dos sistemas informáticos da sua empresa, é possível que deseje colocar informações sobre empregados, como números de telefone e endereços de correio electrónico num repositório de LDAP central.

Objectivos

Neste cenário, a MinhaEmp, Lda. pretende configurar um Directory Server e criar uma base de dados de directórios que contenha informações sobre empregados, tais como o nome, o endereço de correio electrónico e o número de telefone .

Os objectivos deste cenário são os seguintes:

- Disponibilizar as informações sobre empregados em qualquer ponto da rede da empresa para os empregados que estejam a utilizar um cliente de correio do Lotus Notes® ou do Microsoft Outlook Express.
- Permitir que os gestores alterem dados sobre empregados na base de dados de directórios, impedindo, ao mesmo tempo, que os utilizadores não gestores o façam.
- Permitir que o servidor iSeries publique dados sobre empregados na base de dados de directórios.

Detalhes

O Directory Server será executado no servidor iSeries chamado meuiSeries.

O exemplo seguinte ilustra as informações que a MinhaEmp, Lda. pretende incluir na respectiva base de dados de directórios para cada empregado.

```
Nome: José Álvares
Departamento: DEPTA
Número de Telefone: 999 999 999
End. correio electrónico: jalvares@minha_emp.com
```

A estrutura de directórios para este cenário pode ser visualizada como algo semelhante a:

```
/
|
+- minha_emp.com
   |
   +- empregados
      |
      +- José Álvares
      |  DEPTA
      |  999-555-123
      |  jalvares@minha_emp.com
      |
      +- João Silva
      |  DEPTA
      |  999-555-124
      |  jsilva@minha_emp.com
      |
      +  Grupo de gestores
         José Álvares
```

```
        meuiSeries.minha_emp.com
.
.
.
```

Todos os empregados (gestores e não gestores) estão presentes na árvore de directório de empregados. Os gestores também pertencem ao grupo de gestores. Os membros do grupo de gestores têm autoridade para alterar dados sobre empregados.

O servidor iSeries (meuiSeries) também necessita de ter autoridade para alterar dados sobre empregados. Neste cenário, o servidor iSeries é colocado na árvore de directório de empregados e tornado membro do grupo de gestores.

Se pretender que as entradas de empregados sejam separadas da entrada do servidor iSeries, pode criar outra árvore de directórios (por exemplo: computadores) e adicionar-lhe o servidor iSeries. O servidor iSeries terá de ter a mesma autoridade que os gestores.

Pré-requisitos e pressupostos

A ferramenta de Administração da Web está devidamente configurada e a funcionar. Consulte a secção "Administração da Web" na página 90 para obter mais informações.

Passos de configuração

Complete as seguintes tarefas:
1. "Detalhes do cenário: Configurar o Directory Server".
2. "Detalhes do cenário: Criar a base de dados de directórios" na página 97.
3. "Detalhes do cenário: Publicar os dados do iSeries na base de dados de directórios" na página 100.
4. "Detalhes do cenário: Introduzir informações na base de dados de directórios" na página 101.
5. "Detalhes do cenário: Testar a base de dados de directórios" na página 101.

Detalhes do cenário: Configurar o Directory Server

Passo 1: Configurar o Directory Server

Nota: Para configurar o servidor, tem de ter as autoridades especiais *ALLOBJ e *IOSYSCFG.

1. No iSeries Navigator, faça clique sobre **Rede —> Servidores —> TCP/IP**.
2. Faça clique sobre **Configurar sistema como Directory Server** na janela **Tarefas de Configuração do Servidor**, no canto inferior direito do iSeries Navigator.
3. É apresentado o **Assistente de Configuração do Directory Server**.
4. Faça clique sobre **Configurar um Directory Server de LDAP local** na janela **Assistente de Configuração do IBM Directory Server - Bem-vindo**.
5. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Bem-vindo**.
6. Seleccione **Não** na janela **Assistente de Configuração do IBM Directory Server - Especificar Definições**. Desta forma, poderá configurar o servidor de LDAP sem as definições assumidas.
7. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Especificar Definições**.
8. Desmarque **System-generated** (Gerado pelo sistema) na janela **IBM Directory Server Configuration Wizard - Specify Administrator DN** (Assistente de configuração do IBM Directory Server - Especificar DN do administrador) e introduza o seguinte:

DN do Administrador	`cn=administrador`
Palavra-passe	`secreta`

Confirmar palavra-passe	secreta

Nota: Todas as palavras-passe especificadas neste cenário destinam-se exclusivamente a fins exemplificativos. Para evitar comprometer a segurança do seu sistema ou rede, nunca deverá utilizar estas palavras-passe como parte da sua própria configuração.

9. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Especificar DN do Administrador**.
10. Escreva `dc=minha_emp,dc=com` no campo **Sufixo** da janela **Assistente de Configuração do IBM Directory Server - Especificar Sufixos**.
11. Faça clique sobre **Adicionar** na janela **Assistente de Configuração do IBM Directory Server - Especificar Sufixos**.
12. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Especificar Sufixos**.
13. Seleccione **Sim, utilizar todos os endereços de IP** na janela **Assistente de Configuração do IBM Directory Server - Seleccionar Endereços de IP**.
14. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Seleccionar Endereços de IP**.
15. Seleccione **Sim** na janela **Assistente de Configuração do IBM Directory Server - Especificar Preferência de TCP/IP**.
16. Faça clique sobre **Seguinte** na janela **Assistente de Configuração do IBM Directory Server - Especificar Preferência de TCP/IP**.
17. Faça clique sobre **Terminar** na janela **Assistente de Configuração do IBM Directory Server - Resumo**.
18. Faça clique com o botão direito do rato sobre **IBM Directory Server** e faça clique sobre **Iniciar**.

Passo 2: Configurar a ferramenta de Administração da Web do Directory Server

1. Aponte o seu browser para http://*meuiSeries.minha_emp.com*:9080/IDSWebApp/IDSjsp/Login.jsp, em que *meuiSeries.minha_emp.com* é o seu servidor iSeries.
2. Deverá aparecer uma página de início de sessão. Faça clique sobre a lista **Nome de Sistema Central de LDAP** e seleccione **Admin da Consola**. Escreva `superadmin` para o nome de utilizador e `secreta` para a palavra-passe. Faça clique sobre **Iniciar Sessão**.
3. Configure a ferramenta de Administração da Web para ligação ao servidor de LDAP do seu iSeries. Seleccione **Administração da consola—> Gerir servidores da consola** na área de navegação da esquerda.
4. Faça clique sobre **Adicionar**.
5. No campo **Adicionar servidor**, escreva `meuiSeries.minha_emp.com`.
6. Faça clique sobre **OK**. O novo servidor aparece na lista sob **Gerir servidores da consola**.
7. Faça clique sobre **terminar sessão** na área de navegação da esquerda.
8. Na página de início de sessão da ferramenta de administração da Web, faça clique sobre a lista **Nome de Sistema Central de LDAP** e seleccione o servidor que acabou de configurar (**meuiSeries.minha_emp.com**).
9. No campo **Nome do Utilizador**, escreva `cn=administrador` e, no campo **Palavra-passe**, escreva `secreta`. Faça clique sobre **Iniciar Sessão**. Deverá ver a página principal da ferramenta de Administração da Web do IBM Directory Server.

Detalhes do cenário: Criar a base de dados de directórios

Antes de poder começar a introduzir dados, tem de criar um local para os armazenar.

Passo 1: Criar um objecto DN base

1. Faça clique sobre **Gestão de directórios —> Gerir entradas**. Poderá ver uma listagem dos objectos no nível base do directório. Como o servidor é novo, só poderá ver os objectos estruturais que contêm as informações de configuração.
2. Suponha que pretende adicionar um novo objecto para conter os dados da MinhaEmp, Lda. Primeiro, faça clique sobre **Adicionar...** do lado direito da janela. Na janela seguinte, desloque-se na lista **Classe de objecto** para seleccionar **domínio** e faça clique sobre **Seguinte**.
3. Como não pretende adicionar outras classes de objecto auxiliares, faça de novo clique sobre **Seguinte**.
4. Na janela **Introduzir os atributos**, introduza os dados correspondentes ao sufixo que criou anteriormente no assistente. Deixe a lista de selecção **Classe de objecto** em **domínio**. Escreva `dc=minha_emp` no campo **DN Relativo**. Escreva `dc=com` no campo **DN Ascendente**. Escreva minha_emp no campo **dc**.
5. Faça clique sobre **Terminar** na parte inferior da janela. Se regressar ao nível base, deverá ver o novo DN base.

Passo 2: Criar um modelo de utilizador

Irá criar um modelo de utilizador como uma ajuda para a adição dos dados sobre empregados da MinhaEmp, Lda.

1. Faça clique sobre **Domínios e modelos —> Adicionar modelo de utilizador**.
2. No campo **Nome do modelo de utilizador**, escreva `Empregado`.
3. Faça clique sobre o botão **Procurar...** ao lado do campo **DN Ascendente**. Faça clique sobre o DN base que criou na secção anterior,**dc=minha_emp,dc=com**, e faça clique sobre **Seleccionar**, do lado direito da janela.
4. Faça clique em **Next** (Seguinte).
5. Na lista de selecção **Classe de objecto estrutural**,
6. Escolha **inetOrgPerson** e faça clique sobre **Seguinte**.
7. Na lista de selecção **Atributo de nomenclatura**, seleccione **cn**.
8. Na lista **Separadores**, seleccione **Obrigatórios** e faça clique sobre **Editar**.
9. É na janela **Editar separador** que pode escolher quais os campos a incluir no modelo de utilizador. **sn** e **cn** são obrigatórios.
10. Na lista **Atributos**, seleccione **departmentNumber** e faça clique sobre **Adicionar >>>**.
11. Seleccione **telephoneNumber** e faça clique em **Add >>>** (Adicionar).
12. Seleccione **mail** e faça clique sobre **Adicionar >>>**.
13. Seleccione **userPassword** e faça clique sobre **Adicionar >>>**.
14. Faça clique sobre **OK** e, em seguida, sobre **Terminar** para criar o modelo de utilizador.

Passo 3: Criar um domínio

1. Na ferramenta de Administração da Web, faça clique sobre **Domínios e modelos —> Adicionar domínio**.
2. No campo **Nome do domínio**, escreva `empregados`.
3. Faça clique sobre **Procurar...** à direita do campo **DN Ascendente**.
4. Seleccione o DN ascendente que criou, **dc=minha_emp,dc=com** e faça clique sobre **Seleccionar** do lado direito da janela.
5. Faça clique sobre **Seguinte**.
6. Na janela seguinte, só precisa de alterar a lista de selecção **Modelo de utilizador**. Seleccione o modelo de utilizador que criou, **cn=empregados,dc=minha_emp,dc=com**.
7. Faça clique sobre **Terminar**.

Passo 4: Criar um grupo de gestores

1. Crie o grupo de gestores.
   a. Faça clique sobre **Utilizadores e grupos —> Adicionar grupo**.
   b. No campo **Nome do grupo**, escreva `gestores`.
   c. Certifique-se de que está seleccionado **empregados** na lista de selecção **Domínio**.
   d. Faça clique sobre **Terminar**.
2. Configure o administrador do grupo de gestores para o domínio **empregados**.
   a. Faça clique sobre **Domínios e modelos —> Gerir domínios**.
   b. Seleccione o domínio que criou **cn=empregados,dc=minha_emp,dc=com**, e faça clique sobre **Editar**.
   c. À direita do campo **Grupo de administradores**, faça clique sobre **Procurar...**.
   d. Seleccione **dc=minha_emp,dc=com** e faça clique sobre **Expandir**.
   e. Seleccione **cn=empregados** e faça clique sobre **Expandir**.
   f. Seleccione **cn=gestores** e faça clique sobre **Seleccionar**.
   g. Na janela **Editar domínio**, faça clique sobre **OK**.
3. Atribua ao grupo de gestores autoridade sobre o sufixo **dc=minha_emp,dc=com**.
   a. Faça clique sobre **Gestão de directórios —> Gerir entradas**.
   b. Seleccione **dc=minha_emp,dc=com** e faça clique sobre **Editar ACL...**.
   c. Na janela **Editar ACL**, faça clique sobre o separador **Proprietários**.
   d. Seleccione o quadrado de opção **Propagar proprietário**. Todos os utilizadores que sejam membros do grupo de gestores tornar-se-ão proprietários da árvore de dados **dc=minha_emp,dc=com**.
   e. Na lista pendente **Tipo**, seleccione **Grupo**.
   f. No campo **DN (Nome exclusivo)**, escreva `cn=gestores,cn=empregados,dc=minha_emp,dc=com`.
   g. Faça clique sobre **Adicionar**.
   h. Faça clique sobre **OK**.

Passo 5: Adicionar um utilizador como gestor

1. Na ferramenta de Administração da Web, faça clique sobre **Utilizadores e grupos —> Adicionar utilizador**.
2. Seleccione o domínio que criou, **empregados**, no menu pendente **Domínio**, e faça clique sobre **Seguinte**.
3. No campo **cn**, escreva `José Álvares`.
4. No campo ***sn** (apelido), escreva `Álvares`.
5. No campo ***cn** (nome completo), escreva `José Álvares`. cn é utilizado para criar o DN da entrada. *cn é um atributo do objecto.
6. No campo **telephoneNumber**, escreva `999 555 123`.
7. No campo **departmentNumber**, escreva `DEPTA`.
8. No campo **mail**, escreva `jalvares@minha_emp.com`.
9. No campo **userPassword**, escreva `secreta`.
10. Faça clique sobre o separador **Grupos de utilizadores**.
11. Na lista **Grupos disponíveis**, seleccione **gestores** e faça clique sobre **Adicionar —>**.
12. Na parte inferior da janela, faça clique sobre **Terminar**.
13. Termine sessão na ferramenta de administração da Web fazendo clique sobre **Terminar sessão** na área de navegação da esquerda.

Detalhes do cenário: Publicar os dados do iSeries na base de dados de directórios

Configure a publicação de modo a permitir que o seu servidor iSeries introduza automaticamente informações sobre utilizadores no directório de LDAP. As informações de utilizadores extraídas do directório de distribuição do sistema são publicadas no directório de LDAP.

Nota: Aos utilizadores criados com o iSeries Navigator, são atribuídos um perfil de utilizador e uma entrada de utilizador do directório de distribuição do sistema. Se utilizar comandos de CL para criar utilizadores, terá de criar um perfil de utilizador (**CRTUSRPRF**) e uma entrada de utilizador do directório de distribuição do sistema (**WRKDIRE**). Se os seus utilizadores só existirem como perfis de utilizador e pretender que sejam publicados no directório de LDAP, terá de criar entradas de utilizador do directório de distribuição do sistema para eles.

Passo 1: Criar o servidor iSeries como um utilizador do Directory Server

1. Inicie sessão na ferramenta de Administração da Web (http://**meuiSeries.minha_emp.com**:9080/IDSWebApp/IDSjsp/Login.jsp) como administrador.
   a. Seleccione **meuiSeries.minha_emp.com** na lista **LDAP Hostname** (Nome de sistema central de LDAP).
   b. Escreva `cn=administrador` no campo **Nome do Utilizador**
   c. Escreva `secreta` no campo **Palavra-passe**.
   d. Faça clique sobre **Iniciar Sessão**.
2. Seleccione **Utilizadores e grupos —> Adicionar utilizador**.
3. Seleccione **empregados** na lista **Domínio**.
4. Faça clique sobre **Seguinte**.
5. Escreva `meuiSeries.minha_smp.com` no campo **cn**.
6. Escreva `meuiSeries.minha_smp.com` no campo ***sn**.
7. Escreva `meuiSeries.minha_smp.com` no campo ***cn**.
8. Escreva `secreta` no campo **userPassword**.
9. Faça clique sobre o separador **Grupos de utilizadores**.
10. Seleccione o grupo **gestores**.
11. Faça clique sobre **Adicionar —>**.
12. Faça clique sobre **Terminar**.

Passo 2: Configurar o servidor iSeries para publicar dados

1. No iSeries Navigator, faça clique com o botão direito do rato sobre o seuiSeries na área de navegação da esquerda e seleccione **Propriedades**.
2. Na caixa de diálogo **Propriedades**, escolha o separador **Directory Server**.
3. Seleccione **Utilizadores** e faça clique sobre **Detalhes**.
4. Seleccione o quadrado de opção **Publicar informações sobre utilizadores**.
5. Na secção **Onde publicar**, faça clique sobre o botão **Editar**. É apresentada uma janela.
6. Escreva `meuiSeries.minha_emp.com`.
7. No campo **Sob o DN**, escreva `cn=empregados,dc=minha_emp,dc=com`.
8. Na secção **Ligação ao servidor**, certifique-se de que o número de porta assumido, **389**, foi introduzido no campo **Porta**. Na lista de selecção **Método de autenticação**, escolha **Nome exclusivo** e introduza `cn=meuiSeries,cn=empregados,dc=minha_emp,dc=com` no campo **Nome exclusivo**.
9. Faça clique sobre **Palavra-passe**.
10. Escreva `secreta` no campo **Palavra-passe**.
11. Escreva `secreta` no campo **Confirmar Palavra-passe**.

12. Faça clique sobre **OK**.
13. Faça clique sobre o botão **Verificar**. Deste modo, certificar-se-á de que introduziu todas as informações correctamente e que o iSeries poderá estabelecer ligação com o directório de LDAP.
14. Faça clique sobre **OK**.
15. Faça clique sobre **OK**.

Detalhes do cenário: Introduzir informações na base de dados de directórios

Enquanto gestor, José Álvares adiciona e actualiza agora os dados individuais dos empregados deste departamento. Ele terá de adicionar algumas informações suplementares sobre Joana Silva.Joana Silva é uma utilizadora do servidor iSeries e as respectivas informações foram publicadas. José Álvares também terá de adicionar informações sobre João Silva. João Silva não é utilizador do servidor iSeries. José Álvares executa o seguinte procedimento:

Passo 1: Iniciar sessão na ferramenta de Administração da Web

Inicie sessão na ferramenta de Administração da Web. (http://**meuiSeries.minha_emp.com**:9080/IDSWebApp/IDSjsp/Login.) do seguinte modo:

1. Seleccione **meuiSeries.minha_emp.com** na lista **Nome de Sistema Central de LDAP**.
2. Escreva `cn=José Álvares,cn=minhaemp empregados,dc=minha_emp,dc=com` no campo Nome do Utilizador.
3. Escreva `secreta` no campo de palavra-passe.
4. Faça clique sobre **Iniciar Sessão**.

Passo 2: Modificar dados de empregados

1. Faça clique sobre **Utilizadores e grupos —> Gerir utilizadores**.
2. Seleccione **empregados** na lista **Domínio** e faça clique sobre **Ver utilizadores**.
3. Seleccione **Joana Silva** na lista de utilizadores e faça clique sobre **Editar**.
4. Escreva `DEPTA` no campo **departmentNumber**.
5. Faça clique sobre **OK**.
6. Faça clique sobre **Fechar**.

Passo 3: Adicionar dados de empregados

1. Faça clique sobre **Utilizadores e grupos —> Adicionar utilizador**.
2. Seleccione **empregados** no menu pendente **Domínio** e faça clique sobre **Seguinte**.
3. No campo **cn**, escreva `João Silva`.
4. No campo ***sn**, escreva `Silva`.
5. No campo ***cn**, escreva `João Silva`.
6. No campo **telephoneNumber**, escreva `999 555 124`.
7. No campo **departmentNumber**, escreva `DEPTA`.
8. No campo **mail**, escreva`jsilva@minha_emp.com`.
9. Faça clique sobre **Terminar** na parte inferior da janela.

Detalhes do cenário: Testar a base de dados de directórios

Após ter introduzido os dados dos empregados na base de dados de directórios, teste a base de dados de directórios e o Directory Server, do seguinte modo:

Procure a base de dados de directórios utilizando o seu livro de endereços de correio electrónico

As informações existentes num directório de LDAP podem ser facilmente procuradas através de programas que suportem o LDAP. Muitos clientes de correio electrónico podem pesquisar Directory Servers de LDAP como parte da respectiva função do livro de endereços. Seguem-se alguns procedimentos exemplo para configurar o Lotus Notes 6 e o Microsoft Outlook Express 6. O procedimento para configurar muitos outros clientes de correio electrónico é semelhante.

Lotus Notes

1. Abra o seu livro de endereços.
2. Faça clique sobre **Acções —> Nova —> Conta**.
3. Escreva `meuiSeries` no campo **Nome da conta**.
4. Escreva `meuiSeries.minha_emp.com` no campo **Nome do servidor de contas**.
5. Seleccione **LDAP** no campo **Protocolo**.
6. Faça clique sobre o separador **Configuração do Protocolo**.
7. Escreva `dc=minha_emp,dc=com` no campo **Base de procura**.
8. Faça clique sobre **Guardar e fechar**.
9. Faça clique sobre **Criar —> Correio —> Memorando**.
10. Faça clique sobre **Endereço...**.
11. Seleccione `meuiSeries` no campo **Escolher livro de endereços**.
12. Escreva `Álvares` no campo **Procurar**.
13. Faça clique sobre **Procurar**. São apresentados os dados de José Álvares.

Microsoft Outlook Express

1. Faça clique sobre **Ferramentas —> Contas**.
2. Faça clique sobre **Adicionar —> Serviço de Directório**.
3. Escreva o endereço da Web do iSeries no campo **Directory Server (LDAP) da Internet** (`meuiSeries.minha_emp.com`).
4. Desmarque o quadrado de opção **O meu servidor de LDAP requer que eu inicie sessão**
5. Faça clique sobre **Seguinte**.
6. Faça clique sobre **Seguinte**.
7. Faça clique sobre **Terminar**.
8. Seleccione `meuiSeries.minha_emp.com` (o serviço de directório que acabou de configurar) e faça clique sobre **Propriedades**.
9. Faça clique sobre **Avançadas**.
10. Escreva `dc=minha_emp,dc=com` no campo **Base de procura**.
11. Faça clique sobre **OK**.
12. Faça clique sobre **Fechar**.
13. Escreva `Ctrl+E` para abrir a janela **Procurar Pessoas**.
14. Seleccione `meuiSeries.minha_emp.com` na lista **Procurar em**.
15. Escreva `Álvares` no campo **Nome**.
16. Faça clique sobre **Procurar agora**. São apresentados os dados de José Álvares.

Pesquisar a base de dados de directórios utilizando o comando da linha de comandos ldapsearch

1. Na interface baseada em caracteres, introduza o comando de CL **QSH** para abrir uma sessão de Qshell.
2. Introduza o que se segue para obter uma lista de todas as entradas de LDAP existentes na base de dados.

   ```
   ldapsearch –h meuiSeries.minha_emp.com –b dc=minha_emp,dc=com objectclass=*
   ```

   Em que:

–h é o nome da máquina sistema central que está a executar o servidor de LDAP.

–b é o DN base sob qual deve ser efectuada a procura.

objectclass=*
devolve todas as entradas do directório.

Este comando devolve algo semelhante a:

```
 dc=minha_emp,dc=com
 dc=minha_emp
 objectclass=domain
objectclass=superior

 cn=MinhaEmp empregado,dc=minha_emp,dc=com

.
.
.

cn=José Álvares,cn=Empregados da MinhaEmp,dc=minha_emp,dc=com

sn=Álvares
departmentNumber=DEPTA
mail=jalvares@minha_emp.com
telephoneNumber=999 999 999
objectclass=superior
objectclass=inetOrgPerson
objectclass=organizationalPerson
objectclass=person
cn=José Álvares

.
.
.
```

A primeira linha de cada entrada é o nome exclusivo (DN). Os DNs são como o nome de ficheiro completo de cada entrada. Algumas das entradas não contêm dados e são só estruturais. As que contêm a linha **objectclass=inetOrgPerson** correspondem às entradas criadas para pessoas. O DN de José Álvares é**cn=José Álvares,cn=Empregados da MinhaEmp,dc=minha_emp,dc=com**.

Capítulo 7. Administrar o Directory Server

Para administrar o Directory Server, terá de ter os seguintes conjuntos de autoridades:

- Para configurar o servidor ou alterar a configuração do servidor: Autoridades especiais Sobre Todos os Objectos (*ALLOBJ) e Configuração do Sistema de I/O (*IOSYSCFG)
- Para iniciar ou parar o servidor: Autoridade de Controlo de Trabalhos (*JOBCTL) e autoridade sobre objectos para os comandos Terminar TCP/IP (ENDTCP), Iniciar TCP/IP (STRTCP), Iniciar Servidor de TCP/IP (STRTCPSVR) e Terminar Servidor de TCP/IP (ENDTCPSVR)
- Para definir o comportamento de auditoria para o Directory Server: Autoridade especial Auditoria (*AUDIT)
- Para ver o registo de trabalhos do servidor: Autoridade especial de Controlo de Spool (*SPLCTL)

Para gerir objectos de directório (incluindo listas para controlo do acesso, propriedade de objectos e réplicas), estabeleça ligação com o directório utilizando o DN do administrador ou outro DN com a autoridade de LDAP adequada. Se estiver a ser utilizada a integração da autoridade, um administrador também poderá ser um utilizador projectado (consulte "Sistema origem de projecção do sistema operativo" na página 70) que tem autoridade para o ID da função de Administrador do Directory Server (consulte "Trabalhar com o acesso administrativo para utilizadores autorizados" na página 111).

Tarefas gerais de administração

Tarefas de conteúdo relacionado com directórios

- "Gerir domínios e modelos de utilizador" na página 154
- "Gerir listas de controlo de acesso (ACLs)" na página 162

Tarefas de publicação

- "Publicar informações no Directory Server" na página 167

Iniciar o Directory Server

Para iniciar o Directory Server, execute estes passos:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Iniciar**.

   O Directory Server pode demorar alguns minutos a ser iniciado, dependendo da velocidade do servidor e da quantidade de memória disponível. A primeira vez que iniciar o Directory Server pode demorar mais alguns minutos do que habitualmente porque o servidor tem de criar ficheiros novos. De modo semelhante, o início do Directory Server, pela primeira vez, após a actualização de uma versão anterior do Directory Server pode demorar mais alguns minutos do que o habitual, já que o servidor tem de migrar ficheiros. Pode verificar periodicamente o estado do servidor(consulte "Verificar o estado do Directory Server" na página 107), para ver se já foi iniciado.

O Directory Server também pode ser iniciado a partir da interface baseada em caracteres, através da introdução do comando `STRTCPSVR *DIRSRV`. Adicionalmente, se o Directory Server estiver configurado para ser iniciado quando inicia o TCP/IP, poderá igualmente iniciá-lo escrevendo o comando `STRTCP`.

Modo só de configuração

O Directory Server pode ser iniciado no modo só de configuração a partir da interface baseada em caracteres, através da introdução do comando `TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE)`.

O modo só de configuração inicia o servidor apenas com o sufixo cn=configuração activo e não depende do início bem sucedido dos sistemas de suporte da base de dados.

Parar o Directory Server

A paragem do Directory Server afecta todas as aplicações que estiverem a utilizar o servidor quando é parado. Isto inclui as aplicações de Enterprise Identity Mapping (EIM) que estão presentemente a utilizar o Directory Server para operações de EIM. Todas as aplicações são desligadas do Directory Server, embora não sejam impedidas de tentar estabelecer nova ligação com o servidor.

Para parar o Directory Server, execute estes passos:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Parar**.

   O Directory Server pode demorar alguns minutos a parar, dependendo da velocidade do sistema, da quantidade de actividade do servidor e da quantidade de memória disponível. Pode verificar periodicamente o estado do servidor(consulte "Verificar o estado do Directory Server" na página 107), para ver se já foi iniciado.

Nota: O Directory Server pode igualmente ser parado a partir de uma sessão de 5250 escrevendo os comandos `ENDTCPSVR *DIRSRV`, `ENDTCPSVR *ALL` ou `ENDTCP`. Os comandos `ENDTCPSVR *ALL` e `ENDTCP` afectam igualmente quaisquer outros servidores de TCP/IP utilizados no sistema. O comando `ENDTCP` também terminará o TCP/IP.

Verificar o estado do Directory Server

O iSeries Navigator apresenta o estado do Directory Server na coluna **Estado** na estrutura da direita.

Para verificar o estado do Directory Server, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.O iSeries Navigator apresenta o estado de todos os servidores de TCP/IP, incluindo o Directory Server, na coluna **Estado**. Para actualizar o estado dos servidores, faça clique sobre o menu **Ver** e seleccione **Actualizar**.
4. Para ver mais informações sobre o estado do Directory Server, faça clique com o botão direito do rato sobre **Directório** e seleccione **Estado**. Esta acção mostrar-lhe-á o número de ligações activas e outras informações como, por exemplo, níveis de actividade anteriores e actuais.

   Para além de fornecer informações adicionais, a visualização do estado através desta opção pode ajudá-lo a poupar tempo. Pode actualizar o estado do Directory Server sem perder o tempo adicional que é necessário para verificar o estado dos outros servidores de TCP/IP.

Verificar trabalhos no Directory Server

Por vezes, pode achar conveniente supervisionar trabalhos específicos no Directory Server. Para verificar os trabalhos do servidor, siga estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato em **Directory** (Directório) e seleccione **Server Jobs** (Trabalhos do servidor).

Activar a notificação de acontecimentos

O Directory Server suporta a notificação de acontecimentos, o que permite que os clientes se registem com o servidor de LDAP para serem notificados quando ocorrer um determinado acontecimento como, por exemplo, uma adição ao directório.

Siga estes passos para activar a notificação de acontecimentos para o servidor:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre **Acontecimentos**.
6. Seleccione **Permitir que os clientes se registem para a notificação de acontecimentos**.

Também poderá especificar o número máximo de registos permitidos para cada ligação e o total máximo de registos permitidos pelo servidor.

Para obter informações adicionais sobre a notificação de acontecimentos, consulte a secção Notificação de acontecimentos do IBM Directory Server Version 5.1 Programming Reference  .

Especificar definições de transacção

O Directory Server suporta transacções, o que permite que um grupo de operações de directório de LDAP seja tratado como uma unidade. Para obter mais informações, consulte a secção “Transacções” na página 43.

Para configurar as definições de transacção do servidor, siga estes passos:
1. No iSeries Navigator, expanda **Rede**.

2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre **Transacções**.
6. Especifique as definições da transacção.

   Nota: As definições de transacção podem causar impacto no rendimento dos servidores de LDAP, pelo que pode optar por fazer algumas experiências com definições diferentes.

Alterar a porta ou endereço de IP

O Directory Server utiliza as seguintes portas assumidas:
- 389 para ligações não protegidas.
- 636 para ligações protegidas (se tiver utilizado o Gestor de Certificados Digitais para activar o Directory Server como uma aplicação que pode utilizar uma porta segura).

Nota: Por valor assumido, todos os endereços de IP definidos no sistema local estão ligados ao servidor.

Se já estiver a utilizar estas portas para outra aplicação, pode atribuir uma porta diferente ao Directory Server ou utilizar endereços de IP diferentes para os dois servidores, caso a aplicação suporte a ligação a um endereço de IP específico.

Para obter um exemplo do conflito entre o servidor de LDAP do Domino e o Directory Server, consulte o tópico ″Hospedar o Domino LDAP e o Directory Server no mesmo iSeries″.

Para alterar as portas utilizadas pelo Directory Server, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Rede**.
6. Escreva os números das portas adequados e, em seguida, faça clique sobre **OK**.

Para alterar o endereço de IP em que o Directory Server aceita ligações, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Rede**.
6. Faça clique sobre o botão **Endereços de IP...**
7. Seleccione **Utilizar endereços de IP seleccionados** e seleccione os endereços de IP a serem utilizados pelo servidor ao aceitar ligações.

Definir política de palavras-passe

Para definir a política de palavras-passe, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Palavra-passe**.

6. Introduza as informações sobre a política de palavras-passe. Opcionalmente, faça clique sobre **Validação e Bloqueio de Palavra-passe** para especificar outras informações sobre a política de palavras-passe e, em seguida, faça clique sobre **OK**.
7. Faça clique sobre **OK**.

Nota: Também pode usar o utilitário ldapmodify (consulte "ldapmodify e ldapadd" na página 175) para definir a política de palavras-passe.

Para obter mais informações sobre a política de palavras-passe, consulte "Política de palavras-passe" na página 63.

Importar um ficheiro de LDIF

Pode transferir informações entre diferentes Directory Servers utilizando ficheiros do Formato de Permuta de Dados de LDAP (LDIF). Consulte a secção "Formato de permuta de dados de LDAP (LDIF)" na página 202 para obter mais informações.Antes de iniciar este procedimento, transfira o ficheiro de LDIF para o servidor iSeries como um ficheiro de dados contínuos.

Para importar um ficheiro de LDIF para o Directory Server, execute os seguintes passos:
1. Se o Directory Server tiver sido iniciado, interrompa a execução. Consulte "Parar o Directory Server" na página 106 para obter informações sobre como parar o Directory Server.
2. No iSeries Navigator, expanda **Rede**.
3. Expanda **Servidores**.
4. Faça clique sobre **TCP/IP**.
5. Faça clique com o botão direito do rato sobre **Directório**, seleccione **Ferramentas** e, em seguida, **Importar Ficheiro**.

   Opcionalmente, pode fazer com que o servidor replique os dados recém-importados da próxima vez que for iniciado seleccionando **Replicar dados importados**. Esta acção é útil ao adicionar novas entradas a uma árvore de directórios existente num servidor principal. Se estiver a importar dados para inicializar um servidor de réplica (ou de unidade), em condições normais, não pretenderá que os dados sejam replicados, uma vez que, possivelmente, já existem nos servidores dos quais este é fornecedor.

Nota: Também pode usar o utilitário ldapadd (consulte "ldapmodify e ldapadd" na página 175) para importar ficheiros de LDIF.

Exportar um ficheiro de LDIF

Pode transferir informações entre diferentes Directory Servers através da utilização de ficheiros do Formato de Permuta de Dados de LDAP (LDIF); consulte "Formato de permuta de dados de LDAP (LDIF)" na página 202. Pode exportar a totalidade ou parte do directório de LDAP para um ficheiro de LDIF.

Para exportar um ficheiro de LDIF a partir do Directory Server, efectue o seguinte procedimento:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório**, seleccione **Ferramentas** e, em seguida, **Exportar Ficheiro**.

   Nota: Se não especificar um caminho completo para o qual o ficheiro de LDIF deverá exportar dados, o ficheiro será criado no directório inicial especificado no seu perfil de utilizador do i5/OS.

Notas:

1. Não se esqueça de definir a autoridade para o ficheiro de LDIF, para impedir o acesso não autorizado aos dados do directório. Para efectuar este procedimento, faça clique com o botão direito do rato sobre o ficheiro no iSeries Navigator e, em seguida, seleccione **Permissões**.
2. Pode também criar um ficheiro de LDIF completo ou parcial com o utilitário ldapsearch, consulte "ldapsearch" na página 188.Utilize a opção -L e redireccione o output para um ficheiro.

Especificar um servidor para consultas de directório

Para definir servidores de referência para o Directory Server, execute estes passos:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e, em seguida, seleccione **Propriedades**.
5. Seleccione a página **Geral** das propriedades.
6. No campo **Nova referência**, especifique o URL do servidor de referência.
7. No pedido de informação, especifique o nome do servidor de referência no formato URL. Os exemplos que se seguem são URLs de LDAP aceitáveis:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Nota: Se o servidor de referência não utilizar a porta assumida, especifique o número de porta correcto como parte do URL, já que a porta 400 está especificada no segundo exemplo anterior.
8. Faça clique sobre **Adicionar**.
9. Faça clique sobre **OK**.

Adicionar e remover sufixos do Directory Server

A adição de um sufixo ao Directory Server permite que o servidor efectue a gestão dessa parte da árvore de directórios.

Nota: Não pode adicionar um sufixo que esteja sob outro sufixo já existente no servidor. Por exemplo, se `o=ibm, c=po` for um sufixo no servidor, não poderá adicionar `ou=coimbra, o=ibm, c=po`.

Para adicionar um sufixo ao Directory Server, efectue o seguinte procedimento:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Base de dados/Sufixos**.
6. No campo **Novo sufixo**, escreva o nome do novo sufixo.
7. Faça clique sobre **Adicionar**.
8. Faça clique sobre **OK**.

Nota: Adicionar um sufixo aponta o servidor para uma secção do directório. No entanto, não cria nenhuns objectos. Se um objecto correspondente ao novo sufixo não existir anteriormente, terá de criá-lo, tal como teria de fazer com qualquer outro objecto.

Para remover um sufixo do Directory Server, execute estes passos:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Base de dados/Sufixos**.

6. Faça clique sobre o sufixo que pretende remover para o seleccionar.
7. Faça clique sobre **Remover**.

Nota: Pode escolher eliminar um sufixo sem eliminar os objectos de directório dele dependentes. Isto torna os dados inacessíveis a partir do Directory Server. No entanto, poderá posteriormente readquirir o acesso aos dados adicionando de novo o sufixo.

Guardar e restaurar informações do Directory Server

O Directory Server guarda informações nas seguintes localizações:

- Biblioteca de bases de dados (QUSRDIRDB por valor assumido), que inclui o conteúdo dos Directory Servers.
- A biblioteca QDIRSRV2, utilizada para guardar as informações sobre publicações.
- A biblioteca QUSRSYS, que guarda os diversos itens em objectos que comecem por QGLD (especifique QUSRSYS/QGLD* para guardá-los).
- Se configurar o Directory Server para registar alterações nos directórios, uma biblioteca da base de dados chamada QUSRDIRCL, utilizada pelo registo de alterações.

Se o conteúdo do directório for frequentemente alterado, deverá guardar a biblioteca da base de dados e os objectos regularmente. Os dados de configuração estão também arquivados no seguinte directório:

```
/QIBM/UserData/OS400/Dirsrv/
```

Deve também guardar os ficheiros nesse directório sempre que alterar a configuração ou aplicar PTFs.

Consulte Cópia de Segurança e Recuperação SC17-5326 para obter informações sobre como guardar e restaurar dados de OS/400.

Trabalhar com o acesso administrativo para utilizadores autorizados

Pode conceder, ao administrador, acesso a perfis de utilizador aos quais foi concedido acesso para o identificador (ID) da função Administrador do Directory Server (QIBM_DIRSRV_ADMIN).

Por exemplo, se for concedido, ao perfil de utilizador JOAOSILVA, acesso para o ID da função Administrador do Directory Server e a opção Conceder acesso ao administrador para utilizadores autorizados estiver seleccionada na caixa de diálogo Propriedades de directório, o perfil JOAOSILVA terá autoridade de administrador. Quando este perfil é utilizado para ligar ao Directory Server utilizando o DN que se segue, os400-profile=JOAOSILVA,cn=contas,os400-sys=sistemaA.empresa.com, o utilizador tem autoridade de administrador. O sufixo do objecto do sistema neste exemplo é os400-sys=sistemaA.empresa.com. Para obter mais informações sobre utilizadores projectados, consulte “Sistema origem de projecção do sistema operativo” na página 70.

Para seleccionar esta opção, execute estes passos:

1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
4. No separador **Geral**, em **Informações do administrador**, seleccione a opção **Conceder acesso de administrador a utilizadores autorizados**.

Para definir o ID da função de autoridade do Administrador do Directory Server num perfil de utilizador, execute estes passos:

1. No iSeries Navigator, faça clique com o botão direito do rato sobre o nome do sistema e seleccione **Administração de Aplicações**.
2. Faça clique sobre o separador **Aplicações do Sistema Central**.

3. Expanda **Operating System/400**.
4. Faça clique sobre **Administrador do Directory Server** para evidenciar a opção.
5. Faça clique sobre o botão **Personalizar**.
6. Expanda **Utilizadores**, **Grupos** ou **Utilizações sem ser de um grupo**, conforme o que for apropriado para o utilizador que pretende.
7. Seleccione um utilizador ou grupo a adicionar à lista **Acesso permitido**.
8. Faça clique sobre o botão **Adicionar**.
9. Faça clique sobre **OK** para guardar as alterações.
10. Faça clique sobre **OK** na caixa de diálogo **Administração de Aplicações**.

Controlar o acesso e as alterações ao directório de LDAP

Poderá pretender registar o acesso e alterações ao directório de LDAP. Pode utilizar o registo de alterações de directórios de LDAP para controlar a localização das alterações ao directório.O registo de alterações está localizado no sufixo especial `cn=registoalterações`. É armazenado na biblioteca QUSRDIRCL.

Para activar o registo de alterações, siga estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Registo de Alterações**.
6. Seleccione **Alterações no directório de registo**.
7. (Opcional) No campo **Máximo de entradas**, especifique o número máximo de entradas que o registo de alterações deve manter. No campo **Duração máxima**, especifique durante quanto tempo as entradas do registo de alterações serão retidas.

   Nota: Embora estes parâmetros sejam opcionais, deverá considerar seriamente a especificação de um número máximo de entradas ou da duração máxima. Se não especificar nenhum deles, o registo de alterações manterá todas as entradas e poderá tornar-se muito grande.

A classe de objectos `changeLogEntry` é utilizada para representar as alterações aplicadas ao Directory Server. O conjunto de alterações é dado pelo conjunto ordenado de todas as entradas dentro do contentor changelog, como foi definido por `changeNumber`. As informações contidas no registo de alterações são só de leitura.

Qualquer utilizador que conste da Lista de Controlo de Acesso para o sufixo`cn=registoalterações` pode pesquisar as entradas do registo de alterações. Execute procuras apenas no sufixo do registo de alterações `cn=registoalterações`. Não tente adicionar, alterar ou eliminar entradas no sufixo do registo de alterações, mesmo que tenha autoridade para o fazer. Esta acção terá resultados imprevisíveis.

Exemplo:

O exemplo seguinte utiliza o utilitário da linha de comandos ldapsearch para recuperar todas as entradas do registo de alterações registadas no servidor:

```
ldapsearch -h ldaphost -D cn=admininistrador -w palavra-passe -b cn=registoalterações  (changetype=*)
```

Activar a auditoria de objectos para o Directory Server

O Directory Server suporta a auditoria de segurança de OS/400. Se o valor de sistema QAUDCTL estiver definido como *OBJAUD, poderá activar a auditoria de objectos através do iSeries Navigator.

Siga estes passos para activar a auditoria de objectos para o Directory Server:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Auditoria**.
6. Seleccione as definições de auditoria que deseja utilizar para o servidor.

As alterações implementadas às definições de auditoria ficarão activas quando fizer clique sobre **OK**. Não é necessário reiniciar o Directory Server. Para obter mais informações, consulte a secção "Segurança do Directory Server" na página 43

Ajustar definições de procura

Pode definir parâmetros de procura para controlar as capacidades de procura dos utilizadores, tais como a procura por página e ordenada.

Os resultados da procura por página permitem gerir a quantidade de dados devolvidos por um pedido de procura. É possível pedir um subconjunto de entradas (uma página) em vez de receber todos os resultados de uma só vez. Os pedidos de procura subsequentes apresentam a página seguinte de resultados, até a operação ser cancelada ou após ser devolvido o último resultado.

A procura ordenada permite que um cliente receba resultados de procura ordenados por uma lista de critérios, em que cada critério representa uma chave de ordenação. Esta faculdade passa a responsabilidade da ordenação da aplicação do cliente para o servidor.

Para ajustar os valores de procura do Directory Server, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Procurar**.

Ajustar definições de rendimento

Pode ajustar as definições de rendimento do seu Directory Server alterando uma das seguintes opções:
- O tamanho da memória cache da ACL, o tamanho da memória cache da entrada, o número máximo de procuras a armazenar na memória cache do filtro e a procura maior a guardar na memória cache do filtro.
- As definições da transacção dos servidores
- O número de ligações à base de dados e de módulos do servidor

Para ajustar os valores da memória cache do Directory Server, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Rendimento**.

Para ajustar os valores de transacção do Directory Server, execute estes passos:
1. No iSeries Navigator, expanda **Rede**.

2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Transacções**.

Pode também ajustar o rendimento do Directory Server alterando o número de ligações a bases de dados e módulos de servidor que o servidor utiliza. Para alterar este valor, siga estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Base de dados/Sufixos**.

Gerir a replicação

Para gerir a replicação, expanda a categoria **Gestão de replicação** da ferramenta de administração da Web. Para obter mais informações sobre conceitos de replicação, consulte "Replicação" na página 37.

Consulte o seguinte para obter mais informações:
- "Criar uma topologia de principal-réplica"
- "Criar uma topologia de servidor principal reencaminhador para réplica" na página 120
- "Descrição geral da criação de uma topologia de replicação complexa" na página 121
- "Criar uma topologia complexa com a replicação de unidade" na página 122
- "Gerir topologias" na página 125
- "Modificar propriedades de replicação" na página 128
- "Criar marcações de replicação" na página 129
- "Gerir filas" na página 131

Criar uma topologia de principal-réplica

Para definir uma topologia de principal-réplica, terá de:
1. Criar um servidor principal e definir o respectivo conteúdo. Seleccionar a sub-árvore que pretende replicar e especificar o servidor como principal. Consulte "Criar um servidor principal (sub-árvore replicada)" na página 115.
2. Criar credenciais a utilizar pelo fornecedor. Consulte "Criar credenciais" na página 115.
3. Criar um servidor de réplica. Consulte "Criar um servidor de réplica" na página 117.
4. Exportar a topologia do servidor principal para a réplica. Consulte "Copiar dados para a réplica" na página 118.
5. Altere a configuração da réplica para identificar quem está autorizado a replicar alterações nela efectuadas e adicione uma referência a um servidor principal. Consulte "Adicionar as informações sobre o fornecedor à réplica" na página 119.

Nota:

Se a entrada na raiz da sub-árvore que pretende replicar não for um sufixo no servidor, antes de poder utilizar a função **Adicionar sub-árvore**, terá de assegurar que as respectivas ACLs estão definidas do seguinte modo:

Para ACLs não filtradas:

```
ownersource: <igual ao DN da entrada>
ownerpropagate : TRUE
aclsource: <igual ao DN da entrada>
aclpropagate: TRUE
```

Para ACLs filtradas:

```
ibm-filteraclinherit : FALSE
```

Para satisfazer os requisitos da ACL, se a entrada não for um sufixo no servidor, edite a ACL para essa entrada no painel **Gerir entradas**. Seleccione a entrada e faça clique sobre **Editar ACL**. Se pretender adicionar ACLs não filtradas, seleccione esse separador e seleccione o quadrado de opção para especificar se as ACLs são explícitas ou não, quer relativamente às ACLs, quer aos respectivos proprietários. Certifique-se de que as opções **Propagar ACLs** e **Propagar proprietário** estão marcadas. Se pretender adicionar ACLs Filtradas, seleccione esse separador e adicione uma entrada **cn=este** com a função **id-acesso** para as ACLs e respectivos proprietários. Certifique-se de que a opção **Acumular ACLs filtradas** não está marcada e que **Propagar proprietário** está marcada. Consulte "Gerir listas de controlo de acesso (ACLs)" na página 162 para obter informações mais detalhadas.

Inicialmente, o objecto **ibm-replicagroup** criado por este processo herda a ACL da entrada raiz da sub-árvore da réplica. Estas ACLs podem não ser apropriadas para o controlo do acesso às informações de replicação existentes no directório.

Criar um servidor principal (sub-árvore replicada)

Nota: O servidor tem de estar a funcionar para que esta tarefa possa ser executada.

Esta tarefa designa uma entrada como raiz de uma sub-árvore replicada independentemente e cria uma **ibm-replicasubentry** que representa este servidor como o único servidor principal da sub-árvore. Para criar uma sub-árvore replicada, terá de designar a sub-árvore que pretende que o servidor replique.

Expanda a categoria Gestão de replicações na área de navegação e faça clique sobre **Gerir topologia**.

1. Faça clique sobre **Adicionar sub-árvore**.
2. Introduza o DN da entrada raiz da sub-árvore que pretende replicar ou faça clique sobre **Procurar** para expandir as entradas para seleccionar a entrada que deverá ser a raiz da sub-árvore.
3. O URL de referência do servidor principal é apresentado sob a forma de um URL de LDAP como, por exemplo:

   ldap://<*meuservidor*>.<*minhalocalização*>.<*minhaempresa*>.com

   Nota: O URL de referência do servidor principal é opcional. Só é utilizado:
   - Se o servidor contiver (ou vier a conter) quaisquer sub-árvores só de leitura.
   - Para definir um URL de referência que é devolvido para actualizações a qualquer sub-árvore só de leitura no servidor.
4. Faça clique sobre **OK**.
5. O novo servidor é apresentado no painel Gerir topologia, sob o título **Sub-árvores replicadas**.

Criar credenciais

Expanda a categoria Gestão de replicações na área de navegação da ferramenta de administração da Web e faça clique sobre **Gerir credenciais**.

1. Seleccione a localização que pretende utilizar para armazenar as credenciais na lista de sub-árvores. A ferramenta de administração da Web permite definir credenciais nestas localizações:
   - **cn=replicação,cn=sistcentrallocal**, que mantém as credenciais no servidor actual.

     Nota: Na maioria das situações de replicação, a localização das credenciais em cn=replicação,cn=sistcentrallocal é preferível porque fornece uma maior segurança do que as credenciais replicadas que se encontram na sub-árvore. No entanto, existem certas situações em que as credenciais localizadas em cn=replicação,cn=sistcentrallocal.

Se está a tentar adicionar uma réplica sob um servidor, por exemplo, o servidorA, e estiver ligado a um servidor diferente com a ferramenta de administração da Web, servidorB, o campo **Seleccionar credenciais** não apresenta a opção **cn=replicação,cn=sistcentrallocal**. Isto acontece porque o utilizador não pode ler as informações ou actualizar quaisquer informações sob **cn=sistcentrallocal** do servidorA quando está ligado ao servidorB.

A opção cn=replicação,cn=sistcentrallocal só está disponível quando o servidor sob o qual está a tentar adicionar uma réplica é o mesmo ao qual está ligado com a ferramenta de administração da Web.

- Na sub-árvore replicada, caso em que as credenciais são replicadas com o resto da sub-árvore. As credenciais colocadas na sub-árvore replicada são criadas abaixo da entrada **ibm-replicagroup=default** dessa sub-árvore.

  Nota: Se não estiverem apresentadas sub-árvores, vá para "Criar um servidor principal (sub-árvore replicada)" na página 115 para obter instruções sobre a criação da sub-árvore que pretende replicar.

2. Faça clique sobre **Adicionar**.
3. Introduza o nome das credenciais que está a criar como, por exemplo, **minhascreds**, em que cn= já está preenchido no campo.
4. Seleccione o tipo de método de autenticação que pretende utilizar e faça clique sobre **Seguinte**.
   - Se tiver seleccionado uma autenticação por ligação simples:
     a. Introduza o DN que o servidor utiliza para ligação à réplica como, por exemplo, cn=qualquer
     b. Introduza a palavra-passe que o servidor utiliza quando se ligar à réplica como, por exemplo, `secreta`.
     c. Introduza de novo a palavra-passe para confirmar que não existem erros de tipografia.
     d. Se quiser, introduza uma breve descrição das credenciais.
     e. Faça clique sobre **Terminar**.

     Nota: Pode achar conveniente registar o DN e palavra-passe de ligação das credenciais para referência futura. Irá necessitar desta palavra-passe quando criar o acordo de réplica.
   - Se tiver seleccionado a autenticação de Kerberos:
     a. Introduza o seu DN de ligação de Kerberos.
     b. Introduza a palavra-passe de ligação.
     c. Reintroduza a palavra-passe de ligação para a confirmar.
     d. Se quiser, introduza uma breve descrição das credenciais. Não são necessárias outras informações. Consulte "Activar a autenticação de Kerberos no Directory Server" na página 133 para obter informações adicionais.
     e. Faça clique sobre **Terminar**.

     Por valor assumido, o fornecedor utiliza o seu próprio servidor de serviço principal para ligação ao consumidor. Por exemplo, se o fornecedor se chamar principal.nossa.org.com e o domínio for QUALQUER.DOMÍNIO, o DN será **ibm-Kn=ldap/principal.nossa.org.com@QUALQUER.DOMÍNIO**. O valor do domínio não é sensível a maiúsculas e minúsculas. Se existir mais do que um fornecedor, terá de especificar o servidor principal e a palavra-passe a serem utilizados por todos os fornecedores.

     No servidor onde criou as credenciais:

     a. Expanda **Gestão de directórios** e faça clique sobre **Gerir entradas**.
     b. Seleccione a sub-árvore onde armazenou as credenciais como, por exemplo, **cn=sistcentrallocal** e faça clique sobre **Expandir**.
     c. Seleccione **cn=replicação** e faça clique sobre **Expandir**.

d. Seleccione as credenciais do Kerberos (ibm-replicationCredentialsKerberos) e faça clique em **Editar atributos**.
e. Faça clique sobre o separador **Outros atributos**.
f. Introduza o **replicaBindDN** como, por exemplo, **ibm-kn=meuservprincipal@QUALQUER.DOMÍNIO**.
g. Introduza as **replicaCredentials**. Esta é a palavra-passe de KDC utilizada para **meuservprincipal**.

Nota: Este servidor principal e palavra-passe devem ser iguais aos que irá utilizar para executar **kinit** na linha de comandos.

Na réplica

a. Faça clique sobre **Gerir propriedades de replicação** na área de navegação.
b. Seleccione um fornecedor no menu de selecção **Informações sobre o fornecedor** ou introduza o nome da sub-árvore replicada para a qual pretende configurar credenciais do fornecedor.
c. Faça clique sobre **Editar**.
d. Introduza o bindDN da replicação. Neste exemplo, **ibm-kn=meuservprincipal@QUALQUER.DOMÍNIO**.
e. Introduza e confirme a **Palavra-passe de ligação de replicação**. Esta é a palavra-passe de KDC utilizada para **meuservprincipal**.

- Se tiver seleccionado SSL com autenticação de certificados, não necessita de fornecer nenhuma informação adicional, caso esteja a utilizar o certificado do servidor. Se optar por utilizar um certificado diferente do do servidor:
  a. Introduza o nome do ficheiro de chaves.
  b. Introduza a palavra-passe do ficheiro de chaves.
  c. Introduza de novo a palavra-passe do ficheiro de chaves para a confirmar.
  d. Introduza a etiqueta da chave.
  e. Se quiser, introduza uma breve descrição.
  f. Faça clique sobre **Terminar**.

  Consulte "Activar SSL no Directory Server" na página 131 para obter informações adicionais.

5. No servidor onde criou as credenciais, defina o valor de sistema Permitir retenção das informações de segurança do servidor (QRETSVRSEC) como 1 (reter dados). O facto de as credenciais de replicação serem armazenadas numa lista de validação permite que o servidor obtenha as credenciais a partir da lista de validação quando estabelecer ligação com a réplica.

Criar um servidor de réplica

Nota: O servidor tem de estar a funcionar para que esta tarefa possa ser executada.

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir topologia**.

1. Seleccione a sub-árvore que pretende replicar e faça clique sobre **Mostrar topologia**.
2. Faça clique sobre a seta ao lado da opção **Topologia de replicação** para expandir a lista de servidores fornecedores.
3. Seleccione o servidor fornecedor e faça clique sobre **Adicionar réplica**.

No separador **Servidor** da janela **Adicionar réplica**:

- Introduza o nome de sistema central e número da porta para a réplica que está a criar. A porta assumida é 389 para não SSL e 636 para SSL. Estes campos são obrigatórios.
- Seleccione se pretende ou não activar as comunicações por SSL.
- Introduza o nome da réplica ou deixe este campo em branco para utilizar o nome do sistema central.

- Introduza o ID da réplica. Se o servidor em que está a criar a réplica estiver a funcionar, faça clique sobre **Obter ID da réplica** para preencher este campo automaticamente. Este campo é obrigatório, caso pretenda que o servidor que está a adicionar seja um servidor de unidade ou de reencaminhamento. Recomenda-se que todos os servidores tenham a mesma edição instalada.
- Introduza uma descrição do servidor de réplica.

No separador **Adicional**:

1. Especifique as credenciais que a réplica utiliza para comunicar com o servidor principal.

   Nota: A ferramenta de administração da Web permite definir credenciais nos seguintes locais:
   - **cn=replication,cn=localhost**, que mantém as credenciais apenas no servidor que as utiliza
   - Na sub-árvore replicada, caso em que as credenciais são replicadas com o resto da sub-árvore. As credenciais colocadas na sub-árvore replicada são criadas abaixo da entrada **ibm-replicagroup=default** dessa sub-árvore.

   Considera-se mais seguro colocar as credenciais em cn=replicação,cn=sistcentrallocal.

   a. Faça clique sobre **Seleccionar**.
   b. Seleccione a localização das credenciais que pretende utilizar. O ideal é que esta seja cn=replicação,cn=sistcentrallocal.
   c. Faça clique sobre **Mostrar credenciais**.
   d. Expanda a lista de credenciais e seleccione aquela que pretende utilizar.
   e. Faça clique sobre **OK**.

   Consulte “Criar credenciais” na página 115 para obter informações adicionais sobre credenciais do acordo.
2. Especifique uma marcação de replicação na lista de selecção ou faça clique sobre **Adicionar** para criar uma. Consulte o tópico “Criar marcações de replicação” na página 129.
3. Na lista de capacidades do fornecedor, pode desmarcar quaisquer capacidades que não pretenda replicar para o consumidor.

   Se a sua rede tiver vários servidores com edições diferentes, determinadas capacidades estão disponíveis apenas em edições posteriores. Determinadas capacidades, como a filtragem de ACLs e a política de palavras-passe, utilizam atributos operacionais que são replicados com outras alterações. Na maioria dos casos, se estas funções forem utilizadas, irá desejar que todos os servidores as suportem. Se nenhum dos servidores suportar uma capacidade, não irá desejar utilizá-la. Por exemplo, não vai querer ACLs diferentes a funcionar em cada servidor. No entanto, podem ocorrer casos em que, eventualmente, deseje utilizar uma capacidade nos servidores que a suportam e não pretender que as alterações relacionadas com ela sejam replicadas para servidores que não a suportem. Nestes casos, pode utilizar a lista de capacidades para marcar certas capacidades para não serem replicadas.
4. Faça clique sobre **OK** para criar a réplica.
5. É apresentada uma mensagem a indicar que deverão ser executadas acções adicionais. Faça clique sobre **OK**.

Nota: Se estiver a adicionar mais servidores como réplicas adicionais ou a criar uma topologia complexa, não continue com “Copiar dados para a réplica” ou “Adicionar as informações sobre o fornecedor à réplica” na página 119 enquanto não tiver acabado de definir a topologia no servidor principal. Se criar o ficheiro *fichprincipal.ldif* depois de ter concluído a topologia, ele contém as entradas de directório do servidor principal e uma cópia completa dos acordos da topologia. Quando carregar este ficheiro para cada um dos servidores, cada servidor passará a ter as mesmas informações.

Copiar dados para a réplica

Após criar a réplica, deverá exportar a topologia do servidor principal para a réplica.

1. No servidor principal, crie um ficheiro de LDIF para os dados. Para copiar todos os dados contidos no servidor principal, execute o seguinte procedimento:
   a. No iSeries Navigator, expanda **Rede**.
   b. Expanda **Servidores**.
   c. Faça clique sobre **TCP/IP**.
   d. Faça clique com o botão direito do rato sobre **Directório**, seleccione **Ferramentas** e, em seguida, **Exportar Ficheiro**.
   e. Especifique o nome do ficheiro de LDIF de output (por exemplo, `fichprincipal.ldif`), especifique, opcionalmente, uma sub-árvore a exportar (por exemplo `subtreeDN`) e faça clique sobre **OK**.
2. Na máquina onde está a criar a réplica, efectue o seguinte procedimento:
   a. Certifique-se de que os sufixos replicados estão definidos na configuração do servidor de réplica.
   b. Pare o servidor de réplica.
   c. Copie os ficheiros de LDIF para a réplica e execute os seguintes procedimentos:
      1) No iSeries Navigator, expanda **Rede**.
      2) Expanda **Servidores**.
      3) Faça clique sobre **TCP/IP**.
      4) Faça clique com o botão direito do rato sobre **Directório**, seleccione **Ferramentas** e, em seguida, **Importar Ficheiro**.
      5) Especifique o nome do ficheiro de LDIF de input (por exemplo, `fichprincipal.ldif`), especifique, opcionalmente, se pretende replicar dados e faça clique sobre **OK**.

      Os acordos, marcações e credenciais da replicação (se estiverem armazenados na sub-árvore replicada) e os dados de entrada são carregados para a réplica.
   d. Inicie o servidor.

Adicionar as informações sobre o fornecedor à réplica

É necessário alterar a configuração da réplica para identificar quem está autorizado a replicar as alterações efectuadas à mesma, e adicionar uma referência a um servidor principal.

Na máquina onde está a criar a réplica:

1. Expanda **Gestão de replicações** na área de navegação e faça clique sobre **Gerir propriedades de replicação**.
2. Faça clique sobre **Adicionar**.
3. Seleccione um fornecedor no menu de selecção **Sub-árvore replicada** ou introduza o nome da sub-árvore replicada para a qual pretende configurar credenciais do fornecedor. Se estiver a editar credenciais do fornecedor, este campo não é editável.
4. Introduza o bindDN da replicação. Neste exemplo, cn=qualquer.

   Nota: Pode utilizar qualquer uma destas opções, dependendo do seu caso.

   - Defina o DN (e a palavra-passe) de ligação da replicação e uma referência assumida para todas as sub-árvores replicadas para um servidor utilizando as 'credenciais e referência assumidas'. Estes podem ser utilizados quando todas as sub-árvores são replicadas a partir do mesmo fornecedor.
   - Defina o DN e a palavra-passe de ligação da replicação independentemente para cada sub-árvore replicada adicionando informações sobre o fornecedor para cada sub-árvore. Este procedimento pode ser utilizado quando cada sub-árvore tem um fornecedor diferente (ou seja, um servidor principal diferente para cada sub-árvore).
5. Dependendo do tipo de credencial, introduza e confirme a palavra-passe da credencial. (Esta palavra-passe foi registada anteriormente para utilização futura.)
   - **Ligação Simples** - Especifique o DN e a palavra-passe
   - **Kerberos** - Se as credenciais do fornecedor não identificarem o servidor principal e a palavra-passe, ou seja, se for utilizado o servidor principal de serviço próprio do servidor, o DN de ligação é

ibm-kn=ldap/<*seuservidor@seudomínio*>. Se as credenciais tiverem um nome de servidor principal, como <*meuservprincipal@meudomínio*>, utilize-o como o DN. Seja qual for o caso, não é necessária uma palavra-passe

- **SSL c/ ligação EXTERNA** - Especifique o DN do sujeito para o certificado sem palavra-passe

Consulte "Criar credenciais" na página 115.

6. Faça clique sobre **OK**.
7. Tem de reiniciar a réplica para que as alterações entrem em vigor.

Consulte "Modificar propriedades de replicação" na página 128 para obter informações adicionais.

A réplica está num estado suspenso e não está ocorrer replicação. Depois de acabar de configurar a sua topologia de replicação, terá de fazer clique sobre **Gerir filas**, seleccionar a réplica e fazer clique sobre **Suspender/retomar** para iniciar a replicação. Consulte "Gerir filas" na página 131 para obter informações mais detalhadas. A réplica recebe agora actualizações do servidor principal.

Criar uma topologia de servidor principal reencaminhador para réplica

Para definir uma topologia de servidor principal reencaminhador para réplica, é necessário:

1. Criar um servidor principal e um servidor de réplica. Consulte "Criar uma topologia de principal-réplica" na página 114.
2. Criar um novo servidor de réplica para a réplica original. Consulte "Criar um novo servidor de réplica".
3. Copiar dados para as réplicas. Consulte "Copiar dados para a réplica" na página 118.

Criar um novo servidor de réplica

Se tiver configurado uma topologia de replicação (consulte "Criar um servidor principal (sub-árvore replicada)" na página 115) com um servidor principal (servidor1) e uma réplica (servidor2), pode alterar a função do servidor2 para a de um servidor de reencaminhamento. Para tal, necessitará de criar uma nova réplica (servidor3) sob o servidor2.

1. Ligue Web Administration (Administração da Web) ao servidor principal (servidor1).
2. Expanda a categoria Gestão de replicações na área de navegação e faça clique sobre **Gerir topologia**.
3. Seleccione a sub-árvore que pretende replicar e faça clique sobre **Mostrar topologia**.
4. Faça clique sobre a seta ao lado da opção **Topologia de replicação** para expandir a lista de servidores fornecedores.
5. Faça clique sobre a seta ao lado da opção **servidor1** para expandir a lista de servidores.
6. Seleccione servidor2 e faça clique sobre **Adicionar réplica**.
7. No separador **Servidor** da janela **Adicionar réplica**:
   - Introduza o nome de sistema central e número da porta para a réplica (servidor3) que está a criar. A porta assumida é 389 para não SSL e 636 para SSL. Estes campos são obrigatórios.
   - Seleccione se pretende ou não activar as comunicações por SSL.
   - Introduza o nome da réplica ou deixe este campo em branco para utilizar o nome do sistema central.
   - Introduza o ID da réplica. Se o servidor em que está a criar a réplica estiver a funcionar, faça clique sobre **Obter ID da réplica** para preencher este campo automaticamente. Este campo é obrigatório, caso pretenda que o servidor que está a adicionar seja um servidor de unidade ou de reencaminhamento. Recomenda-se que todos os servidores tenham a mesma edição instalada.
   - Introduza uma descrição do servidor de réplica.

   No separador **Adicional**:

   a. Especifique as credenciais que a réplica utiliza para comunicar com o servidor principal.

      Nota: A ferramenta de administração da Web permite definir credenciais em dois locais:

- **cn=replicação,cn=sistcentrallocal**, o que mantém as credenciais apenas no servidor que as utiliza.
- Na sub-árvore replicada, caso em que as credenciais são replicadas com o resto da sub-árvore.

Considera-se mais seguro colocar as credenciais em cn=replicação,cn=sistcentrallocal. As credenciais colocadas na sub-árvore replicada são criadas abaixo da entrada **ibm-replicagroup=default** dessa sub-árvore.

1) Faça clique sobre **Seleccionar**.
2) Seleccione a localização das credenciais que pretende utilizar. O ideal é que esta seja cn=replicação,cn=sistcentrallocal.
3) Faça clique sobre **Mostrar credenciais**.
4) Expanda a lista de credenciais e seleccione aquela que pretende utilizar.
5) Faça clique sobre **OK**.

Consulte "Criar credenciais" na página 115 para obter informações adicionais sobre credenciais do acordo.

b. Especifique uma marcação de replicação na lista de selecção ou faça clique sobre **Adicionar** para criar uma. Consulte "Criar marcações de replicação" na página 129.

c. Na lista de capacidades do fornecedor, pode desmarcar quaisquer capacidades que não pretenda replicar para o consumidor.

Se a sua rede tiver vários servidores com edições diferentes, determinadas capacidades estão disponíveis apenas em edições posteriores. Determinadas capacidades, como a filtragem de ACLs e a política de palavras-passe, utilizam atributos operacionais que são replicados com outras alterações. Na maioria dos casos, se estas funções forem utilizadas, irá desejar que todos os servidores as suportem. Se nenhum dos servidores suportar uma capacidade, não irá desejar utilizá-la. Por exemplo, não vai querer ACLs diferentes a funcionar em cada servidor. No entanto, podem ocorrer casos em que, eventualmente, deseje utilizar uma capacidade nos servidores que a suportam e não pretender que as alterações relacionadas com ela sejam replicadas para servidores que não a suportem. Nestes casos, pode utilizar a lista de capacidades para marcar certas capacidades para não serem replicadas.

d. Faça clique sobre **OK** para criar a réplica.

8. Copie dados do servidor2 para a nova réplica, servidor3. Consulte "Copiar dados para a réplica" na página 118 para obter informações sobre como fazê-lo.
9. Adicione o acordo do fornecedor ao servidor3 que torna o servidor2 num fornecedor do servidor3 e o servidor3 num consumidor do servidor2. Consulte "Adicionar as informações sobre o fornecedor à réplica" na página 119 para obter informações sobre como fazê-lo.

As funções do servidor são representadas por símbolos da ferramenta de administração da Web. A sua topologia passa a ser:

- servidor1 (principal)
  - servidor2 (reencaminhador)
    - servidor3 (réplica)

Descrição geral da criação de uma topologia de replicação complexa

Utilize esta descrição de alto nível como guia para configurar uma topologia de replicação complexa.

1. Inicie todos os servidores de unidade ou futuras réplicas. Esta acção é obrigatória para que a ferramenta de administração da Web recolha informações dos servidores.
2. Inicie o 'primeiro' servidor principal e configure-o como servidor principal para o contexto.
3. Carregue os dados para a sub-árvore a replicar no 'primeiro' servidor principal, caso ainda não tenham sido carregados.
4. Seleccione a sub-árvore a replicar.

5. Adicione todos os servidores de unidade em potencial como réplicas do 'primeiro' servidor principal.
6. Adicione todas as outras réplicas.
7. Mova os outros servidores principais de unidade para os promover.
8. Adicione acordos de réplica referentes às réplicas a cada um dos servidores principais de unidade.

   Nota: Se pretender criar as credenciais em **cn=replicação,cn=sistcentrallocal**, as credenciais terão de ser criadas em cada servidor depois de serem reiniciadas. A replicação pelos servidores de unidade falhará enquanto os objectos credenciais não forem criados.
9. Adicione acordos de réplica referentes aos outros servidores principais a cada um dos servidores principais de unidade. O 'primeiro' servidor principal já dispõe dessa informação.
10. Desactive a sub-árvore replicada. Esta acção impede que sejam efectuadas actualizações durante a cópia dos dados para os outros servidores.
11. Utilize Gestão de filas para ignorar actualizações em todas as filas.
12. Exporte os dados para a sub-árvore replicada, a partir do 'primeiro' servidor principal.
13. Active a sub-árvore.
14. Pare os servidores de réplica e importe os dados para a sub-árvore replicada para cada servidor de réplica e servidor principal de unidade. Em seguida, reinicie os servidores.
15. Efectue a gestão das propriedades de replicação em cada servidor de réplica e servidor principal de unidade para definir as credenciais a serem utilizadas por fornecedores.

Criar uma topologia complexa com a replicação de unidade

A replicação de unidade é uma topologia de replicação em que vários servidores são servidores principais. No entanto, ao contrário de um ambiente de vários servidores principais, não é executada a resolução de conflitos entre os servidores de unidade. Os servidores de LDAP aceitam as actualizações fornecidas pelos servidores de unidade e actualizam as suas próprias cópias dos dados. A ordem pela qual as actualizações são recebidas não é tomada em consideração, nem o facto de várias actualizações entrarem em conflito.

Para adicionar outros servidores principais (unidades), terá primeiro de adicionar o servidor como uma réplica só de leitura dos servidores principais existentes (consulte "Criar um servidor de réplica" na página 117), inicializar os dados de directório e, em seguida, promover o servidor a servidor principal (consulte "Mover ou promover um servidor" na página 125).

Inicialmente, o objecto **ibm-replicagroup** criado por este processo herda a ACL da entrada raiz da sub-árvore da réplica. Estas ACLs podem não ser apropriadas para o controlo do acesso às informações de replicação existentes no directório.

Para que a operação Adicionar sub-árvore tenha êxito, o DN da entrada que está a adicionar tem de ter ACLs correctas, caso não seja um sufixo no servidor.

Para ACLs Não Filtradas:

- ownersource : *<o DN da entrada>*
- ownerpropagate : TRUE
- aclsource : *<o DN da entrada>*
- aclpropagate: TRUE

ACLs Filtradas:

- ownersource : *<o DN da entrada>*
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : *<qualquer valor>*

Utilize a função **Editar ACLs** da ferramenta de administração da Web para definir ACLs para as informações de replicação associadas à sub-árvore replicada recém-criada (consulte "Editar listas de controlo de acesso" na página 127).

A réplica está num estado suspenso e não está ocorrer replicação. Depois de acabar de configurar a sua topologia de replicação, terá de fazer clique sobre **Gerir filas**, seleccionar a réplica e fazer clique sobre **Suspender/retomar** para iniciar a replicação. Consulte "Gerir filas" na página 131 para obter informações mais detalhadas. A réplica recebe agora actualizações do servidor principal.

Utilize a replicação de unidade apenas em ambientes em que o padrão de actualizações de directórios for bem conhecido. As actualizações a objectos específicos no directório só podem ser executadas por um servidor de unidade. Este facto tem como objectivo impedir que um servidor elimine um objecto e, em seguida, que outro servidor o modifique. Este cenário cria a possibilidade de um servidor de unidade receber um comando eliminar seguido de um comando modificar, o que cria um conflito.

Para definir uma topologia de unidade reencaminhadora para réplica, consistindo em dois servidores unidade-principal, dois servidores de reencaminhamento e quatro réplicas, é necessário:

1. Criar um servidor principal e um servidor de réplica. Consulte "Criar uma topologia de principal-réplica" na página 114.
2. Criar dois servidores de réplica adicionais para o servidor principal. Consulte "Criar um servidor de réplica" na página 117.
3. Criar duas réplicas sob cada um dos dois servidores de réplica recém-criados.
4. Promover a réplica original a servidor principal. Consulte "Promover um servidor a unidade".

   Nota: O servidor que pretende promover a principal tem de ser uma réplica terminal sem réplicas subordinadas.
5. Copiar os dados do servidor principal para o novo servidor principal e para as réplicas. Consulte "Copiar dados para a réplica" na página 118.

Promover um servidor a unidade

Utilizando a topologia de reencaminhamento criada em "Criar uma topologia de servidor principal reencaminhador para réplica" na página 120, pode promover um servidor a unidade. Neste exemplo, vamos promover a réplica (servidor3) a unidade no servidor principal (servidor1).

1. Ligue a Administração da Web ao servidor principal (servidor1).
2. Expanda a categoria Gestão de replicações na área de navegação e faça clique sobre **Gerir topologia**.
3. Seleccione a sub-árvore que pretende replicar e faça clique sobre **Mostrar topologia**.
4. Faça clique sobre a seta ao lado da opção **Topologia de replicação** para expandir a lista de servidores.
5. Faça clique sobre a seta ao lado da opção **servidor1** para expandir a lista de servidores.
6. Faça clique sobre a seta ao lado da opção **servidor2** para expandir a lista de servidores.
7. Faça clique sobre **servidor1** e sobre **Adicionar réplica**. Crie o servidor4. Consulte "Criar um servidor de réplica" na página 117.Siga o mesmo procedimento para criar o servidor5. As funções do servidor são representadas por símbolos da ferramenta de administração da Web. A sua topologia passa a ser:
   - servidor1 (principal)
     - servidor2 (reencaminhador)
       - servidor3 (réplica)
     - servidor4 (réplica)
     - servidor5 (réplica)
8. Faça clique sobre **servidor2** e faça clique sobre **Adicionar réplica** para criar o servidor6.
9. Faça clique sobre **servidor4** e sobre **Adicionar réplica** para criar o servidor7. Siga o mesmo procedimento para criar o servidor8. A sua topologia passa a ser:

- servidor1 (principal)
  - servidor2 (reencaminhador)
    - servidor3 (réplica)
    - servidor6 (réplica)
  - servidor4 (reencaminhador)
    - servidor7 (réplica)
    - servidor8 (réplica)
  - servidor5 (réplica)

10. Seleccione **servidor5** e faça clique sobre **Mover**.

    Nota: O servidor que pretende mover tem de ser uma réplica terminal sem réplicas subordinadas.
11. Seleccione **Topologia de replicação** para promover a réplica a servidor principal. Faça clique sobre **Mover**.
12. É apresentado o **painel Criar acordos adicionais de fornecedores**. A replicação de unidade requer que cada servidor principal seja fornecedor e consumidor de cada um dos outros servidores principais da topologia e de cada uma das réplicas de primeiro nível, o servidor2 e servidor4. O servidor5 já é consumidor do servidor1 e agora terá de se tornar fornecedor do servidor1, servidor2 e servidor4. Certifique-se de que os quadrados de acordos de fornecedores estão marcados relativamente a:

Tabela 3.

	Fornecedor	Consumidor
✓	servidor5	servidor1
✓	servidor5	servidor2
✓	servidor5	servidor4

Faça clique sobre **Continuar**.

Nota: Em certos casos o painel Seleccionar credenciais aparece a pedir uma credencial que se encontra num local diferente de cn=replicação,cn=sistcentrallocal. Nestas situações, é necessário fornecer um objecto credencial que se encontre num local diferente decn=replicação,cn=sistcentrallocal. Seleccione as credenciais que a sub-árvore vai utilizar nos conjuntos de credenciais existentes ou crie novas credenciais. Consulte o tópico "Criar credenciais" na página 115.

.

13. Faça clique sobre **OK**.A sua topologia passa a ser:
    - servidor1 (principal)
      - servidor2 (reencaminhador)
        - servidor3 (réplica)
        - servidor6 (réplica)
      - servidor4 (reencaminhador)
        - servidor7 (réplica)
        - servidor8 (réplica)
      - servidor5 (principal)
    - servidor5 (principal)
      - servidor1 (principal)
      - servidor2 (reencaminhador)
      - servidor4 (reencaminhador)

14. Copie dados do servidor1 para todos os servidores. Consulte “Copiar dados para a réplica” na página 118 para obter informações sobre como fazê-lo.

Gerir topologias

As topologias são específicas das sub-árvores replicadas.

- “Ver a topologia”
- “Adicionar uma réplica”
- “Editar um acordo”
- “Mover ou promover um servidor”
- “Despromover um servidor principal” na página 126
- “Replicar uma sub-árvore” na página 126
- “Editar uma sub-árvore” na página 126
- “Remover uma sub-árvore” na página 127
- “Desactivar a sub-árvore” na página 127
- “Editar listas de controlo de acesso” na página 127

Ver a topologia

Nota: O servidor tem de estar a funcionar para que esta tarefa possa ser executada.

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir topologia**.

1. Seleccione a sub-árvore que pretende ver e faça clique sobre **Mostrar topologia**.

A topologia é apresentada na lista Topologia de replicação. Expanda as topologias fazendo clique sobre os triângulos azuis. A partir da lista, pode:

- Adicionar uma réplica.
- Editar as informações numa réplica existente.
- Mudar a réplica para um servidor fornecedor diferente ou promova a réplica a servidor principal.
- Eliminar uma réplica.

Adicionar uma réplica

Consulte “Criar um servidor de réplica” na página 117.

Editar um acordo

Pode alterar as seguintes informações da réplica:

No separador **Servidor**, só pode alterar:

- Nome do sistema central
- Porta
- Activar SSL
- Descrição

No separador **Adicional**, pode alterar:

- Credenciais - consulte “Criar credenciais” na página 115.
- Marcações de replicação - consulte “Criar marcações de replicação” na página 129.
- Altere as capacidades replicadas para a réplica do consumidor. Na lista de capacidades do fornecedor, pode desmarcar quaisquer capacidades que não pretenda replicar para o consumidor.
- Quando terminar, faça clique em **OK**.

Mover ou promover um servidor

1. Seleccione o servidor que pretende e faça clique sobre **Mover**.

2. Seleccione o servidor para o qual pretende mover a réplica ou seleccione **Topologia de replicação** para promover a réplica a servidor principal. Faça clique sobre **Mover**.
3. Em certos casos o painel Seleccionar credenciais aparece a pedir uma credencial que se encontra num local diferente de cn=replicação,cn=sistcentrallocal. Nestas situações, é necessário fornecer um objecto credencial que se encontre num local diferente decn=replicação,cn=sistcentrallocal. Seleccione as credenciais que a sub-árvore vai utilizar nos conjuntos de credenciais existentes ou crie novas credenciais. Consulte "Criar credenciais" na página 115.
4. É apresentado **Criar acordos adicionais de fornecedores**. Seleccione os acordos de fornecedores apropriados para a função do servidor. Por exemplo, se um servidor de réplica for promovido a servidor de unidade, tem de seleccionar a criação de acordos de fornecedores com todos os outros servidores e as respectivas réplicas de primeiro nível. Estes acordos permitem que o servidor promovido funcione como fornecedor dos outros servidores e das respectivas réplicas. Os acordos de fornecedores existentes provenientes dos outros servidores para o servidor recém-promovido continuam em vigor e não é necessário recriá-los.
5. Faça clique sobre **OK**.

A alteração na árvore da topologia reflecte a deslocação do servidor.

Consulte a secção "Criar uma topologia complexa com a replicação de unidade" na página 122 para obter mais informações.

Despromover um servidor principal

Para alterar a função de um servidor de principal para réplica, proceda do seguinte modo:

1. Ligue a ferramenta de administração da Web ao servidor que pretende despromover.
2. Faça clique sobre **Gerir topologia**.
3. Seleccione a sub-árvore e faça clique sobre **Mostrar topologia**.
4. Elimine todos os acordos referentes ao servidor que pretende despromover.
5. Seleccione o servidor que está a despromover e faça clique sobre **Mover**.
6. Seleccione o servidor sob o qual pretende colocar o servidor despromovido e faça clique sobre **Mover**.
7. Tal como faria para qualquer nova réplica, crie novos acordos de fornecedores entre o servidor despromovido e respectivo fornecedor. Consulte "Criar um servidor de réplica" na página 117 para obter instruções.

Replicar uma sub-árvore

Nota: O servidor tem de estar a funcionar para que esta tarefa possa ser executada.

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir topologia**.

- Faça clique sobre **Adicionar sub-árvore**.
- Introduza o DN da sub-árvore que pretende replicar ou faça clique sobre **Procurar** para expandir as entradas de modo a seleccionar a entrada que deverá ser a raiz da sub-árvore.
- Introduza o URL de referência do servidor principal. Este tem de estar no formato de um URL de LDAP como, por exemplo:

  `ldap://<meuservidor>.<minhalocalização>.<minhaempresa>.com`
- Faça clique sobre **OK**.
- O novo servidor é apresentado no painel Gerir topologia, sob o título **Sub-árvores replicadas**.

Editar uma sub-árvore

Utilize esta opção para alterar o URL do servidor principal para o qual esta sub-árvore e as respectivas réplicas enviam actualizações. Terá de executar esta operação se alterar o número da porta ou o nome de sistema central do servidor principal ou mudar o servidor principal para outro servidor

1. Seleccione a sub-árvore que pretende editar.

2. Faça clique sobre **Editar sub-árvore**.
3. Introduza o URL de referência do servidor principal. Este tem de estar no formato de um URL de LDAP como, por exemplo:

   ldap://<*meunovoservidor*>.<*minhalocalização*>.<*minhaempresa*>.com

Dependendo da função que estiver a ser executada pelo servidor nesta sub-árvore (quer se trate de um servidor principal, de réplica ou de reencaminhamento), aparecem diferentes etiquetas e botões no painel.

- Quando a função da sub-árvore for réplica, será apresentada uma etiqueta a indicar que o servidor está a funcionar como uma réplica ou reencaminhador, juntamente com o botão **Tornar servidor num servidor principal**. Se este botão for premido, o servidor ao qual a ferramenta de administração da Web está ligada torna-se num servidor principal.
- Quando a sub-árvore é configurada para replicação apenas através da adição da classe auxiliar (sem nenhum grupo assumido e sub-entrada presentes), a etiqueta **Esta sub-árvore não está replicada** é apresentada juntamente com o botão **Replicar sub-árvore**. Se este botão for premido, o grupo assumido e a sub-entrada são adicionados de modo a que o servidor ao qual a ferramenta de administração da Web está ligada se torne num servidor principal.
- Se não forem encontradas sub-entradas dos servidores principais, a etiqueta **Não está definido nenhum servidor principal para esta sub-árvore** é apresentada juntamente com o botão intitulado **Tornar servidor num servidor principal**. Se este botão for premido, a sub-entrada em falta será adicionada de modo a que o servidor ao qual a ferramenta de administração da Web está ligada se torne num servidor principal.

Remover uma sub-árvore

1. Seleccione a sub-árvore que pretende remover.
2. Faça clique sobre **Eliminar sub-árvore**.
3. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.

A sub-árvore é removida da lista **Sub-árvore replicada**.

Nota: Esta operação só terá êxito se a entrada ibm-replicaGroup=default estiver vazia.

Desactivar a sub-árvore

Esta função é útil quando pretender executar a manutenção ou efectuar alterações à topologia. Minimiza o número de actualizações que podem ser executadas no servidor. Um servidor inactivo não aceita pedidos de clientes. Só aceita pedidos de um administrador que utilize o controlo de Administração do Servidor.

Esta função é Booleana.

1. Faça clique sobre **Desactivar/Activar** para desactivar a sub-árvore.
2. Quando lhe for pedido que confirme a acção, faça clique sobre **OK**.
3. Faça clique sobre **Desactivar/Activar** para desactivar a sub-árvore.
4. Quando lhe for pedido que confirme a acção, faça clique sobre **OK**.

Editar listas de controlo de acesso

As informações sobre replicação (sub-entradas de réplica, acordos de replicação, marcações, possivelmente, credenciais) estão armazenadas sob um objecto especial **ibm-replicagroup=default**. O objecto ibm-replicagroup está localizado imediatamente abaixo da entrada raiz da sub-árvore replicada. Por valor assumido, esta sub-árvore herda a ACL da entrada raiz da sub-árvore replicada. Esta ACL pode não ser apropriada para controlar o acesso às informações de replicação.

Autoridades necessárias:

- Replicação de controlo - Tem de ter acesso de escrita para o objectoibm-replicagroup=default (ou ser o proprietário/administrador).

- Replicação de controlo em cascata - Tem de ter acesso de escrita para o objectoibm-replicagroup=default (ou ser o proprietário/administrador).
- Fila de controlo - Tem de ter acesso de escrita para o acordo de replicação.

Para ver propriedades de ACL utilizando a ferramenta de administração da Web e para trabalhar com ACLs, consulte “Gerir listas de controlo de acesso (ACLs)” na página 162.

Consulte “Listas de controlo de acesso” na página 51 para obter informações adicionais.

Modificar propriedades de replicação

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir propriedades de replicação**. Tem de iniciar sessão na Ferramenta de Administração da Web como um utilizador projectado do i5/OS com as autoridades especiais *ALLOBJ e *IOSYSCFG, para que a opção Manage replication properties (Gerir propriedades de replicação) seja apresentada.

Neste painel, pode:

- Altere o número máximo de alterações pendentes a devolver pelas consultas de estado da replicação. O valor assumido é 200.
- Adicione, edite ou elimine informações sobre o fornecedor.

  Nota: O DN do fornecedor pode ser o DN de um perfil de utilizador projectado do i5/OS. O perfil de utilizador projectado do i5/OS não pode ter autoridade administrativa de LDAP. O utilizador não pode ter as autoridades especiais *ALLOBJ e *IOSYSCFG, nem lhe pode ter sido concedida autoridade administrativa através do ID de aplicação do administrador do Directory Server.

Para obter mais informações, consulte:

- “Adicionar informações sobre o fornecedor”
- “Editar informações do fornecedor” na página 129
- “Remover informações sobre o fornecedor” na página 129

Adicionar informações sobre o fornecedor

1. Faça clique sobre **Adicionar**.
2. Seleccione um fornecedor no menu de selecção ou introduza o nome da sub-árvore replicada que pretende adicionar como fornecedor.
3. Introduza o DN de ligação da replicação para as credenciais.

   Nota: Pode utilizar qualquer uma destas opções, dependendo do seu caso.
   - Defina o DN (e a palavra-passe) de ligação da replicação e uma referência assumida para todas as sub-árvores replicadas para um servidor utilizando as ’credenciais e referência assumidas’. Estes podem ser utilizados quando todas as sub-árvores são replicadas a partir do mesmo fornecedor.
   - Defina o DN e a palavra-passe de ligação da replicação independentemente para cada sub-árvore replicada adicionando informações sobre o fornecedor para cada sub-árvore. Este procedimento pode ser utilizado quando cada sub-árvore tem um fornecedor diferente (ou seja, um servidor principal diferente para cada sub-árvore).
4. Dependendo do tipo de credencial, introduza e confirme a palavra-passe da credencial. (Esta palavra-passe foi registada anteriormente para utilização futura.)
   - **Ligação Simples** - especifique o DN e a palavra-passe
   - **Kerberos** - especifique um pseudo-DN no formato ’ibm-kn=nome-serviço-LDAP@domínio’ sem uma palavra-passe
   - **SSL c/ ligação EXTERNA** - especifique o DN do sujeito para o certificado, sem palavra-passe

Consulte “Criar credenciais” na página 115.

5. Faça clique sobre **OK**.

A sub-árvore do fornecedor é adicionada à lista de Informações do fornecedor.

Editar informações do fornecedor

1. Seleccione a sub-árvore de fornecedores que pretende editar.
2. Faça clique sobre **Editar**.
3. Se estiver a editar **Credenciais e referências assumidas**, que é utilizado para criar a entrada cn=Servidor Principal sob cn=configuração, introduza o URL do servidor do qual o cliente pretende receber actualizações de réplica no campo URL de LDAP do fornecedor assumido. Este URL de LDAP tem de ser válido (ldap://). Caso contrário, passe para o passo 4.
4. Introduza o DN de ligação da replicação para as novas credenciais que pretende utilizar.
5. Introduza e confirme a palavra-passe das credenciais.
6. Faça clique sobre **OK**.

Remover informações sobre o fornecedor

1. Seleccione a sub-árvore de fornecedores que pretende remover.
2. Faça clique sobre **Eliminar**.
3. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.

A sub-árvore é removida da lista Informações do fornecedor.

Criar marcações de replicação

Opcionalmente, pode definir marcações de replicação para horas específicas ou pode determinar que a replicação não deve ocorrer noutras horas. Se não utilizar uma marcação, o servidor marcará a replicação sempre que for efectuada uma alteração. Isto equivale a especificar uma marcação em que a replicação começa automaticamente todos os dias às 12:00.

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir marcações**.

No separador **Marcação semanal**, seleccione a sub-árvore para a qual pretende criar uma marcação e faça clique sobre **Mostrar marcações**. Se já existirem marcações, elas serão apresentadas na caixa **Marcações semanais**. Para criar ou adicionar uma nova marcação:

1. Faça clique sobre **Adicionar**.
2. Introduza um nome para a marcação. Por exemplo, **marcação1**.
3. Para cada dia, de Domingo a Sábado, a marcação diária é especificada como **Nenhuma**. Isto significa que não estão marcadas actualizações à replicação. O último acontecimento de replicação, se existir, ainda está em vigor. Uma vez que se trata de uma nova réplica, não existem acontecimentos de replicação anteriores. Assim, a marcação tem como valor assumido a replicação imediata.
4. Pode seleccionar um dia e fazer clique sobre **Adicionar uma marcação diária** para criar uma marcação de replicação diária para esse dia. Se criar uma marcação diária, ela torna-se na marcação assumida para cada dia da semana. Pode:
   - Manter a marcação diária como valor assumido para cada dia ou seleccionar um dia específico e voltar a alterar a marcação para nenhuma. Não se esqueça de que o último acontecimento de replicação ocorrido ainda se encontra em vigor num dia para o qual não foram marcados acontecimentos de replicação.
   - Modificar a marcação diária seleccionando um dia e fazendo clique sobre **Editar uma marcação diária**. Não se esqueça de que as alterações a uma marcação diária afectam todos os dias abrangidos por essa marcação e não apenas os dias seleccionados.

- Criar uma marcação diária diferente seleccionando um dia e fazendo clique sobre **Adicionar uma marcação diária**. Após ter criado esta marcação, ela será adicionada ao menu de selecção **Marcação diária**. Tem de seleccionar esta marcação para cada dia em que pretende que a mesma seja utilizada.

Consulte "Criar uma marcação diária" para obter mais informações sobre a configuração de marcações diárias.

5. Quando terminar, faça clique em **OK**.

Criar uma marcação diária

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir marcações**.

No separador **Marcação diária**, seleccione a sub-árvore para a qual pretende criar a marcação e faça clique sobre **Mostrar marcações**. Se já existirem marcações, elas serão apresentadas na caixa **Marcações diárias**. Para criar ou adicionar uma nova marcação:

1. Faça clique sobre **Adicionar**.
2. Introduza um nome para a marcação. Por exemplo, **segundafeira1**.
3. Seleccione a definição do fuso horário, ou UTC ou local.
4. Seleccione um tipo de replicação no menu de selecção:

   Imediata
   Executa todas as actualizações pendentes em entradas desde o último acontecimento de replicação e, em seguida, actualiza entradas continuamente até ao próximo acontecimento de actualização marcado.

   Uma vez
   Executa todas as actualizações pendentes anteriores à hora de início. Todas as actualizações efectuadas após a hora de início aguardarão o acontecimento de replicação marcado seguinte.
5. Seleccione uma hora de início para o acontecimento de replicação.
6. Faça clique sobre **Adicionar**. São apresentados o tipo e a hora do acontecimento de replicação.
7. Adicione ou remova acontecimentos de modo a completar a sua marcação. A lista de acontecimentos é actualizada por ordem cronológica.
8. Quando terminar, faça clique em **OK**.

Por exemplo:

Tabela 4.

Tipo de replicação	Hora de início
Imediata	00:00
Uma vez	10:00
Uma vez	14:00
Imediata	16:00
Uma vez	20:00

Nesta marcação, o primeiro acontecimento de replicação ocorre à meia-noite e actualiza todas as alterações pendentes anteriores a essa hora. As actualizações à replicação continuam a ocorrer até às 10:00. As actualizações efectuadas entre as 10:00 e as 14:00 aguardam pelas 14:00 para serem replicadas. Todas as actualizações efectuadas entre as 14:00 e as 16:00 aguardam o acontecimento de replicação marcado para as 16:00 e, em seguida, as actualizações à replicação continuam até ao próximo acontecimento de replicação, marcado para as 20:00. Todas as actualizações efectuadas após as 20:00 aguardam o próximo acontecimento de replicação marcado.

Nota: Se os acontecimentos de replicação forem marcados com um intervalo demasiado curto entre cada um, é possível que um deles seja ignorado, caso as actualizações ao acontecimento anterior ainda estejam em curso quando chegar a hora de marcação do acontecimento seguinte.

Gerir filas

Esta tarefa permite supervisionar o estado de replicação para cada acordo de replicação (fila) utilizado por este servidor.

Expanda a categoria **Gestão de replicações** na área de navegação e faça clique sobre **Gerir filas**.

Seleccione a réplica cuja fila pretende gerir.

- Dependendo do estado da réplica, pode fazer clique sobre **Suspender/retomar**, para parar ou iniciar a replicação.
- Faça clique sobre **Forçar replicação** para replicar todas as alterações pendentes seja qual for a hora para a qual está marcada a próxima replicação.
- Faça clique sobre **Detalhes da fila** para obter informações mais completas sobre a fila da réplica. Também pode gerir a fila a partir desta selecção.
- Faça clique sobre **Actualizar** para actualizar as filas e limpar mensagens do servidor.

Detalhes da fila

Se tiver feito clique sobre **Detalhes da fila**, são apresentados três separadores:

- Estado
- Detalhes da última tentativa
- Alterações pendentes

O separador **Estado** apresenta o nome da réplica, a respectiva sub-árvore, o estado e um registo das horas da replicação. Neste painel, pode suspender ou retomar a replicação fazendo clique sobre **Retomar**. Faça clique sobre **Actualizar** para actualizar as informações da fila.

O separador **Detalhes da última tentativa** fornece informações sobre a última tentativa de actualização. Se não conseguir carregar uma entrada, prima **Ignorar entrada de bloqueio** para continuar a replicação com a entrada pendente seguinte. Faça clique sobre **Actualizar** para actualizar as informações da fila.

O separador **Alterações pendentes** mostra todas as alterações pendentes à réplica. Se a replicação estiver bloqueada, pode eliminar todas as alterações pendentes fazendo clique sobre **Ignorar todas**. Faça clique sobre **Actualizar** para actualizar a lista de alterações pendentes de modo a reflectir qualquer nova actualização ou as actualizações que foram processadas.

Nota: Se optar por ignorar as alterações de bloqueio, terá de assegurar que o servidor consumidor está actualizado. Consulte a secção “ldapdiff” na página 198 para obter mais informações.

Activar SSL no Directory Server

Se tiver o Gestor de Certificados Digitais instalado no sistema, pode utilizar a segurança de Secure Sockets Layer (SSL) para proteger o acesso ao seu Directory Server. Antes de activar o SSL no Directory Server, talvez seja conveniente ler “Secure Sockets Layer (SSL) e Transport Layer Security com o Directory Server” na página 44.

Para utilizar uma ligação por SSL ao administrar o Directory Server a partir do iSeries Navigator, ou para utilizar SSL com o cliente de LDAP do Windows, tem de ter um dos produtos de Client Encryption (5722CE2 ou 5722CE3) instalado no PC.

Para activar o SSL no seu servidor de LDAP, proceda do seguinte modo:

1. **Associar um certificado ao Directory Server**

a. Se pretender gerir o Directory Server através de uma ligação por SSL do iSeries Navigator, consulte o iSeries Access for Windows User's Guide (que é, opcionalmente, instalado no PC aquando da instalação do iSeries Navigator). Se tenciona permitir ligações por SSL e sem ser por SSL ao Directory Server, pode ignorar este passo.

b. Inicie o Gestor de Certificados Digitais da IBM. Consulte Iniciar Gestor de Certificados Digitais no tópico "Gestor de Certificados Digitais", para obter mais informações.

c. Se necessitar de obter ou criar certificados, ou ainda configurar ou alterar o seu sistema de certificados, faça-o agora. Consulte Gestor de Certificados Digitais para obter informações sobre a configuração de um sistema de certificados. Existem duas aplicações de servidor e uma aplicação de cliente associadas ao Directory Server. São as seguintes:

   Aplicação do Directory Server
   A aplicação do Directory Server é o próprio servidor.

   Aplicação de publicação do Directory Server
   A aplicação de publicação do Directory Server identifica o certificado utilizado pela publicação.

   Aplicação de cliente do Directory Server
   A aplicação de cliente do Directory Server identifica o certificado assumido utilizado pela aplicação através da utilização das APIs de ILE do cliente de LDAP.

d. Faça clique sobre o botão **Seleccionar um Armazenamento de Certificados**.

e. Seleccione ***SYSTEM**. Faça clique em **Continue** (Continuar).

f. Introduza a palavra-passe apropriada para o armazenamento de certificados *SYSTEM. Faça clique sobre **Continuar**.

g. Quando o menu de navegação da esquerda for recarregado, expanda **Gerir Aplicações**.

h. Faça clique sobre **Actualizar atribuição de certificados**.

i. No ecrã seguinte, seleccione a aplicação **Servidor**. Faça clique sobre **Continuar**.

j. Seleccione o **Servidor do Directory Server**.

k. Faça clique sobre **Actualizar Atribuição de Certificados** de modo a atribuir um certificado ao Directory Server a utilizar para estabelecer a respectiva identidade para clientes do iSeries Access para Windows.

   Nota: Se escolher um certificado de uma AC cujo certificado de AC não se encontre na sua base de dados de chaves de clientes do iSeries Access para Windows, terá de o adicionar para poder utilizar o SSL. Termine este procedimento antes de começar esse.

l. Seleccione, na lista, um certificado a atribuir ao servidor.

m. Faça clique sobre **Atribuir Novo Certificado**.

n. O DCM é recarregado para a página **Actualizar Atribuição de Certificados** com uma mensagem de confirmação. Quando acabar de configurar os certificados para o Directory Server, faça clique sobre **Terminado**.

2. **Associar um certificado à publicação do Directory Server**. (passo opcional) Se também pretender activar a publicação a partir do sistema para um Directory Server através de uma ligação por SSL, pode desejar igualmente associar um certificado à publicação do Directory Server. Esta acção identifica o certificado assumido e as ACs fidedignas para aplicações que utilizam as APIs de ILE de LDAP que não especificam o respectivo id de aplicação ou uma base de dados de chaves alternativa.

   a. Inicie o Gestor de Certificados Digitais da IBM.

   b. Faça clique sobre o botão **Seleccionar um Armazenamento de Certificados**.

   c. Seleccione ***SYSTEM**. Faça clique em **Continue** (Continuar).

   d. Introduza a palavra-passe apropriada para o armazenamento de certificados *SYSTEM. Faça clique sobre **Continuar**.

   e. Quando o menu de navegação da esquerda for recarregado, expanda **Gerir Aplicações**.

f. Faça clique sobre **Actualizar atribuição de certificados**.
g. No ecrã seguinte, seleccione a aplicação **Cliente**. Faça clique sobre **Continuar**.
h. Seleccione a **Publicação do Directory Server**.
i. Faça clique sobre **Actualizar Atribuição de Certificados** de modo a atribuir um certificado à publicação do Directory Server que irá estabelecer a respectiva identidade.
j. Seleccione, na lista, um certificado a atribuir ao servidor.
k. Faça clique sobre **Atribuir novo certificado**.
l. O DCM é recarregado para a página **Actualizar Atribuição de Certificados** com uma mensagem de confirmação.

Nota: Estes passos assumem que já está a publicar informações no Directory Server com uma ligação não SSL. Consulte "Publicar informações no Directory Server" na página 167 para obter informações completas sobre a configuração da publicação.

3. **Associar um certificado ao cliente do Directory Server**. (passo opcional) Se tiver outras aplicações que usem ligações por SSL a um Directory Server, também terá de associar um certificado a um cliente do Directory Server.
   a. Inicie o Gestor de Certificados Digitais da IBM.
   b. Faça clique sobre o botão **Seleccionar um Armazenamento de Certificados**.
   c. Seleccione ***SYSTEM**. Faça clique em **Continue** (Continuar).
   d. Introduza a palavra-passe apropriada para o armazenamento de certificados *SYSTEM. Faça clique sobre **Continuar**.
   e. Quando o menu de navegação da esquerda for recarregado, expanda **Gerir Aplicações**.
   f. Faça clique sobre **Actualizar atribuição de certificados**.
   g. No ecrã seguinte, seleccione a aplicação **Cliente**. Faça clique sobre **Continuar**.
   h. Seleccione o **cliente do Directory Server**.
   i. Faça clique sobre **Actualizar Atribuição de Certificados** de modo a atribuir um certificado ao cliente do Directory Server que irá estabelecer a respectiva identidade.
   j. Seleccione, na lista, um certificado a atribuir ao servidor.
   k. Faça clique sobre **Atribuir Novo Certificado**.
   l. O DCM é recarregado para a página **Actualizar Atribuição de Certificados** com uma mensagem de confirmação.

Após a activação de SSL, poderá alterar a porta utilizada pelo Directory Server para ligações seguras.

Activar a autenticação de Kerberos no Directory Server

Se tiver o Serviço de Autenticação de Rede configurado no seu sistema, pode configurar o Directory Server para utilizar a autenticação de Kerberos. A autenticação de Kerberos aplica-se aos utilizadores e ao administrador. Antes de activar o Kerberos no Directory Server, poderá achar útil ler uma descrição geral da utilização do Kerberos com o Directory Server.

Para activar a autenticação de Kerberos, siga estes passos:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
5. Faça clique sobre o separador **Kerberos**.
6. Seleccione **Activar a autenticação de Kerberos**.
7. Especifique outras definições na página **Kerberos** de acordo com a sua situação. Consulte a ajuda online da página para obter informações sobre campos individuais.

Gerir o esquema

Para obter mais informações sobre o esquema, consulte “Esquema” na página 16.

O esquema pode ser gerido com a utilização da ferramenta de administração da Web ou de uma aplicação de LDAP, como ldapmodify, em combinação com ficheiros de LDIF. Quando definir pela primeira vez novas objectclasses ou atributos, pode ser conveniente utilizar a ferramenta de administração da Web. Se tiver de copiar o novo esquema para outros servidores (talvez como parte de um produto ou ferramenta que esteja a implementar), o utilitário ldapmodify pode ser mais útil; consulte “Copiar o esquema para outros servidores” na página 144 para obter mais informações.

Consulte o seguinte para obter mais informações:

Ver classes de objecto

Pode ver as classes de objecto no esquema utilizando a ferramenta de administração da Web, o método preferencial ou a linha de comandos.

Administração da Web

Expanda **Gestão do esquema** na área de navegação e faça clique sobre **Gerir classes de objecto**. É apresentado um painel só de leitura que permite ver as classes de objecto existentes no esquema e as respectivas características. As classes de objecto são apresentadas por ordem alfabética. Pode mover uma página para trás ou para a frente fazendo clique sobre Anterior ou Seguinte. O campo ao lado destes botões identifica a página em que se encontra. Também pode utilizar o menu pendente deste campo para saltar para uma página específica. A primeira classe de objecto listada na página é apresentada com o número de página para o ajudar a localizar a classe de objecto que pretende ver. Por exemplo, se procurar a classe de objecto **person**, deve expandir o menu pendente e deslocar-se para baixo até ver **Página 14 de 16 nsLiServer** e **Página 15 de 16 printerLPR**. Uma vez que person está entre nsLiServer e printerLPR no alfabeto, deve seleccionar Página 14 e fazer clique sobre **Ir Para**.

Também pode ver as classes de objecto ordenadas por tipo. Seleccione **Tipo** e faça clique sobre **Ordenar**. As classes de objecto são ordenadas alfabeticamente de acordo com o tipo, quer seja Abstracto, Auxiliar ou Estrutural. De modo semelhante, pode inverter a ordem da lista seleccionando **Descendente** e fazendo clique sobre **Ordenar**.

Depois de localizar a classe de objecto pretendida, pode ver o respectivo tipo, herança, atributos obrigatórios e atributos opcionais. Expanda os menus pendentes para herança, atributos obrigatórios e atributos opcionais para ver a listagem completa para cada característica.

Pode escolher as operações que pretende executar na classe de objecto na barra de ferramentas da direita, do seguinte modo:

- Adicionar

- Editar
- Copiar
- Eliminar

Quando terminar, faça clique sobre **Fechar** para regressar ao painel **Bem-vindo** do IBM Directory Server.

Linha de comandos

Para ver as classes de objecto contidas no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* objectclasses
```

Adicionar uma classe de objecto

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir classes de objecto**. Para criar uma nova classe de objecto:

1. Faça clique sobre **Adicionar**.

   Nota: Também pode aceder a este painel expandindo **Gestão do esquema** na área de navegação e faça clique sobre **Adicionar uma classe de objecto**.
2. No separador **Propriedades gerais**:
   - Introduza o **Nome da classe de objecto**. Este campo é obrigatório e descreve a função da classe de objecto. Por exemplo, **tempEmployee** para uma classe de objecto utilizada para controlar empregados temporários.
   - Introduza uma **Descrição** da classe de objecto, por exemplo, **Classe de objecto utilizada para empregados temporários**.
   - Introduza o **OID** da classe de objecto. Este campo é obrigatório. Consulte "Identificador de objecto (OID)" na página 27. Se não tiver um OID, pode utilizar o **Nome da classe de objecto** com **-oid** anexado. Por exemplo, se o nome da classe de objecto for **tempEmployee**, o OID será **tempEmployee-oid**. Pode alterar o valor deste campo.
   - Seleccione uma **Classe de objecto superior** na lista de selecção. Esta determina a classe de objecto da qual são herdados outros atributos. Normalmente, a **Classe de objecto superior** é **top**, mas pode ser outra. Por exemplo, uma classe de objecto superior para **tempEmployee** poderia ser **ePerson**.
   - Seleccione um **Tipo de classe de objecto**. Consulte "Classes de objecto" na página 18 para obter informações adicionais sobre tipos de classes de objecto.
   - Faça clique sobre o separador Atributos para especificar os atributos obrigatórios e opcionais para a classe de objecto e ver os atributos herdados, faça clique sobre **OK** para adicionar uma nova classe de objecto ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.
3. No separador **Atributos**:
   - Seleccionar um atributo na lista alfabética de **Atributos disponíveis** e fazer clique sobre **Adicionar aos obrigatórios**, para tornar o atributo obrigatório, ou fazer clique sobre **Adicionar aos opcionais**, para tornar o atributo opcional para a classe de objecto. O atributo é apresentado na lista apropriada de atributos seleccionados.
   - Repita este processo para todos os atributos que pretende seleccionar.
   - Pode mover um atributo de uma lista para outra ou eliminar um atributo das listas seleccionadas seleccionando-o e fazendo clique sobre o botão **Mover para** ou **Eliminar** apropriado.
   - Pode ver as listas de atributos herdados obrigatórios e opcionais. Os atributos herdados baseiam-se na **Classe de objecto superior** seleccionada no separador **Geral**. Não pode alterar os atributos herdados. No entanto, se alterar a **Classe de objecto superior** no separador **Geral**, será apresentado outro conjunto de atributos herdados.

4. Faça clique sobre **OK** para adicionar a nova classe de objecto ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.

Nota: Se tiver feito clique sobre **OK** no separador**Geral** sem adicionar quaisquer atributos, poderá adicionar atributos aditando a nova classe de objecto.

Linha de comandos

Para adicionar uma classe de objecto utilizando a linha de comandos, emita o seguinte comando:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nomeficheiro>
```

em que <*nomeficheiro*>contém:

```
dn: cn=Esquema
changetype: modify
add: objectclasses
objectclasses: ( <minhaClasseobjecto-oid> NAME '<minhaClasseObjecto>' DESC '<Uma classe de objecto
                 que defini para a minha aplicação de LDAP>' SUP '< objectclassinheritance>'
                 <objectclasstype> MAY (<atributo1> $ <atributo2>))
```

Editar uma classe de objecto

Nem todas as alterações ao esquema são permitidas. Consulte “Alterações a esquemas não permitidas” na página 29 para ver restrições às alterações.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir classes de objecto**. Para editar uma classe de objecto:

1. Faça clique sobre o botão ao lado da classe de objecto que pretende editar.
2. Faça clique sobre **Editar**.
3. Seleccione um separador:
   - Utilize o separador **Geral** para:
     - Modifique a **Description** (Descrição).
     - Altere a **Classe de objecto superior**. Seleccione uma Classe de objecto superior na lista de selecção. Esta determina a classe de objecto da qual são herdados outros atributos. Normalmente, a **Classe de objecto superior** é **top**, mas pode ser outra. Por exemplo, uma classe de objecto superior para **tempEmployee** poderia ser **ePerson**.
     - Altere o **Tipo de classe de objecto**. Seleccione um tipo de classe de objecto. Consulte “Classes de objecto” na página 18 para obter informações adicionais sobre tipos de classes de objecto.
     - Faça clique sobre o separador Atributos para alterar os atributos obrigatórios e opcionais da classe de objecto e ver os atributos herdados, faça clique sobre **OK** para aplicar as suas alterações ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar quaisquer alterações.
   - Utilize o separador **Atributos** para:

     Seleccionar um atributo na lista alfabética de **Atributos disponíveis** e fazer clique sobre **Adicionar aos obrigatórios**, para tornar o atributo obrigatório, ou fazer clique sobre **Adicionar aos opcionais**, para tornar o atributo opcional para a classe de objecto. O atributo é apresentado na lista apropriada de atributos seleccionados.

     Repita este processo para todos os atributos que pretende seleccionar.

     Pode mover um atributo de uma lista para outra ou eliminar um atributo das listas seleccionadas seleccionando-o e fazendo clique sobre o botão **Mover para** ou **Eliminar** apropriado.

Pode ver as listas de atributos herdados obrigatórios e opcionais. Os atributos herdados baseiam-se na **Classe de objecto superior** seleccionada no separador **Geral**. Não pode alterar os atributos herdados. No entanto, se alterar a **Classe de objecto superior** no separador **Geral**, será apresentado outro conjunto de atributos herdados.

4. Faça clique sobre **OK** para aplicar as alterações ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.

Linha de comandos

Para ver as classes de objecto contidas no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* objectclasses
```

Para editar uma classe de objecto utilizando a linha de comandos, emita o seguinte comando:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nomeficheiro>
```

em que <*nomeficheiro*>contém:

```
dn: cn=esquema
changetype: modify
replace: objectclasses
objectclasses: ( <minhaClasseobjecto-oid> NAME '<minhaClasseObjecto>' DESC '<Uma classe de objecto
                 que defini para a minha aplicação de LDAP>' SUP '< newsuperiorclassobject>'
                 <newobjectclasstype> MAY (atributo1> $ <atributo2>
                  $ <novoatributo3>) )
```

Copiar uma classe de objecto

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir classes de objecto**. Para copiar uma classe de objecto:

1. Faça clique sobre o botão ao lado da classe de objecto que pretende copiar.
2. Faça clique sobre **Copiar**.
3. Seleccione um separador:
   - Utilize o separador **Geral** para:
     - Modifique o **nome da classe de objecto**. O nome assumido é o nome da classe de objecto copiada, com a palavra COPY anexada. Por exemplo, **tempPerson** é copiado como **tempPersonCOPY**.
     - Modifique a **Description** (Descrição).
     - Modifique o **OID**. O OID assumido é o OID da classe de objecto copiada com a palavra COPY anexada. Por exemplo, **tempPerson-oid** é copiado como **tempPerson-oidCOPY**.
     - Altere a **Classe de objecto superior**. Seleccione uma classe de objecto superior na lista de selecção. Esta determina a classe de objecto da qual são herdados outros atributos. Normalmente, a **Classe de objecto superior** é **top**, mas pode ser outra. Por exemplo, uma classe de objecto superior para **tempEmployeeCOPY** poderia ser **ePerson**.
     - Altere o **Tipo de classe de objecto**. Seleccione um tipo de classe de objecto. Consulte “Classes de objecto” na página 18 para obter informações adicionais sobre tipos de classes de objecto.
     - Faça clique sobre o separador **Atributos** para alterar os atributos obrigatórios e opcionais para a classe de objecto e ver os atributos herdados, faça clique sobre **OK** para aplicar as alterações ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.
   - Utilize o separador **Atributos** para:

     Seleccionar um atributo na lista alfabética de **Atributos disponíveis** e fazer clique sobre **Adicionar aos obrigatórios**, para tornar o atributo obrigatório, ou fazer clique sobre **Adicionar aos opcionais**, para tornar o atributo opcional para a classe de objecto. O atributo é apresentado na lista apropriada de atributos seleccionados.

Repita este processo para todos os atributos que pretende seleccionar.

Pode mover um atributo de uma lista para outra ou eliminar um atributo das listas seleccionadas seleccionando-o e fazendo clique sobre o botão **Mover para** ou **Eliminar** apropriado.

Pode ver as listas de atributos herdados obrigatórios e opcionais. Os atributos herdados baseiam-se na **Classe de objecto superior** seleccionada no separador **Geral**. Não pode alterar os atributos herdados. No entanto, se alterar a **Classe de objecto superior** no separador **Geral**, será apresentado outro conjunto de atributos herdados.

4. Faça clique sobre **OK** para aplicar as alterações ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.

Linha de comandos

Para ver as classes de objecto contidas no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* objectclasses
```

Seleccione a classe de objecto que pretende copiar. Utilize um editor para alterar as informações apropriadas e guarde as alterações em <*nomeficheiro*>. Em seguida, emita o seguinte comando:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nomeficheiro>
```

em que <*nomeficheiro*>contém:

```
dn: cn=esquema
changetype: modify
add: objectclasses
objectclasses: ( <minhanovaClasseobjecto-oid> NAME '<minhanovaClasseObjecto>'
                DESC '<Uma nova classe de objecto
                  que copiei para a minha aplicação de LDAP>'
               SUP '<superiorclassobject>'<objectclasstype> MAY (atributo1>
               $ <atributo2> $ <atributo3>) )
```

Eliminar uma classe de objecto

Nem todas as alterações ao esquema são permitidas. Consulte "Alterações a esquemas não permitidas" na página 29 para ver restrições às alterações.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir classes de objecto**. Para eliminar uma classe de objecto:

1. Faça clique sobre o botão ao lado da classe de objecto que pretende eliminar.
2. Faça clique sobre **Eliminar**.
3. É-lhe pedido que confirme a eliminação da classe de objecto. Faça clique sobre **OK** para eliminar a classe de objecto ou faça clique sobre **Cancelar** para regressar a **Gerir classes de objecto** sem efectuar alterações.

Linha de comandos

Para ver as classes de objecto contidas no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* objectclasses
```

Seleccione a classe de objecto que pretende eliminar e emita o seguinte comando:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nomeficheiro>
```

em que <*nomeficheiro*>contém:

```
dn: cn=esquema
changetype: modify
delete: objectclasses
objectclasses: (<minhaClasseobjecto-oid>)
```

Ver atributos

Pode ver os atributos do esquema utilizando a ferramenta de administração da Web, o método preferencial ou a linha de comandos.

Administração da Web

Expanda **Gestão do esquema** na área de navegação e faça clique sobre **Gerir atributos**. É apresentado um painel só de leitura que lhe permite ver os atributos existentes no esquema e as respectivas características. Os atributos são apresentados por ordem alfabética. Pode mover uma página para trás ou para a frente fazendo clique sobre Anterior ou Seguinte. O campo ao lado destes botões identifica a página em que se encontra. Também pode utilizar o menu pendente deste campo para saltar para uma página específica. A primeira classe de objecto listada na página é apresentada com o número de página para o ajudar a localizar a classe de objecto que pretende ver. Por exemplo, se procurar o atributo **authenticationUserID**, deve expandir o menu pendente e deslocar-se para baixo até ver **Página 3 de 62 applSystemHint** e **Página 4 de 62 authorityRevocatonList**. Uma vez que authenticationUserID está entre applSystemHint e authorityRevocatonList no alfabeto, deve seleccionar Página 3 e fazer clique sobre **Ir Para**.

Também pode ver os atributos ordenados por sintaxe. Seleccione **Sintaxe** e faça clique sobre **Ordenar**. Os atributos são apresentados por ordem alfabética de acordo com a respectiva sintaxe. Consulte “Sintaxe de atributos” na página 26 para obter uma listagem dos tipos de sintaxe. De modo semelhante, pode inverter a ordem da lista seleccionando **Descendente** e fazendo clique sobre **Ordenar**.

Depois de localizar o atributo pretendido, pode ver a respectiva sintaxe, se tem valores múltiplos e as classes de objecto que o contêm. Expanda o menu pendente das classes de objecto para ver a lista de classes de objecto referentes ao atributo.

Quando terminar, faça clique sobre **Fechar** para regressar ao painel **Bem-vindo** do IBM Directory Server.

Linha de comandos

Para ver os atributos contidos no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Adicionar um atributo

Utilize um dos métodos que se seguem para criar um novo atributo. A ferramenta de administração da Web é o método preferencial.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir atributos**. Para criar um novo atributo:

1. Faça clique sobre **Adicionar**.

   Nota: Também pode aceder a este painel expandindo a **Gestão do esquema** na área de navegação e, em seguida, fazendo clique sobre **Adicionar um atributo**.
2. Introduza o **Nome do atributo** como, por exemplo, **tempId**. Este campo é obrigatório e tem de começar por um carácter alfabético.
3. Introduza uma **Descrição** do atributo como, por exemplo, **O número do ID atribuído a um empregado temporário**.

4. Introduza o **OID** do atributo. Este campo é obrigatório. Consulte "Identificador de objecto (OID)" na página 27. Se não tiver um OID, pode utilizar o nome do atributo, com -oid anexado. Por exemplo, se o nome do atributo for **tempID**, o OID assumido será **tempID-oid**. Pode alterar o valor deste campo.
5. Seleccione um **Atributo superior** na lista de selecção. O atributo superior determina o atributo do qual são herdadas propriedades.
6. Seleccione uma **Sintaxe** na lista de selecção. Consulte "Sintaxe de atributos" na página 26 para obter informações adicionais sobre a sintaxe.
7. Introduza um **Comprimento de atributo** que especifique o comprimento máximo deste atributo. O comprimento é expresso como o número de bytes.
8. Seleccione o quadrado de opção **Permitir valores múltiplos** para permitir que o atributo tenha múltiplos valores.
9. Seleccione uma regra de correspondência em cada um dos menus de selecção para as regras de correspondência igualdade, ordenação e subcadeia. Consulte o "Regras de correspondência" na página 24 para obter uma listagem completa de regras de correspondência.
10. Faça clique sobre o separador **Extensões** da IBM para especificar extensões adicionais para o atributo, faça clique sobre **OK** para adicionar o novo atributo ou faça clique sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.
11. No separador **Extensões** da IBM:
    - Modifique o **nome da tabela** da DB2. O servidor gera o nome da tabela da DB2 se este campo for deixado em branco. Se introduzir um nome de tabela da DB2, também terá de introduzir um nome de coluna da DB2.
    - Modifique o **nome de coluna** da DB2. O servidor gera o nome de coluna da DB2 se este campo for deixado em branco. Se introduzir um nome de coluna da DB2, também terá de introduzir um nome de tabela da DB2.
    - Defina a **Classe de segurança** seleccionando **normal**, **sensível** ou **crítica** na lista de selecção.
    - Defina as **Regras de indexação** seleccionando uma ou mais. Consulte "Regras de indexação" na página 25 para obter informações adicionais sobre regras de indexação.

      Nota: No mínimo, recomenda-se que especifique uma indexação de Igualdade ou quaisquer atributos que devam ser utilizados em filtros de procura.
12. Faça clique sobre **OK** para adicionar os novos atributos ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.

Nota: Se tiver feito clique sobre OK no separador Geral sem adicionar quaisquer extensões, poderá adicionar extensões aditando o novo atributo.

Linha de comandos

O exemplo seguinte adiciona uma definição de tipo de atributo a um atributo denominado ″meuAtributo″, com a sintaxe da Cadeia de Directórios(consulte "Sintaxe de atributos" na página 26) e correspondência de Igualdade Não Sensível a Maiúsculas e Minúsculas(consulte "Regras de correspondência" na página 24). A parte da definição específica da IBM indica que os dados do atributo estão armazenados numa coluna denominada ″minhaColunaAtrib″ na tabela ″minhaTabelaAtrib″. Se estes nomes não tiverem sido especificados, tanto o nome da coluna como o da tabela terão como valor assumido ″meuAtributo″. O atributo foi atribuído à classe de acesso″normal″ e os valores têm um comprimento máximo de 200 bytes.

```
ldapmodify -D <admindn> -w <adminpw> -i meuesquema.ldif
```

em que o ficheiro **meuesquema.ldif** contém:

```
dn: cn=esquema
changetype: modify
add: attributetypes
```

```
attributetypes: ( meuAtributo-oid NAME ( 'meuAtributo' )
                  DESC 'Um atributo que defini para a minha aplicação de LDAP'
                  EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
  USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( meuAtributo-oid  DBNAME ( 'minhaTabelaAtrib' 'minhaColunaAtrib' )
                     ACCESS-CLASS normal LENGTH 200 )
```

Consulte “ldapmodify e ldapadd” na página 175 para obter mais informações sobre este comando.

Editar um atributo

Nem todas as alterações ao esquema são permitidas. Consulte “Alterações a esquemas não permitidas” na página 29 para ver restrições às alterações.

Qualquer parte de uma definição pode ser alterada antes de o utilizador ter adicionado entradas que utilizem o atributo. Utilize um dos métodos que se seguem para editar um atributo. A ferramenta de administração da Web é o método preferencial.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir atributos**. Para editar um atributo:

1. Faça clique sobre o botão ao lado do atributo que pretende editar.
2. Faça clique sobre **Editar**.
3. Seleccione um separador:
   - Utilize o separador **Geral** para:
     - Seleccione um separador, que pode ser:
       - **Geral** para:
         - Modificar a **Descrição**
         - Alterar a **Sintaxe**
         - Definir o **Comprimento do atributo**
         - Alterar as definições de **Valores múltiplos**
         - Seleccionar uma **Regra de correspondência**
         - Alterar o **Atributo superior**
       - Faça clique sobre o separador **Extensões** da IBM para editar as extensões para o atributo, sobre **OK** para aplicar as suas alterações ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.
       - ou **Extensões** da IBM, se estiver a utilizar o IBM Directory Server para:
         - Alterar a **Classe de segurança**
         - Alterar as **Regras de indexação**
     - Faça clique sobre **OK** para aplicar as suas alterações ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.
4. Faça clique sobre **OK** para aplicar as alterações ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.

Linha de comandos

Este exemplo adiciona indexação ao atributo, para acelerar as procuras nele efectuadas. Utilize o comando ldapmodify e o ficheiro de LDIF para alterar a definição:

```
ldapmodify -D <admindn> -w <adminpw> -i alteraçãomeuesquema.ldif
```

em que o ficheiro **alteraçãomeuesquema.ldif** contém:

```
dn: cn=esquema
changetype: modify
replace: attributetypes
attributetypes: ( meuAtributo-oid NAME ( 'meuAtributo' ) DESC 'Um atributo
                 que defini para a minha aplicação de LDAP'  EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( meuAtributo-oid  DBNAME ( 'minhaTabelaAtrib' 'minhaColunaAtrib' )
                  ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Nota: Ambas as partes da definição (**attributetypes** e **ibmattributetypes**) têm de ser incluídas na operação substituir, mesmo que a secção **ibmattributetypes** seja alterada. A única alteração é a adição de ″EQUALITY SUBSTR″ ao fim da definição de modo a pedir índices para fins de igualdade e correspondência de subcadeias.

Consulte “ldapmodify e ldapadd” na página 175 para obter mais informações sobre este comando.

Copiar um atributo

Utilize um dos métodos que se seguem para copiar um atributo. A ferramenta de administração da Web é o método preferencial.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir atributos**. Para copiar um atributo:

1. Faça clique sobre o botão ao lado do atributo que pretende copiar.
2. Faça clique sobre **Copiar**.
3. Modifique o **Nome do atributo**. O nome assumido é o nome do atributo copiado, com a palavra COPY anexada. Por exemplo, **tempID** é copiado como **tempIDCOPY**.
4. Modifique uma **Descrição** do atributo como, por exemplo, **O número do ID atribuído a um empregado temporário**.
5. Modifique o **OID**. O OID assumido é o OID do atributo copiado, com a palavra COPYOID anexada. Por exemplo, **tempID-oid** é copiado como **tempID-oidCOPYOID**.
6. Seleccione um **Atributo superior** na lista de selecção. O atributo superior determina o atributo do qual são herdadas propriedades.
7. Seleccione uma **Sintaxe** na lista de selecção. Consulte “Sintaxe de atributos” na página 26 para obter informações adicionais sobre a sintaxe.
8. Introduza um **Comprimento de atributo** que especifique o comprimento máximo deste atributo. O comprimento é expresso como o número de bytes.
9. Seleccione o quadrado de opção **Permitir valores múltiplos** para permitir que o atributo tenha múltiplos valores.
10. Seleccione uma regra de correspondência em cada um dos menus de selecção para as regras de correspondência igualdade, ordenação e subcadeia. Consulte o “Regras de correspondência” na página 24 para obter uma listagem completa de regras de correspondência.
11. Faça clique sobre o separador**Extensões** da IBM para modificar extensões adicionais para o atributo, sobre **OK** para aplicar as suas alterações ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.
12. No separador **Extensões** da IBM:
    - Modifique o **nome da tabela** da DB2. O servidor gera o nome da tabela da DB2 se este campo for deixado em branco. Se introduzir um nome de tabela da DB2, também terá de introduzir um nome de coluna da DB2.

- Modifique o **nome de coluna** da DB2. O servidor gera o nome de coluna da DB2 se este campo for deixado em branco. Se introduzir um nome de coluna da DB2, também terá de introduzir um nome de tabela da DB2.
- Modifique a **Classe de segurança** seleccionando **normal**, **sensível** ou **crítica** na lista de selecção.
- Modifique as **Regras de indexação** seleccionando uma ou mais. Consulte "Regras de indexação" na página 25 para obter informações adicionais sobre regras de indexação.

  Nota: No mínimo, recomenda-se que especifique uma indexação Igual em todos os atributos que deverão ser utilizados em filtros de procura.

13. Faça clique sobre **OK** para aplicar as suas alterações ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.

Nota: Se tiver feito clique sobre **OK** no separador **Geral** sem adicionar quaisquer extensões, poderá adicionar ou modificar extensões editando o novo atributo.

Linha de comandos

Para ver os atributos contidos no esquema, emita o comando:

```
ldapsearch -b cn=esquema -s base objectclass=* attributeTypes IBMAttributeTypes
```

Seleccione o atributo que pretende copiar. Utilize um editor para alterar as informações apropriadas e guarde as alterações em <*nomeficheiro*>. Em seguida, emita o seguinte comando:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nomeficheiro>
```

em que <*nomeficheiro*>contém:

```
dn: cn=esquema
changetype: modify
add: attributetypes
attributetypes: ( <meunovoAtributo-oid> NAME '<meunovoAtributo>' DESC '<Um novo
                atributo que copiei para a minha aplicação de LDAP> EQUALITY 2.5.13.2
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( meuAtributo-oid  DBNAME ( 'minhaTabelaAtrib' 'minhaColunaAtrib' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Eliminar um atributo

Nem todas as alterações ao esquema são permitidas. Consulte "Alterações a esquemas não permitidas" na página 29 para ver restrições às alterações.

Utilize um dos métodos que se seguem para eliminar um atributo. A ferramenta de administração da Web é o método preferencial.

Administração da Web

Se ainda não o tiver feito, expanda **Gestão do esquema** na área de navegação e, em seguida, faça clique sobre **Gerir atributos**. Para eliminar um atributo:

1. Faça clique sobre o botão ao lado do atributo que pretende eliminar.
2. Faça clique sobre **Eliminar**.
3. É-lhe pedido que confirme a eliminação do atributo. Faça clique sobre **OK** para eliminar o atributo ou sobre **Cancelar** para regressar a **Gerir atributos** sem efectuar alterações.

Linha de comandos

```
ldapmodify -D <admindn> -w <adminpw> -i eliminaçãomeuesquema.ldif
```

Em que o ficheiro **eliminaçãomeuesquema.ldif** inclui:

```
dn: cn=esquema
changetype: modify
delete: attributetypes
attributetypes: (<meuAtributo-oid>)
```

Consulte “ldapmodify e ldapadd” na página 175 para obter mais informações sobre este comando.

Copiar o esquema para outros servidores

Para copiar um esquema para outros servidores, proceda do seguinte modo:

1. Use o utilitário ldapsearch para copiar o esquema para um ficheiro:

   ```
   ldapsearch -b cn=esquema -L "(objectclass=*)" > esquema.ldif
   ```

2. O ficheiro do esquema incluirá todas as objectclasses e atributos. Edite o ficheiro de LDIF para incluir apenas os elementos do esquema que pretende; talvez possa filtrar o output de ldapsearch utilizando uma ferramenta como ″grep″. Lembre-se de colocar os atributos antes das objectclasses que lhes fazem referência. Por exemplo, pode acabar por obter o seguinte ficheiro (note que cada linha continuada tem um único espaço no fim e que a linha de continuação tem, pelo menos, um espaço no início).

   ```
   attributetypes: ( meuatrib1-oid NAME 'meuatrib1' DESC 'Algumas
     informações.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( meuatrib1-oid DBNAME( 'meuatrib1'  'meuatrib1' )
     ACCESS-CLASS normal LENGTH 500 )
   attributetypes: ( meuatrib2-oid NAME 'meuatrib2' DESC 'Algumas
     informações.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( meuatrib2-oid DBNAME( 'meuatrib2'  'meuatrib2' )
     ACCESS-CLASS normal LENGTH 500 )
   objectclasses: ( meuobjecto-oid NAME 'meuobjecto' DESC 'Representa
     algo.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( meuatrib1 $ meuatrib2 ) )
   ```

3. Insira linhas antes de cada linha de objectclass ou attributetype de modo a construir directrizes de LDIF para adicionar estes valores à entrada cn=esquema. Cada classe de objecto e atributo tem de ser adicionado como uma modificação individual.

   ```
   dn: cn=esquema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( meuatrib1-oid NAME 'meuatrib1' DESC 'Algumas
     informações.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( meuatrib1-oid DBNAME( 'meuatrib1'  'meuatrib1' )
     ACCESS-CLASS normal LENGTH 500 )

   dn: cn=esquema
   changetype: modify
   add: attributetypes ibmattributetypes
   attributetypes: ( meuatrib2-oid NAME 'meuatrib2' DESC 'Algumas
     informações.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
     USAGE userApplications )
   IBMAttributetypes: ( meuatrib2-oid DBNAME( 'meuatrib2'  'meuatrib2' )
     ACCESS-CLASS normal LENGTH 500 )

   dn: cn=esquema
   changetype: modify
   add: objectclasses
   objectclasses: ( meuobjecto-oid NAME 'meuobjecto' DESC 'Representa
     algo.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( meuatrib1 $ meuatrib2 ) )
   ```

4. Carregue esse esquema para outros servidores usando o utilitário ldapmodify:

   ```
   ldapmodify -D cn=administrador -w <palavra-passe> -f esquema.ldif
   ```

Gerir entradas de directório

Para gerir entradas de directório, expanda a categoria **Gestão do directório** na área de navegação da ferramenta de administração da Web.

Consulte o seguinte para obter mais informações:

- "Procurar a árvore"
- "Adicionar uma entrada"
- "Eliminar uma entrada" na página 146
- "Editar uma entrada" na página 146
- "Copiar uma entrada" na página 147
- "Editar listas de controlo de acesso" na página 147
- "Adicionar uma classe de objecto auxiliar" na página 147
- "Eliminar uma classe auxiliar" na página 148
- "Alterar a filiação de membros em grupos" na página 148
- "Pesquisar as entradas de directório" na página 148
- "Alterar atributos binários" na página 150

Procurar a árvore

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a entrada em que pretende trabalhar. Pode escolher as operações que pretende executar na barra de ferramentas da direita.

Adicionar uma entrada

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação.

1. Faça clique sobre **Adicionar uma entrada**.
2. Seleccione uma **Classe de objecto estrutural** na lista de selecção.
3. Faça clique sobre **Seguinte**.
4. Seleccione quaisquer **Classes de objecto auxiliares** que deseje utilizar na caixa Disponíveis e faça clique sobre **Adicionar**. Repita este processo para cada classe de objecto auxiliar que pretenda adicionar. Também pode eliminar uma classe de objecto auxiliar da caixa Seleccionadas, seleccionando-a e fazendo clique sobre **Remover**.
5. Faça clique sobre **Seguinte**.
6. No campo **DN Relativo**, introduza o nome exclusivo relativo (RDN) da entrada que está a adicionar como, por exemplo, cn=Joaquim Dias.
7. No campo **DN Ascendente**, introduza o nome exclusivo da entrada da árvore que seleccionou como, por exemplo, ou=Almada, o=IBM. Também pode fazer clique sobre **Procurar** para seleccionar o DN ascendente na lista. Também pode expandir a selecção para ver outras opções mais abaixo na sub-árvore. Especifique as suas opções e faça clique sobre **Seleccionar** para especificar o DN Ascendente que pretende. O **DN Ascendente** tem como valor assumido a entrada seleccionada na árvore.

   Nota: Se tiver iniciado esta tarefa a partir do painel **Gerir entradas**, este campo estará preenchido. Seleccionou o **DN Ascendente** antes de fazer clique sobre **Adicionar** para iniciar o processo de adição da entrada.
8. No separador **Atributos obrigatórios**, introduza os valores dos atributos obrigatórios. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.
9. Faça clique sobre **Atributos opcionais**.

10. No separador **Atributos opcionais**, introduza os valores como for apropriado para os atributos opcionais. Consulte "Alterar atributos binários" na página 150 para obter informações sobre como adicionar valores binários. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.
11. Faça clique sobre OK para criar a entrada.
12. Faça clique sobre o botão **ACL** para modificar a lista de controlo de acesso para esta entrada. Consulte "Listas de controlo de acesso" na página 51 para obter informações sobre ACLs.
13. Depois de preencher, pelo menos, os campos obrigatórios, faça clique sobre **Adicionar** para adicionar a nova entrada ou sobre **Cancelar** para regressar a **Procurar a árvore** sem efectuar alterações ao directório.

Eliminar uma entrada

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a sub-árvore, o sufixo ou a entrada em que pretende trabalhar. Faça clique sobre **Eliminar** na barra de ferramentas da direita.

- É-lhe pedido que confirme a eliminação. Faça clique sobre **OK**.
- A entrada é eliminada e o sistema fá-lo regressar à lista de entradas.

Editar uma entrada

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a entrada em que pretende trabalhar. Faça clique sobre **Editar atributos** na barra de ferramentas da direita.

1. No separador **Atributos obrigatórios**, introduza os valores dos atributos obrigatórios. Consulte "Alterar atributos binários" na página 150 para obter informações sobre como adicionar valores binários. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.
2. Faça clique sobre **Atributos opcionais**.
3. No separador **Atributos opcionais**, introduza os valores como for apropriado para os atributos opcionais. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.
4. Faça clique sobre **Membros de grupos**.
5. Se tiver criado grupos, no separador **Membros de grupos**:
   - Seleccione um grupo em **Grupos disponíveis** e faça clique sobre **Adicionar** para tornar a entrada num membro do **Grupo de membros estático** seleccionado.
   - Seleccione um grupo em **Grupos de membros estáticos** e faça clique sobre **Remover** para remover a entrada do grupo seleccionado.
6. Se a entrada for uma entrada de grupo, estará disponível um separador **Membros**. O separador **Membros** apresenta os membros do grupo seleccionado. Pode adicionar e remover membros do grupo.
   - Para adicionar um membro ao grupo:
     a. Pode fazer clique sobre **Múltiplos valores** ao lado do separador**Membros** ou sobre **Membros** no separador **Membros**.
     b. No campo Membro, introduza o DN da entrada que pretende adicionar.
     c. Faça clique sobre **Adicionar**.
     d. Faça clique sobre **OK**.
   - Para remover um membro do grupo:
     a. Pode fazer clique sobre **Múltiplos valores** ao lado do separador **Membros** ou sobre o separador **Membros** e, em seguida, sobre **Membros**.
     b. Seleccione a entrada que pretende remover.

c. Faça clique sobre **Remover**.
d. Faça clique sobre **OK**.

- Para actualizar a lista de membros, faça clique sobre **Actualizar**.

7. Faça clique sobre **OK** para modificar a entrada.

Copiar uma entrada

Esta função é útil se estiver a criar entradas semelhantes. A cópia herda todos os atributos do original. Tem de efectuar algumas modificações para atribuir um nome à nova entrada.

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a entrada como, por exemplo, Joaquim Dias, em que pretende trabalhar. Faça clique sobre **Copiar** na barra de ferramentas da direita.

- Altere a entrada RDN no campo DN. Por exemplo, altere cn=Joaquim Dias para cn=João Santos.
- No separador de atributos necessário, altere a entrada do cn para o novo RDN. Neste exemplo, João Santos.
- Altere os outros atributos obrigatórios como for apropriado. Neste exemplo, altere o atributo sn de Dias para Silva.
- Quando acabar de efectuar as alterações necessárias, faça clique sobre **OK** para criar a nova entrada.
- A nova entrada João Santos é adicionada ao fim da lista de entradas.

Nota: Este procedimento só copia os atributos da entrada. As filiações de membros em grupos da entrada original não são copiadas para a nova entrada. Utilize a função Editar atributos para adicionar membros de grupos.

Editar listas de controlo de acesso

Para ver propriedades de ACL utilizando a ferramenta de administração da Web e para trabalhar com ACLs, consulte “Gerir listas de controlo de acesso (ACLs)” na página 162.

Consulte “Listas de controlo de acesso” na página 51 para obter informações adicionais.

Adicionar uma classe de objecto auxiliar

Utilize o botão **Adicionar classe auxiliar** da barra de ferramentas para adicionar uma classe de objecto auxiliar a uma entrada existente na árvore de directórios. Uma classe de objecto auxiliar fornece atributos adicionais à entrada à qual é adicionada.

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a entrada como, por exemplo, Joaquim Dias, em que pretende trabalhar. Faça clique sobre **Adicionar classe auxiliar** na barra de ferramentas da direita.

1. Seleccione quaisquer **Classes de objecto auxiliares** que deseje utilizar na caixa Disponíveis e faça clique sobre **Adicionar**. Repita este processo para cada classe de objecto auxiliar que pretenda adicionar. Também pode eliminar uma classe de objecto auxiliar da caixa Seleccionadas, seleccionando-a e fazendo clique sobre **Remover**.
2. No separador **Atributos obrigatórios**, introduza os valores dos atributos obrigatórios. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.
3. Faça clique sobre **Atributos opcionais**.
4. No separador **Atributos opcionais**, introduza os valores como for apropriado para os atributos opcionais. Se pretender adicionar mais de um valor para um atributo específico, faça clique sobre **Múltiplos valores** e, em seguida, adicione os valores um de cada vez.

5. Faça clique sobre **Membros de grupos**.
6. Se tiver criado grupos, no separador **Membros de grupos**:
   - Seleccione um grupo em **Grupos disponíveis** e faça clique sobre **Adicionar** para tornar a entrada num membro do **Grupo de membros estático** seleccionado.
   - Seleccione um grupo em **Grupos de membros estáticos** e faça clique sobre **Remover** para remover a entrada do grupo seleccionado.
7. Faça clique sobre **OK** para modificar a entrada.

Eliminar uma classe auxiliar

Embora possa eliminar uma classe auxiliar durante o procedimento para adicionar uma classe auxiliar, é mais fácil utilizar a função eliminar classe auxiliar se pretender eliminar uma única classe auxiliar de uma entrada. No entanto, pode ser mais conveniente utilizar o procedimento para adicionar uma classe auxiliar se pretender eliminar várias classes auxiliares de uma entrada.

1. Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação e, em seguida, faça clique sobre **Gerir entradas**. Pode expandir as várias sub-árvores e seleccionar a entrada como, por exemplo, Joaquim Dias, em que pretende trabalhar. Faça clique sobre **Eliminar classe auxiliar** na barra de ferramentas da direita.
2. Na lista de classes auxiliares, seleccione a classe que pretende eliminar e prima **OK**.
3. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.
4. A classe auxiliar é eliminada da entrada e o sistema fá-lo regressar à lista de entradas.

Repita estes passos para cada classe auxiliar que pretenda eliminar.

Alterar a filiação de membros em grupos

Se ainda não o tiver feito, expanda a categoria **Gestão do directório** na área de navegação.

1. Faça clique sobre **Gerir entradas**.
2. Seleccione um utilizador na árvore de directórios e faça clique sobre o símbolo **Editar atributos** da barra de ferramentas.
3. Faça clique sobre o separador **Membros de grupos**.
4. Para modificar os membros de grupos para o utilizador. O painel **Alterar membros de grupos** apresenta os**Grupos disponíveis** aos quais o utilizador pode ser adicionado, bem como os **Grupos de Membros Estáticos**.
   - Seleccione um grupo em **Grupos disponíveis** e faça clique sobre **Adicionar** para tornar a entrada num membro do grupo seleccionado.
   - Seleccione um grupo em **Grupos de Membros Estáticos** e faça clique sobre **Remover** para remover a entrada do grupo seleccionado.
5. Faça clique sobre **OK** para guardar as alterações ou sobre **Cancelar** para regressar ao painel anterior sem guardar as alterações.

Pesquisar as entradas de directório

Existem três opções para pesquisar a árvore de directórios:

- Uma procura Simples, com a utilização de um conjunto predefinido de critérios de procura
- Uma procura Avançada, com a utilização de um conjunto de critérios de procura definidos pelo utilizador
- Uma procura Manual

As opções de procura estarão acessíveis se expandir a categoria **Gestão do directório** da área de navegação e se fizer clique sobre **Localizar entradas**. Seleccione o separador **Filtros de procura** ou **Opções**.

Nota: As entradas binárias como, por exemplo, palavras-passe, não podem ser pesquisadas.

Filtros de procura

Seleccione um dos seguintes tipos de procuras:

Procura simples

Uma procura simples utiliza critérios de procura assumidos:

- Um DN Base é **Todos os sufixos**
- O âmbito da procura é **Sub-árvore**
- O tamanho da procura é **Ilimitado**
- O tempo limite é **Ilimitado**
- O reenvio para nomes alternativos é **nunca**
- A busca de referências é desmarcada (desactivada)

Para executar uma procura simples:

1. No separador **Filtro de procura**, faça clique sobre **Procura simples**.
2. Seleccione uma classe de objecto na lista de selecção.
3. Seleccione um atributo específico para o tipo de entrada seleccionado. Se seleccionar a pesquisa num atributo específico, seleccione um atributo na lista de selecção e introduza o valor do atributo na caixa **É igual a**. Se não especificar um atributo, a procura devolverá todas as entradas de directório do tipo de entrada seleccionado.

Procura avançada

Uma procura avançada permite especificar restrições de procura e activar filtros de procura. Utilize a procura Simples para utilizar critérios de procura assumidos.

- Para executar uma procura avançada:
  1. No separador **Filtro de procura**, faça clique sobre **Procura avançada**.
  2. Seleccione um **Atributo** na lista de selecção.
  3. Seleccione um operador de **Comparação**
     - =O atributo é igual ao valor.
     - ! O atributo não é igual ao valor.
     - < O atributo é menor ou igual ao valor.
     - > O atributo é maior ou igual ao valor.
     - ~ O atributo é aproximadamente igual ao valor.
  4. Introduza o **Valor** para comparação.
  5. Utilize os botões do operador de procura para consultas complexas.
     - Se já tiver adicionado, pelo menos, um filtro de procura, especifique os critérios adicionais e faça clique sobre **AND**. O comando **AND** devolve entradas que correspondem a ambos os conjuntos de critérios de procura.
     - Se já tiver adicionado, pelo menos, um filtro de procura, especifique os critérios adicionais e faça clique sobre **OR**. O comando **OR** devolve entradas que correspondem a um dos conjuntos de critérios de procura.
  6.
     - Faça clique sobre **Adicionar** para adicionar os critérios do filtro de procura à procura avançada
     - Faça clique sobre **Eliminar** para remover os critérios do filtro de procura da procura avançada
     - Faça clique sobre **Repor** para limpar todos os filtros de procura.

Procura manual

Utilize este método para criar um filtro de procura. Por exemplo, para procurar em apelidos, introduza `sn=*` no campo. Se estiver a pesquisar múltiplos atributos, terá de utilizar a sintaxe de filtros de procura. Por exemplo, para procurar os apelidos de um departamento específico, deve introduzir:

`(&(sn=*)(dept=<nomedepartamento>))`

Opções

No **separador Opções**:

- **Pesquisar DN base** - Seleccione o sufixo na lista de selecção para procurar apenas nesse sufixo.

  Nota: Se tiver iniciado esta tarefa a partir do painel **Gerir entradas**, este campo estará preenchido. Seleccionou o **DN Ascendente** antes de fazer clique sobre **Adicionar** para iniciar o processo de adição da entrada.

  Também pode seleccionar **Todos os sufixos** para pesquisar toda a árvore.
- **Âmbito da procura**
  - Seleccione **Objecto** para pesquisar apenas no objecto seleccionado.
  - Seleccione **Nível único** para pesquisar apenas o descendente imediato do objecto seleccionado.
  - Seleccione **Sub-árvore** para pesquisar todos os descendentes da entrada seleccionada.
- **Limite do tamanho da procura** - Introduza o número máximo de entradas a procurar ou seleccione **Ilimitado**.
- **Limite de tempo da procura** - Introduza o número máximo de segundos para a procura ou seleccione **Ilimitado**.
- Seleccione um tipo de **Retirar referência a nomes alternativos** na lista de selecção.
  - **Nunca** - Se a entrada seleccionada for um nome alternativo, não é retirada a referência ao mesmo na procura, ou seja, a procura ignora a referência ao nome alternativo.
  - **Localizar** - Se a entrada seleccionada for um nome alternativo, a procura retira a referência ao nome alternativo e começa na localização do mesmo.
  - **Procurar** - Não é retirada a referência à entrada seleccionada, mas a todas as entradas encontradas na procura.
  - **Sempre** - É retirada a referência a todos os nomes alternativos encontrados na procura.
- Seleccione o quadrado de opção **Busca de referências** para seguir as referências para outro servidor caso seja devolvida uma referência pela procura. Quando uma referência direcciona a procura para outro servidor, a ligação ao servidor utiliza as credenciais actuais. Se tiver iniciado sessão como Anónimo, pode ter de iniciar sessão no servidor utilizando um DN autenticado.

Consulte “Ajustar definições de procura” na página 113 para obter informações adicionais sobre procuras.

Alterar atributos binários

Se um atributo requerer dados binários, é apresentado um botão **Dados binários** ao lado do campo de atributos. Se o atributo não tiver dados, o campo estará em branco. Como os atributos binários não podem ser apresentados, se um atributo contiver dados binários, o campo apresentará **Dados Binários - 1**. Se o atributo contiver múltiplos valores, o campo será apresentado como uma lista de selecção.

Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.

Pode importar, exportar ou eliminar dados binários.

Para adicionar dados binários ao atributo:

1. Faça clique sobre o botão **Dados binários**.

2. Faça clique sobre **Importar**.
3. Pode introduzir o nome de caminho do ficheiro pretendido ou fazer clique sobre **Procurar** para localizar e seleccionar o ficheiro binário.
4. Faça clique sobre **Submeter ficheiro**. É apresentada uma mensagem `Ficheiro carregado`.
5. Faça clique sobre **Fechar**. **Dados Binários - 1** é agora apresentado sob **Entradas de dados binários**.
6. Repita o processo de importação para todos os ficheiros binários que pretender adicionar. As entradas subsequentes estão mostradas como **Dados Binários - 2**, **Dados Binários -3**, etc.
7. Quando acabar de adicionar dados binários, faça clique sobre **OK**.

Para exportar dados binários:

1. Faça clique sobre o botão **Dados binários**.
2. Faça clique sobre **Exportar**.
3. Faça clique sobre a ligação **Dados binários a descarregar**.
4. Siga as instruções do seu assistente para apresentar o ficheiro binário ou guardá-lo numa nova localização.
5. Faça clique sobre **Fechar**.
6. Repita o processo de importação para todos os ficheiros binários que pretender exportar.
7. Quando acabar de exportar dados, faça clique sobre **OK**.

Para eliminar dados binários:

1. Faça clique sobre o botão **Dados binários**.
2. Marque o ficheiro de dados binários que pretende eliminar. Podem ser seleccionados vários ficheiros.
3. Faça clique sobre **Eliminar**.
4. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**. Os dados binários marcados para eliminação são removidos da lista.
5. Quando acabar de eliminar dados, faça clique sobre **OK**.

Nota: Os atributos binários não são pesquisáveis.

Gerir utilizadores e grupos

Para gerir utilizadores e grupos, expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

Consulte o seguinte para obter mais informações:

- "Gerir utilizadores"
- "Gerir grupos" na página 153

Gerir utilizadores

Após ter configurado os seus domínios e modelos, pode preenchê-los com utilizadores.Consulte o seguinte:

- "Adicionar utilizadores" na página 152
- "Localizar utilizadores no domínio" na página 152
- "Editar as informações de um utilizador" na página 152
- "Copiar um utilizador" na página 152
- "Remover um utilizador" na página 153

Adicionar utilizadores

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar utilizador** ou faça clique sobre **Gerir utilizadores** e faça clique sobre **Adicionar**.
2. Seleccione o domínio ao qual pretende adicionar o utilizador no menu pendente.
3. Faça clique sobre **Seguinte**. É apresentado o modelo que está associado a esse domínio. Preencha os campos necessários, indicados por um asterisco (*), e todos os outros campos dos separadores. Se já tiver criado grupos no domínio, também pode adicionar o utilizador a um ou mais grupos.
4. Quando terminar, faça clique sobre **Terminar**.

Localizar utilizadores no domínio

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Localizar utilizador** ou sobre **Gerir utilizadores** e sobre **Localizar**.
2. Seleccione o domínio que pretende procurar no campo **Seleccionar domínio**.
3. Introduza a cadeia de procura no campo **Atributo de nomenclatura**. São suportados caracteres globais: por exemplo, se tiver introduzido ***silva**, o resultado serão todas as entradas cujo atributo de nomenclatura termine por silva.
4. Pode executar as seguintes operações num utilizador seleccionado:
   - **Editar** - Consulte “Editar as informações de um utilizador”.
   - **Copiar** - Consulte “Copiar um utilizador”.
   - **Eliminar** - Consulte “Remover um utilizador” na página 153.
5. Quando terminar, faça clique em **OK**.

Editar as informações de um utilizador

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir utilizadores**.
2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver utilizadores**, se os utilizadores ainda não estiverem apresentados na caixa **Utilizadores**.
3. Seleccione o utilizador que pretende editar e faça clique sobre **Editar**.
4. Modifique as informações dos separadores e a filiação de membros em grupos.
5. Quando terminar, faça clique sobre **OK**.

Copiar um utilizador

Se for necessário um certo número de utilizadores que tenham, na sua maioria, informações idênticas, pode criar os utilizadores adicionais copiando o utilizador inicial e modificando as informações.

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir utilizadores**.
2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver utilizadores**, se os utilizadores ainda não estiverem apresentados na caixa **Utilizadores**.
3. Seleccione o utilizador que pretende copiar e faça clique sobre **Copiar**.
4. Modifique as informações apropriadas para o novo utilizador como, por exemplo, as informações necessárias que identificam um utilizador específico, como sn ou cn. As informações que sejam comuns a ambos os utilizadores não necessitam de ser alteradas.
5. Quando terminar, faça clique sobre **OK**.

Remover um utilizador

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir utilizadores**.
2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver utilizadores**, se os utilizadores ainda não estiverem apresentados na caixa **Utilizadores**.
3. Seleccione o utilizador que pretende remover e faça clique sobre **Eliminar**.
4. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.
5. O utilizador é removido da lista de utilizadores.

Gerir grupos

Após ter configurado os seus domínios e modelos, pode criar grupos. Consulte o seguinte:

- "Adicionar grupos"
- "Localizar grupos no domínio"
- "Editar as informações de um grupo"
- "Copiar um grupo" na página 154
- "Remover um grupo" na página 154

Adicionar grupos

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar grupo** ou sobre **Gerir grupos** e sobre **Adicionar**.
2. Introduza o nome do grupo que pretende criar.
3. Seleccione o domínio ao qual pretende adicionar o utilizador no menu pendente.
4. Faça clique sobre **Terminar** para criar o grupo. Se já tiver utilizadores no domínio, pode fazer clique sobre **Seguinte** e seleccionar utilizadores a adicionar ao grupo. Em seguida, faça clique sobre **Terminar**.

Consulte "Grupos e funções" na página 45 para obter informações adicionais.

Localizar grupos no domínio

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Localizar grupo** ou sobre **Gerir grupos** e sobre **Localizar**.
2. Seleccione o domínio que pretende procurar no campo **Seleccionar domínio**.
3. Introduza a cadeia de procura no campo **Atributo de nomenclatura**. São suportados caracteres globais: por exemplo, se tiver introduzido ***clube**, o resultado serão todos os grupos que tenham o atributo de nomenclatura clube como, por exemplo, clube de leitura, clube de xadrez, clube de jardinagem, etc.
4. Pode executar as seguintes operações num grupo seleccionado:
   - **Editar** - Consulte "Editar as informações de um grupo".
   - **Copiar** - Consulte "Copiar um grupo" na página 154.
   - **Eliminar** - Consulte "Remover um grupo" na página 154.
5. Quando terminar, faça clique sobre **Fechar**.

Editar as informações de um grupo

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir grupos**.

2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver grupos**, se os grupos ainda não estiverem apresentados na caixa **Grupos**.
3. Seleccione o grupo que pretende editar e faça clique sobre **Editar**.
4. Pode fazer clique sobre **Filtrar** para limitar o número de**Utilizadores disponíveis**. Por exemplo, se introduzir *silva no campo Apelido, limitará os utilizadores disponíveis àqueles cujos nomes terminem por silva, como Ana Silva, Rui Silva, Jorge Madressilva, etc.
5. Pode adicionar ou remover utilizadores do grupo.
6. Quando terminar, faça clique sobre **OK**.

Copiar um grupo

Se for necessário um certo número de grupos que tenham, na sua maioria, os mesmos membros, pode criar os grupos adicionais copiando o grupo inicial e modificando as informações.

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir grupos**.
2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver grupos**, se os utilizadores ainda não estiverem apresentados na caixa**Grupos**.
3. Seleccione o grupo que pretende copiar e faça clique sobre **Copiar**.
4. Altere o nome do grupo no campo **Nome do grupo**. O novo grupo tem os mesmos membros que o grupo original.
5. Pode modificar os membros do grupo.
6. Quando terminar, faça clique sobre **OK**. O novo grupo é criado e contém os mesmos membros que o grupo original com quaisquer modificações de adição ou remoção que tenha efectuado durante o procedimento de cópia.

Remover um grupo

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir grupos**.
2. Seleccione um domínio no menu pendente. Faça clique sobre **Ver grupos**, se os grupos ainda não estiverem apresentados na caixa **Grupos**.
3. Seleccione o grupo que pretende remover e faça clique sobre **Eliminar**.
4. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.
5. O grupo é removido da lista de grupos.

Gerir domínios e modelos de utilizador

Para gerir domínios e modelos de utilizador, faça clique sobre **Domínios e modelos** na área de navegação da ferramenta de administração da Web. Utilize domínios e modelos de utilizador para facilitar a outros utilizadores a introdução de dados no directório. Para obter mais informações sobre conceitos de domínios e modelos de utilizador, consulte “Domínios e modelos de utilizador” na página 41.

Consulte o seguinte para obter mais informações:

- “Criar um domínio” na página 155
- “Criar um administrador de domínio” na página 155
- “Criar um modelo” na página 156
- “Adicionar o modelo a um domínio” na página 158
- “Criar grupos” na página 158
- “Adicionar um utilizador ao domínio” na página 158
- “Gerir domínios” na página 158

• “Gerir modelos” na página 159

Criar um domínio

Para obter mais informações sobre conceitos de domínios e modelos de utilizador, consulte “Domínios e modelos de utilizador” na página 41.

Para criar um domínio, proceda do seguinte modo:

1. Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.
2. Faça clique sobre **Adicionar domínio**.
   - Introduza o nome para o domínio. Por exemplo, **domínio1**.
   - Introduza o DN Ascendente que identifica a localização do domínio. Esta entrada está no formato de um sufixo como, por exemplo, o=ibm,c=po. Esta entrada pode ser um sufixo ou uma entrada noutro ponto do directório. Também pode fazer clique sobre **Procurar** para seleccionar a localização da sub-árvore que pretende.
3. Faça clique sobre **Seguinte** para continuar ou sobre **Terminar**.
4. Se tiver feito clique sobre **Seguinte**, reveja as informações. Como, nesta fase, ainda não criou propriamente o domínio, **Modelo de utilizador** e **Filtro de procura de utilizador** podem ser ignorados.
5. Faça clique sobre **Terminar** para criar o domínio.

Criar um administrador de domínio

Para criar um administrador de domínio, terá, primeiro, de criar um grupo de administração para o domínio, do seguinte modo:

1. Crie o grupo de administração do domínio.
   a. Expanda a categoria **Gestão do directório** na área de navegação da ferramenta de administração da Web.
   b. Faça clique sobre **Gerir entradas**.
   c. Expanda a árvore e seleccione o domínio que acabou de criar, **cn=domínio1,o=ibm,c=po**.
   d. Faça clique sobre **Editar ACL**.
   e. Faça clique sobre o separador **Proprietários**.
   f. Certifique-se de que a caixa **Propagar proprietário** está marcada.
   g. Introduza o DN para o domínio, **cn=domínio1,o=ibm,c=po**.
   h. Altere o **Tipo** para grupo.
   i. Faça clique sobre **Adicionar**.
2. Crie a entrada do administrador. Se ainda não tiver uma entrada de utilizador para o administrador, terá de criar uma.
   a. Expanda a categoria **Gestão do directório** na área de navegação da ferramenta de administração da Web.
   b. Faça clique sobre **Gerir entradas**.
   c. Expanda a árvore para a localização onde pretende que a entrada do administrador resida.

      Nota: Ao posicionar a entrada do administrador fora do domínio, evitará dar a possibilidade ao administrador de se eliminar inadvertidamente. Neste exemplo, a localização poderia ser **o=ibm,c=po**.
   d. Faça clique sobre **Adicionar**.
   e. Seleccione a **Classe de objecto estrutural** como, por exemplo,**inetOrgPerson**.
   f. Faça clique sobre **Seguinte**.
   g. Seleccione qualquer classe de objecto auxiliar que pretenda adicionar.

h. Faça clique sobre **Seguinte**.
i. Introduza os atributos necessários para a entrada. Por exemplo:
   - **RDN** cn=JoaquimDias
   - **DN** o=ibm,c=po
   - **cn** Joaquim Dias
   - **sn** Dias
j. No separador **Outros atributos**, certifique-se de que atribuiu uma palavra-passe.
k. Quando terminar, faça clique sobre **Terminar**.

3. Adicione o administrador ao grupo de administração.
   a. Expanda a categoria **Gestão do directório** na área de navegação da ferramenta de administração da Web.
   b. Faça clique sobre **Gerir entradas**.
   c. Expanda a árvore e seleccione o domínio que acabou de criar, **cn=domínio1,o=ibm,c=po**.
   d. Faça clique sobre **Editar atributos**.
   e. Faça clique sobre o separador **Membros**.
   f. Faça clique sobre **Membros**.
   g. No campo **Membros**, introduza o DN do administrador; neste exemplo, **cn=Joaquim Dias,o=ibm,c=po**.
   h. Faça clique sobre **Adicionar**. O DN é apresentado na lista **Membros**.
   i. Faça clique sobre **OK**.
   j. Faça clique sobre **Actualizar**. O DN é apresentado na lista **Membros actuais**.
   k. Faça clique sobre **OK**.
4. Criou um administrador com capacidade para gerir entradas no domínio.

Criar um modelo

Depois de ter criado um domínio, o seu próximo passo é criar um modelo de utilizador. Um modelo ajuda-o a organizar as informações que pretende introduzir. Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar modelo de utilizador**.
   - Introduza o nome do modelo como, por exemplo, **modelo1**.
   - Introduza a localização onde o modelo vai residir. Para fins de replicação, localize o modelo na sub-árvore do domínio que vai utilizar este modelo. Por exemplo, o domínio criado nas operações anteriores, **cn=domínio1,o=ibm,c=po**. Também pode fazer clique sobre **Procurar** para seleccionar uma sub-árvore diferente para a localização do modelo.
2. Faça clique sobre **Seguinte**. Pode fazer clique sobre **Terminar** para criar um modelo vazio. Para adicionar posteriormente informações ao modelo, consulte o tópico “Editar um modelo” na página 161.
3. Se tiver feito clique sobre **Seguinte**, escolha a classe de objecto estrutural para o modelo como, por exemplo, **inetOrgPerson**. Também pode adicionar quaisquer classes de objecto auxiliares pretendidas.
4. Faça clique sobre **Seguinte**.
5. Foi criado um separador **Obrigatório** no modelo. Pode modificar as informações contidas neste separador.
   a. Seleccione **Obrigatório** no menu de separadores e faça clique sobre **Editar**. É apresentado o painel **Editar separador**. Poderá ver o nome do separador **Obrigatório** e os atributos seleccionados que são necessários à classe de objecto **inetOrgPerson**:
      - *sn - apelido
      - *cn - nome comum

Nota: O * indica informações necessárias.

b. Se pretender adicionar outras informações a este separador, seleccione o atributo no menu **Atributos**. Por exemplo, seleccione **departmentNumber** e faça clique sobre **Adicionar**. Seleccione **title** e faça clique sobre **Adicionar**. O menu **Atributos seleccionados** passa a mostrar:
   - title
   - employeeNumber
   - departmentNumber
   - *sn
   - *cn

c. Pode reorganizar a forma como estes campos aparecem no modelo evidenciando o atributo seleccionado e fazendo clique sobre **Mover para cima** ou **Mover para baixo**. Esta operação faz com que o atributo avance ou recue uma posição. Repita este procedimento até reorganizar os atributos pela ordem pretendida. Por exemplo:
   - *sn
   - *cn
   - title
   - employeeNumber
   - departmentNumber

d. Também pode modificar cada atributo seleccionado.
   1) Evidencie o atributo na caixa **Atributos seleccionados** e faça clique sobre **Editar**.
   2) Pode alterar o nome de visualização do campo utilizado no modelo. Por exemplo, se desejar que **departmentNumber** seja apresentado como **Número do departamento**, introduza essa informação no campo **Nome de visualização**.
   3) Também pode fornecer um valor assumido para preencher previamente o campo do atributo do modelo. Por exemplo, se a maioria dos utilizadores que vão ser introduzidos for membro do Departamento 789, pode introduzir 789 como o valor assumido. O campo do modelo é preenchido com 789. O valor pode ser alterado quando adicionar as informações reais sobre o utilizador.
   4) Faça clique sobre **OK**.

e. Faça clique sobre **OK**.

6. Para criar outra categoria de separadores para informações adicionais, faça clique sobre **Adicionar**.
   - Introduza o nome do novo separador. Por exemplo, Informações sobre endereços.
   - Para este separador, seleccione os atributos no menu **Atributos**. Seleccione **postOfficeBox** e faça clique sobre **Adicionar**. Seleccione **telephoneNumber** e faça clique sobre **Adicionar**. Seleccione **homePhone** e faça clique sobre **Adicionar**. Seleccione **facsimileTelephoneNumber** e faça clique sobre **Adicionar**. O menu **Atributos seleccionados** passa a indicar:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Pode reorganizar a forma como estes campos aparecem no modelo evidenciando o atributo seleccionado e fazendo clique sobre **Mover para cima** ou **Mover para baixo**. Esta operação faz com que o atributo avance ou recue uma posição. Repita este procedimento até reorganizar os atributos pela ordem pretendida. Por exemplo:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber

- facsimileTelephoneNumber
- homePhone

• Faça clique sobre **OK**.

7. Repita este processo para todos os separadores que pretenda criar. Quando terminar, faça clique sobre **Terminar** para criar o modelo.

Adicionar o modelo a um domínio

Após ter criado um domínio e um modelo, terá de adicionar o modelo ao domínio. Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir domínios**.
2. Seleccione o domínio ao qual pretende adicionar o modelo; neste exemplo, **cn=domínio1,o=ibm,c=po**. Faça clique sobre **Editar**.
3. Desloque-se para baixo até **Modelo de utilizador** e expanda o menu pendente.
4. Seleccione o modelo; neste exemplo, **cn=modelo1,cn=domínio1,o=ibm,c=po**.
5. Faça clique sobre **OK**.
6. Faça clique sobre **Fechar**.

Criar grupos

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar grupo**.
2. Introduza o nome do grupo que pretende criar. Por exemplo, **grupo1**.
3. Seleccione o domínio ao qual pretende adicionar o utilizador no menu pendente. Neste caso, **domínio1**.
4. Faça clique sobre **Terminar** para criar o grupo. Se já tiver utilizadores no domínio, pode fazer clique sobre **Seguinte** e seleccionar utilizadores a adicionar ao grupo1. Em seguida, faça clique sobre **Terminar**.

Consulte “Grupos e funções” na página 45 para obter informações adicionais.

Adicionar um utilizador ao domínio

Expanda a categoria **Utilizadores e grupos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar utilizador**.
2. Seleccione o domínio ao qual pretende adicionar o utilizador no menu pendente. Neste caso, **domínio1**.
3. Faça clique sobre **Seguinte**. É apresentado o modelo que acabou de criar, modelo1. Preencha os campos necessários, indicados por um asterisco (*), e todos os outros campos dos separadores. Se já tiver criado grupos no domínio, também pode adicionar o utilizador a um ou mais grupos.
4. Quando terminar, faça clique sobre **Terminar**.

Gerir domínios

Após ter configurado e preenchido o seu domínio inicial, pode adicionar mais domínios ou modificar os existentes.

Expanda a categoria **Domínios e modelos** na área de navegação e faça clique sobre **Gerir domínios**. É apresentada uma lista de domínios existentes. Neste painel, pode adicionar, editar ou remover um domínio ou editar a lista de controlo de acesso (ACL) do domínio. Para obter mais informações, consulte:

• “Adicionar um domínio” na página 159
• “Editar um domínio” na página 159

- "Remover um domínio"
- "Editar ACLs no domínio"

Adicionar um domínio

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar domínio**.
   - Introduza o nome para o domínio. Por exemplo, **domínio2**.
   - Se já tiver domínios pré-existentes, por exemplo, **domínio1**, pode seleccionar um domínio e fazer com que as respectivas definições sejam copiadas para o domínio que está a criar.
   - Introduza o DN Ascendente que identifica a localização do domínio. Esta entrada está no formato de um sufixo como, por exemplo,**o=ibm,c=po**. Também pode fazer clique sobre **Procurar** para seleccionar a localização da sub-árvore que pretende.
2. Faça clique sobre **Seguinte** para continuar ou sobre **Terminar**.
3. Se tiver feito clique sobre **Seguinte**, reveja as informações.
4. Seleccione um **Modelo de utilizador** no menu pendente. Se tiver copiado as definições de um domínio pré-existente, o respectivo modelo será preenchido neste campo.
5. Introduza um **Filtro de procura de utilizador**.
6. Faça clique sobre **Terminar** para criar o domínio.

Editar um domínio

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

- Faça clique sobre **Gerir domínios**.
- Seleccione o domínio que pretende editar na lista de domínios.
- Faça clique sobre **Editar**.
  - Pode utilizar os botões **Procurar** para alterar o
    - Grupo de administradores
    - Contentor de grupos
    - Contentor de utilizadores
  - Pode seleccionar um modelo diferente no menu pendente.
  - Faça clique sobre **Editar** para modificar o **Filtro de procura de utilizador**.
- Faça clique sobre **OK** quando terminar.

Remover um domínio

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir domínios**.
2. Seleccione o domínio que pretende remover.
3. Faça clique sobre **Eliminar**.
4. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.
5. O domínio é removido da lista de domínios.

Editar ACLs no domínio

Para ver propriedades de ACL utilizando a ferramenta de administração da Web e para trabalhar com ACLs, consulte "Gerir listas de controlo de acesso (ACLs)" na página 162.

Consulte "Listas de controlo de acesso" na página 51 para obter informações adicionais.

Gerir modelos

Após ter criado o seu modelo inicial, pode adicionar mais modelos ou modificar os existentes.

Expanda a categoria **Domínios e modelos** na área de navegação e faça clique sobre **Gerir modelos de utilizador**. É apresentada uma lista de modelos existentes. Neste painel, pode adicionar, editar ou remover um modelo ou editar a lista de controlo de acesso (ACL) do modelo. Para obter mais informações, consulte:

- "Adicionar um modelo de utilizador"
- "Editar um modelo" na página 161
- "Remover um modelo" na página 162
- "Editar ACLs no modelo" na página 162

Adicionar um modelo de utilizador

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Adicionar modelo de utilizador** ou sobre **Gerir modelos de utilizador** e sobre **Adicionar**.
   - Introduza o nome do novo modelo. Por exemplo, **modelo2**.
   - Se tiver modelos pré-existentes, por exemplo, **modelo1**, pode seleccionar um modelo e fazer com que as respectivas definições sejam copiadas para o modelo que está a criar.
   - Introduza o DN Ascendente que identifica a localização do modelo. Esta entrada está no formato de um DN como, por exemplo, **cn=domínio1,o=ibm,c=po**. Também pode fazer clique sobre **Procurar** para seleccionar a localização da sub-árvore que pretende.
2. Faça clique sobre **Seguinte**. Pode fazer clique sobre **Terminar** para criar um modelo vazio. Para adicionar posteriormente informações ao modelo, consulte "Editar um modelo" na página 161.
3. Se tiver feito clique sobre **Seguinte**, escolha a classe de objecto estrutural para o modelo como, por exemplo, **inetOrgPerson**. Também pode adicionar quaisquer classes de objecto auxiliares pretendidas.
4. Faça clique sobre **Seguinte**.
5. Foi criado um separador **Obrigatório** no modelo. Pode modificar as informações contidas neste separador.
   a. Seleccione **Obrigatório** no menu de separadores e faça clique sobre **Editar**. É apresentado o painel **Editar separador**. Poderá ver o nome do separador **Obrigatório** e os atributos seleccionados que são necessários à classe de objecto **inetOrgPerson**:
      - *sn - apelido
      - *cn - nome comum

      Nota: O * indica informações necessárias.
   b. Se pretender adicionar outras informações a este separador, seleccione o atributo no menu **Atributos**. Por exemplo, seleccione **departmentNumber** e faça clique sobre **Adicionar**. Seleccione **title** e faça clique sobre **Adicionar**. O menu **Atributos seleccionados** passa a mostrar:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Pode reorganizar a forma como estes campos aparecem no modelo evidenciando o atributo seleccionado e fazendo clique sobre **Mover para cima** ou **Mover para baixo**. Esta operação faz com que o atributo avance ou recue uma posição. Repita este procedimento até reorganizar os atributos pela ordem pretendida. Por exemplo:
      - *sn
      - *cn
      - title
      - employeeNumber

- departmentNumber

d. Também pode modificar cada atributo seleccionado.
   1) Evidencie o atributo na caixa **Atributos seleccionados** e faça clique sobre **Editar**.
   2) Pode alterar o nome de visualização do campo utilizado no modelo. Por exemplo, se desejar que **departmentNumber** seja apresentado como **Número do departamento**, introduza essa informação no campo **Nome de visualização**.
   3) Também pode fornecer um valor assumido para preencher previamente o campo do atributo do modelo. Por exemplo, se a maioria dos utilizadores que vão ser introduzidos for membro do Departamento 789, pode introduzir 789 como o valor assumido. O campo do modelo é preenchido com 789. O valor pode ser alterado quando adicionar as informações reais sobre o utilizador.
   4) Faça clique sobre **OK**.

e. Faça clique sobre **OK**.

6. Para criar outra categoria de separadores para informações adicionais, faça clique sobre **Adicionar**.
   - Introduza o nome do novo separador. Por exemplo, Informações sobre endereços.
   - Para este separador, seleccione o atributo no menu **Atributos**. Seleccione **postOfficeBox** e faça clique sobre **Adicionar**. Seleccione **telephoneNumber** e faça clique sobre **Adicionar**. Seleccione **homePhone** e faça clique sobre **Adicionar**. Seleccione **facsimileTelephoneNumber** e faça clique sobre **Adicionar**. O menu **Atributos seleccionados** passa a indicar:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Pode reorganizar a forma como estes campos aparecem no modelo evidenciando o atributo seleccionado e fazendo clique sobre **Mover para cima** ou **Mover para baixo**. Esta operação faz com que o atributo avance ou recue uma posição. Repita este procedimento até reorganizar os atributos pela ordem pretendida. Por exemplo:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Faça clique sobre **OK**.

7. Repita este processo para todos os separadores que pretenda criar. Quando terminar, faça clique sobre **Terminar** para criar o modelo.

Editar um modelo

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

- Faça clique sobre **Gerir modelos de utilizador**.
- Seleccione o domínio que pretende editar na lista de domínios.
- Faça clique sobre **Editar**.
- Se tiver modelos pré-existentes como, por exemplo, modelo1, pode seleccionar um modelo e fazer com que as respectivas definições sejam copiadas para o modelo que está a editar.
- Faça clique sobre **Seguinte**.
  – Pode utilizar o menu pendente para alterar a classe de objecto estrutural do modelo
  – Pode adicionar ou remover classes de objecto auxiliares.
- Faça clique sobre **Seguinte**.

- Pode modificar os separadores e atributos contidos no modelo. Consulte 5 na página 160 para obter informações sobre como modificar os separadores.
- Quando terminar, faça clique sobre **Terminar**.

Remover um modelo

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir modelos de utilizador**.
2. Seleccione o modelo que pretende remover.
3. Faça clique sobre **Eliminar**.
4. Quando lhe for pedido que confirme a eliminação, faça clique sobre **OK**.
5. O modelo é removido da lista de modelos.

Editar ACLs no modelo

Expanda a categoria **Domínios e modelos** na área de navegação da ferramenta de administração da Web.

1. Faça clique sobre **Gerir modelos de utilizador**.
2. Seleccione o modelo cujas ACLs pretende editar.
3. Faça clique sobre **Editar ACL**.

Para ver propriedades de ACL utilizando a ferramenta de administração da Web e para trabalhar com ACLs, consulte "Gerir listas de controlo de acesso (ACLs)".

Consulte "Listas de controlo de acesso" na página 51 para obter informações adicionais.

Gerir listas de controlo de acesso (ACLs)

Para obter mais informações sobre listas de controlo de acesso, consulte "Listas de controlo de acesso" na página 51.

Para ver propriedades de ACL utilizando a ferramenta de administração da Web e para trabalhar com ACLs, proceda do seguinte modo:

1. Seleccione uma entrada de directório. Por exemplo, cn=Joaquim Dias, ou=Publicidade,o=ibm,c=PO.
2. Faça clique sobre **Editar ACL**. É apresentado o painel Editar Acl com o separador **ACLs Efectivas** pré-seleccionado.

Este painel tem cinco separadores:

- "ACLs Efectivas"
- "Proprietários efectivos" na página 163
- "ACLs não filtradas" na página 163
- "ACLs Filtradas" na página 164
- "Proprietários" na página 166

Os separadores **ACLs efectivas** e **Proprietários Efectivos** contêm informações só de leitura sobre as ACLs.

ACLs Efectivas

As ACLs efectivas são as ACLs explícitas e herdadas da entrada seleccionada. Pode ver os direitos de acesso de um ACL efectiva específica seleccionando-a e fazendo clique sobre o botão **Ver**. Abre-se o painel **Ver direitos de acesso**.

Ver direitos de acesso

- A secção **Direitos** apresenta os direitos de adição e eliminação do sujeito.

- **Adicionar descendente** concede ou recusa ao sujeito o direito de adicionar uma entrada de directório abaixo da entrada seleccionada.
- **Eliminar entrada** concede ou recusa ao sujeito o direito de eliminar a entrada seleccionada.

- A secção da classe **Segurança** define permissões para classes de segurança. Os atributos estão agrupados em classes de segurança:
  - **Normal** - As classes de atributos normais requerem uma segurança mínima como, por exemplo, o atributo commonName.
  - **Sensível** - As classes de atributos sensíveis requerem uma segurança moderada como, por exemplo, homePhone.
  - **Crítica** - As classes de atributo críticas requerem a máxima segurança como, por exemplo o atributo userpassword.

  Cada classe de segurança tem permissões associadas.
  - **Leitura** - o sujeito pode ler atributos.
  - **Escrita** - o sujeito pode modificar os atributos.
  - **Pesquisa** - o sujeito pode pesquisar atributos.
  - **Comparação** - o sujeito pode comparar atributos.

Faça clique sobre **OK** para regressar ao separador ACLs Efectivas.

Faça clique sobre **Cancelar** para regressar ao painel Editar ACL.

Proprietários efectivos

Os proprietários efectivos são os proprietários explícitos e herdados da entrada seleccionada.

ACLs não filtradas

Pode adicionar novas ACLs não filtradas a uma entrada ou editar ACLs não filtradas existentes.

As ACLs não filtradas podem ser propagadas. Isto significa que as informações de controlo de acesso definidas para uma entrada podem ser aplicadas a todas as respectivas entradas subordinadas. A origem da ACL é a origem da ACL actual referente à entrada seleccionada. Se a entrada não tiver uma ACL, ela herda uma ACL de objectos ascendentes com base nas definições da ACL dos objectos ascendentes.

Introduza as seguintes informações no separador ACLs**Não filtradas**:

- Propagar ACLs - Seleccione o quadrado de opção **Propagar** para permitir que os descendentes sem uma ACL explicitamente definida herdem a ACL desta entrada. Se este quadrado de opção for marcado, os descendentes herdam ACLs desta entrada e, se a ACL estiver definida explicitamente para a entrada descendente, a ACL que foi herdada do ascendente será substituída pela nova ACL que foi adicionada. Se o quadrado de opção não estiver marcado, as entradas descendentes sem uma ACL definida explicitamente herdarão ACLs de um ascendente desta entrada que tenha esta opção activada.
- DN (Nome exclusivo) - Introduza o **(DN) Nome exclusivo** da entrada que estiver a solicitar acesso para executar operações na entrada seleccionada como, por exemplo, cn=Grupo de Marketing.
- Tipo - Introduza o **Tipo** do DN. Por exemplo, seleccione id-acesso se o DN for um utilizador.

Adicionar e editar direitos de acesso

Faça clique sobre o botão **Adicionar** para adicionar o DN do campo DN (Nome exclusivo) à lista de ACLs ou o botão Editar para modificar as ACLs de um DN existente.

Os painéis **Adicionar direitos de acesso** e **Editar direitos de acesso** permitem definir os direitos de acesso para uma Lista de Controlo de Acesso (ACL) nova ou já existente. O campo **Tipo** tem como valor assumido o tipo que seleccionou no painel **Editar ACL**. Se estiver a adicionar uma ACL, todos os outros

campos terão como valor assumido um espaço em branco. Se estiver a editar uma ACL, os campos contêm valores definidos da última vez que a ACL foi modificada.

Pode:

- Alterar o tipo de ACL
- Definir direitos de adição e eliminação
- Definir permissões para classes de segurança

Para definir direitos de acesso:

1. Seleccione o **Tipo** de entrada para a ACL. Por exemplo, seleccione id-acesso se o DN for um utilizador.
2. A secção **Direitos** apresenta os direitos de adição e eliminação do sujeito.
   - **Adicionar descendente** concede ou recusa ao sujeito o direito de adicionar uma entrada de directório abaixo da entrada seleccionada.
   - **Eliminar entrada** concede ou recusa ao sujeito o direito de eliminar a entrada seleccionada.
3. A secção **Classe de segurança** define permissões para classes de atributo. Os atributos estão agrupados em classes de segurança:
   - Normal - As classes de atributos normais requerem uma segurança mínima como, por exemplo, o atributo commonName.
   - Sensível - As classes de atributos sensíveis requerem uma segurança moderada, como, por exemplo, homePhone.
   - Crítica - As classes de atributo críticas requerem a máxima segurança como, por exemplo, o atributo userpassword.

   Cada classe de segurança tem permissões associadas.
   - Leitura - o sujeito pode ler os atributos.
   - Escrita - o sujeito pode modificar os atributos.
   - Pesquisa - o sujeito pode pesquisar os atributos.
   - Comparação - o sujeito pode comparar atributos.

   Adicionalmente, pode especificar permissões com base no atributo e, vez da classe de segurança à qual pertence o atributo. A secção de atributos está mostrada abaixo da **Classe de segurança crítica**.
   - Seleccione um atributo na lista de selecção **Definir um atributo**.
   - Faça clique sobre **Definir**. O atributo é apresentado com uma tabela de permissões.
   - Especifique se pretende conceder ou recusar cada uma das quatro permissões de classes de segurança associadas ao atributo.
   - Pode repetir este procedimento para múltiplos atributos.
   - Para remover um atributo, basta seleccioná-lo e fazer clique sobre **Eliminar**.
   - Quando terminar, faça clique sobre **OK**.

Remover ACLs

Pode remover ACLs de duas formas:

- Seleccione o botão ao lado da ACL que pretende eliminar. Faça clique sobre **Remover**.
- Faça clique sobre **Remover todos** para eliminar todos os DNs da lista.

ACLs Filtradas

Pode adicionar novas ACLs filtradas a uma entrada ou editar ACLs filtradas existentes.

As ACLs baseadas em filtros empregam uma comparação baseada em filtros, utilizando um filtro de objecto especificado, para fazer corresponder objectos específicos com o acesso efectivo aplicável aos mesmos.

O comportamento assumido das ACLs baseadas em filtros é serem acumuladas, desde a entrada de conteúdo inferior, no sentido ascendente e paralelamente à cadeia de entrada anterior, até à entrada de conteúdo superior da DIT. O acesso efectivo é calculado como a união dos direitos de acesso concedidos, ou recusados, pelas entradas anteriores constituintes. Existe uma excepção a este comportamento. Por uma questão de compatibilidade com a função de replicação da sub-árvore, e para permitir um maior controlo administrativo, é utilizado um atributo de limite máximo como meio para parar a acumulação na entrada em que está contido.

Introduza as seguintes informações no separador ACLs Filtradas:

- Acumular ACLs filtradas -
  - Seleccione o botão **Não especificado** para remover o atributo ibm-filterACLInherit da entrada seleccionada.
  - Seleccione o botão **Verdadeiro** para permitir que as ACLs referentes à entrada seleccionada sejam acumuladas desde essa entrada, no sentido ascendente e paralelamente à cadeia de entrada anterior, até à entrada de conteúdo superior da ACL filtrada da DIT.
  - Seleccione o botão **Falso** para parar a acumulação de ACLs filtradas na entrada seleccionada.
- DN (Nome exlusivo) - Introduza o **(DN) Nome exclusivo** da entrada que estiver a solicitar acesso para executar operações na entrada seleccionada como, por exemplo, cn=Grupo de Marketing.
- Tipo - Introduza o **Tipo** do DN. Por exemplo, seleccione id-acesso se o DN for um utilizador.

Adicionar e editar direitos de acesso

Faça clique sobre o botão **Adicionar** para adicionar o DN do campo DN (Nome exclusivo) à lista de ACLs ou o botão Editar para modificar as ACLs de um DN existente.

Os painéis **Adicionar direitos de acesso** e **Editar direitos de acesso** permitem definir os direitos de acesso para uma Lista de Controlo de Acesso (ACL) nova ou já existente. O campo Tipo tem como valor assumido o tipo que seleccionou no painel Editar ACL. Se estiver a adicionar uma ACL, todos os outros campos terão como valor assumido um espaço em branco. Se estiver a editar uma ACL, os campos contêm valores definidos da última vez que a ACL foi modificada.

Pode:

- Alterar o tipo de ACL
- Definir direitos de adição e eliminação
- Definir o filtro de objectos para ACLs filtradas
- Definir permissões para classes de segurança

Para definir direitos de acesso:

1. Seleccione o **Tipo** de entrada para a ACL. Por exemplo, seleccione id-acesso se o DN for um utilizador.
2. A secção **Direitos** apresenta os direitos de adição e eliminação do sujeito.
   - **Adicionar descendente** concede ou recusa ao sujeito o direito de adicionar uma entrada de directório abaixo da entrada seleccionada.
   - **Eliminar entrada** concede ou recusa ao sujeito o direito de eliminar a entrada seleccionada.
3. Defina o filtro de objectos para uma comparação baseada em filtros. No campo **Filtro de objectos**, introduza o filtro de objectos desejado para a ACL seleccionada. Faça clique sobre o botão **Editar**

filtro para obter assistência para a composição da cadeia de filtros de procura. A ACL filtrada actual propaga-se para quaisquer objectos descendentes na sub-árvore associada que correspondam ao filtro deste campo.

4. A secção **Classe de segurança** define permissões para classes de atributo. Os atributos estão agrupados em classes de segurança:
   - Normal - As classes de atributos normais requerem uma segurança mínima como, por exemplo, o atributo commonName.
   - Sensível - As classes de atributos sensíveis requerem uma segurança moderada, como, por exemplo, homePhone.
   - Crítica - As classes de atributo críticas requerem a máxima segurança como, por exemplo, o atributo userpassword.

   Cada classe de segurança tem permissões associadas.
   - Leitura - o sujeito pode ler os atributos.
   - Escrita - o sujeito pode modificar os atributos.
   - Pesquisa - o sujeito pode pesquisar os atributos.
   - Comparação - o sujeito pode comparar atributos.

   Adicionalmente, pode especificar permissões com base no atributo e, vez da classe de segurança à qual pertence o atributo. A secção de atributos está mostrada abaixo da **Classe de segurança crítica**.
   - Seleccione um atributo na lista de selecção **Definir um atributo**.
   - Faça clique sobre **Definir**. O atributo é apresentado com uma tabela de permissões.
   - Especifique se pretende conceder ou recusar cada uma das quatro permissões de classes de segurança associadas ao atributo.
   - Pode repetir este procedimento para múltiplos atributos.
   - Para remover um atributo, basta seleccioná-lo e fazer clique sobre **Eliminar**.
   - Quando terminar, faça clique sobre **OK**.

Remover ACLs

Pode remover ACLs de duas formas:

- Seleccione o botão ao lado da ACL que pretende eliminar. Faça clique sobre **Remover**.
- Faça clique sobre **Remover todos** para eliminar todos os DNs da lista.

Proprietários

Os proprietários de entradas têm permissões totais para executar qualquer operação num objecto. Os proprietários de entradas podem ser explícitos ou propagados (herdados).

Introduza as seguintes informações no separador **Proprietários**:

- Seleccione o quadrado de opção **Propagar proprietários** para permitir que os descendentes sem um proprietário definido explicitamente sejam herdados desta entrada. Se o quadrado de opção não estiver marcado, as entradas descendentes sem um proprietário definido explicitamente herdarão o proprietário de um ascendente desta entrada que tenha esta opção activada.
- DN (Nome exclusivo) - Introduza o **(DN) Nome exclusivo** da entidade que solicita o acesso para executar operações na entrada seleccionada como, por exemplo, `cn=Grupo de Marketing`.

  A utilização de `cn=este` com objectos que propagam a respectiva propriedade para outros objectos facilita a criação de uma sub-árvore de directórios em que cada objecto é proprietário de si próprio.
- Tipo - Introduza o **Tipo** do DN. Por exemplo, seleccione id-acesso se o DN for um utilizador.

Adicionar um proprietário

Faça clique sobre **Adicionar** para adicionar o DN existente no campo **DN (Nome exclusivo)** à lista.

Remover um proprietário

Pode remover um proprietário de duas formas:

- Seleccione o botão ao lado do DN do proprietário que pretende eliminar. Faça clique sobre **Remover**.
- Faça clique sobre **Remover todos** para eliminar todos os DNs de proprietários da lista.

Publicar informações no Directory Server

Pode configurar o sistema de modo a publicar certas informações num Directory Server no mesmo ou noutro sistema, bem como informações definidas pelo utilizador. O OS/400 publica automaticamente estas informações no Directory Server quando utiliza o iSeries Navigator para alterar estas informações no OS/400. As informações que pode publicar incluem o sistema (sistemas e impressoras), partilhas de impressão, informações sobre o utilizador e políticas de Quality of service de TCP/IP (para obter mais informações, consulte "Publicação" na página 35).

Se o DN ascendente no qual os dados estão a ser publicados não existir, o Directory Server criá-lo-á automaticamente. Também poderá ter instaladas outras aplicações de OS/400 que publiquem informações num directório de LDAP. Adicionalmente, pode chamar todas as interfaces de programação de aplicações (APIs) dos seus próprios programas para publicar outros tipos de informações no directório de LDAP.

Nota: Também pode publicar informações do OS/400 num Directory Server que não esteja em execução no OS/400 se configurar esse servidor para utilizar o esquema da IBM.

Para configurar o sistema de modo a publicar informações sobre o OS/400 num Directory Server, siga estes passos:

1. No iSeries Navigator, faça clique com o botão direito do rato sobre o sistema e seleccione **Propriedades**.
2. Faça clique sobre o separador **Directory Server**.
3. Faça clique sobre os tipos de informações que pretende publicar.

   Sugestão:

   Se pretende publicar mais do que um tipo de informações na mesma localização, pode poupar tempo ao seleccionar tipos de informação múltiplos para configurar de uma vez só. O Operations Navigator irá utilizar os valores que introduz quando configura o tipo de informação pretendido como valores assumidos ao configurar tipos de informação subsequentes.
4. Faça clique sobre **Detalhes**.
5. Faça clique sobre a caixa de verificação **Publicar informações do sistema**.
6. Especifique o **Método de autenticação** que deseja que o servidor utilize, bem como as informações de autenticação adequadas.
7. Faça clique sobre o botão **Editar** junto ao campo **Directory Server (Activo)**. Na caixa de diálogo apresentada, introduza o nome do Directory Server onde deseja publicar informações sobre o OS/400 e, em seguida, faça clique sobre **OK**.
8. No campo **Sob o DN**, introduza o nome exclusivo ascendente (DN) onde pretende adicionar informações sobre o Directory Server.
9. Preencha os campos na estrutura **Ligação do servidor** adequados para a sua configuração.

   Nota: Para publicar informações sobre o OS/400 no Directory Server utilizando SSL ou Kerberos, primeiro, terá de ter um Directory Server configurado para utilizar o protocolo adequado. Consulte "Autenticação de Kerberos com o Directory Server" na página 44 para obter mais informações sobre SSL e Kerberos.
10. Se o Directory Server não utilizar a porta assumida, escreva o número de porta correcto no campo **Porta**.

11. Faça clique sobre **Verificar** para se certificar de que o DN ascendente existe no servidor e de que as informações sobre a ligação estão correctas. Se o caminho do directório não existir, uma caixa de diálogo pede-lhe para criar um.

    Nota: Se o DN ascendente não existir e não criar um, a publicação não terá êxito.
12. Faça clique sobre **OK**.

Nota: Também pode publicar informações do i5/OS num Directory Server que esteja instalado numa plataforma diferente. Tem de publicar as informações do utilizador e do sistema num Directory Server que utilize um esquema compatível com o esquema do Directory Server da IBM. Para obter mais informações sobre o IBM Directory Schema, consulte "Esquema do IBM Directory Server" na página 16.

APIs para publicar informações sobre o OS/400 no Directory Server

O Directory Server fornece suporte incorporado para publicação de informações sobre o sistema e os utilizadores. Estes itens estão mostrados na página **Directory Server** da caixa de diálogo **Propriedades** do sistema. Pode utilizar a configuração do servidor de LDAP e publicar APIs de modo a activar os programas do OS/400 que escreve de modo a publicar outros tipos de informação. Estes tipos de informações aparecem também na página **Directory Server**. Tal como os utilizadores e os sistemas, estão desactivados inicialmente, e podem ser configurados utilizando o mesmo procedimento. O programa que adiciona os dados ao directório de LDAP é designado agente de publicação. O tipo de informação que é publicado, tal como aparece na página **Directory Server**, é designado nome do agente.

As APIs que se seguem permitem incorporar a publicação nos seus programas:

QgldChgDirSvrA
: Uma aplicação utiliza o formato CSVR0500 para adicionar inicialmente um nome de agente marcado como uma entrada desactivada. As instruções para os utilizadores da aplicação deverão recomendar-lhes a utilização do iSeries Navigator para irem para a página de propriedades do Directory Server de modo a configurarem o agente de publicação. Exemplos de nomes de agente são os nomes de agente dos sistemas e utilizadores que estão disponíveis automaticamente na página **Directory Server**.

QgldLstDirSvrA
: Utilize o formato desta API LSVR0500 para listar os agentes que estão presentemente disponíveis no sistema.

QgldPubDirObj
: Utilize esta API para efectuar a publicação de informações.

Para obter informações detalhadas sobre estas APIs, consulte o tópico ″IBM Lightweight Directory Access Protocol (LDAP)″, em Programming, no iSeries Information Center.

Capítulo 8. Resolução de problemas do Directory Server

Infelizmente, até os servidores fiáveis como o Directory Server, por vezes, têm problemas. Quando o Directory Server tiver problemas, as informações que se seguem poderão ajudá-lo a descobrir o erro e a corrigir o problema.

Pode procurar códigos de retorno para erros de LDAP no ficheiro ldap.h, que está localizado no sistema em QSYSINC/H.LDAP.

"Supervisionar erros e acesso com o registo de trabalhos do Directory Server" na página 170
Quando obtém um erro no seu Directory Server e pretende obter mais detalhes, outra acção a executar é ver o registo de trabalhos QDIRSRV.

"Utilizar TRCTCPAPP para ajudar a localizar problemas" na página 170
Para obter erros reproduzíveis, pode utilizar o comando Rastrear Aplicação de TCP/IP (TRCTCPAPP APP(*DIRSRV)) para executar um rastreio dos erros.

"Utilizar a opção LDAP_OPT_DEBUG para rastrear erros" na página 171
Rastreie problemas com clientes que estejam a utilizar as APIs de C de LDAP.

"Erros comuns do cliente de LDAP" na página 171
Conhecer as causas de erros comuns do cliente de LDAP pode ajudá-lo a resolver problemas com o servidor.

Para obter informações adicionais sobre problemas comuns doDirectory Server, consulte a página inicial do Directory Server (www.iseries.ibm.com/ldap).

O Directory Server utiliza vários servidores de Structured Query Language (SQL) que são trabalhos QSQSRVR do iSeries. Quando ocorre um erro de SQL, o registo de trabalhos QDIRSRV deverá conter a seguinte mensagem:

```
Ocorreu o erro -1 de SQL
```

Nestes casos, o registo de trabalhos QDIRSRV remetê-lo-á para os registos de trabalhos do servidor de SQL. No entanto, nalguns casos, o QDIRSRV pode não conter esta mensagem e esta consulta, mesmo que a causa do problema seja um servidor de SQL. Nestes casos, pode ser útil saber quais os trabalhos do servidor de SQL iniciados pelo servidor, para que possa determinarem que registos de trabalhos QSQSRVR deverá procurar erros adicionais.

Quando o Directory Server é iniciado normalmente, gera mensagens semelhantes às seguintes:

```
                                                    Sistema:  MEUISERIES
 Trab  . :   QDIRSRV       Util . . :   QDIRSRV       Número . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Trabalho 057448/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
     Trabalho 057340/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
     Trabalho 057448/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
     Trabalho 057166/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
     Trabalho 057279/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
   Trabalho 057288/QUSER/QSQSRVR utilizado para o processamento de modo do servidor de SQL.
     O Directory Server foi iniciado com êxito.
```

A mensagem refere-se aos trabalhos QSQSRVR que foram iniciados para o servidor. O número de mensagens pode diferir no seu servidor, dependendo da configuração e do número de trabalhos QSQSRVR necessários para executar o arranque do servidor.

Na página Propriedades de **Base de Dados/Sufixos** do iSeries Navigator, deve especificar o número total de servidores de SQL que o Directory Server utiliza para operações de directório após o arranque do servidor. São iniciados servidores de SQL adicionais para replicação.

Supervisionar erros e acesso com o registo de trabalhos do Directory Server

A visualização do registo de erros do Directory Server poderá alertá-lo para erros e ajudá-lo a supervisionar o acesso ao servidor. O registo de trabalhos contém:

- Mensagens sobre o funcionamento do servidor e quaisquer problemas do servidor, como trabalhos ou falhas de replicação do servidor de SQL.
- Mensagens relacionadas com a segurança que reflictam operações executadas por clientes como, por exemplo, palavras-passe erradas.
- Mensagens que fornecem detalhes sobre erros de clientes como, por exemplo, atributos obrigatórios em falta.

Pode não desejar registar os erros dos clientes, a menos que esteja a depurar problemas relacionados com clientes. Pode controlar o registo de erros de clientes no separador de propriedades **Geral** do Directory Server no iSeries Navigator.

Se o servidor estiver iniciado, execute os seguintes passos para ver o registo de trabalhos QDIRSRV:
1. No iSeries Navigator, expanda **Rede**.
2. Expanda **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Trabalhos do Servidor**.
5. No menu **Ficheiro**, escolha **Registo de Trabalhos**.

Se o servidor estiver parado, efectue os seguintes procedimentos para ver o registo de trabalhos QDIRSRV:
1. No iSeries Navigator, expanda **Operações Básicas**.
2. Faça clique sobre **Output para Impressão**.
3. QDIRSRV aparece na coluna **Utilizador** do painel da direita do iSeries Navigator. Para ver o registo de trabalhos, faça duplo clique sobre **Qpjoblog** à esquerda de QDIRSRV na mesma linha.

   Nota: O iSeries Navigator pode ser configurado para mostrar apenas ficheiros em Spool. Se QDIRSRV não aparecer na lista, faça clique sobre **Output para Impressão** e, em seguida, seleccione **Incluir** no menu **Opções**. Especifique **Todos** no campo **Utilizador** e, em seguida faça clique sobre **OK**.

Nota: O Directory Server utiliza outros recursos de sistema para efectuar algumas tarefas. Se ocorrer um erro com um destes recursos, o registo de trabalhos indicará onde poderá encontrar informações. Nalguns casos, o Directory Server pode não conseguir determinar onde procurar. Nestes casos, consulte o registo de trabalhos do servidor de Structured Query Language (SQL) para ver se o problema estava relacionado com servidores de SQL.

Utilizar TRCTCPAPP para ajudar a localizar problemas

O servidor fornece um rastreio de comunicações para recolher dados numa linha de comunicações, tal como uma interface de rede local (LAN) ou de rede alargada (WAN). O utilizador comum pode não compreender todo o conteúdo dos dados do rastreio. No entanto, pode utilizar as entradas de rastreio para determinar se realmente ocorreu uma troca de dados entre dois pontos.

O comando Rastrear Aplicações de TCP/IP (TRCTCPAPP) com a opção *DIRSRV pode ser utilizado no Directory Server para ajudar a encontrar problemas relacionados com clientes ou aplicações.

Para obter informações mais detalhadas sobre as utilizações do comando TRCTCPAPP com o LDAP, bem como as restrições em autoridades necessárias, consulte Descrição do Comando TRCTCPAPP (Rastrear Aplicação de TCP/IP).

Para obter informações gerais sobre a utilização de um rastreio de comunicações, consulte Rastreio de comunicações.

Utilizar a opção LDAP_OPT_DEBUG para rastrear erros

Pode utilizar a opção LDAP_OPT_DEBUG da API**ldap_set_option()** para rastrear problemas com clientes que estejam a utilizar as APIs de C de LDAP. A opção de depuração tem uma definição de vários níveis de depuração que pode utilizar para ajudar na resolução de problemas com estas aplicações.

Segue-se um exemplo da activação da opção de depuração do rastreio de clientes.

```
int debugvalue= LDAP_DEBUG_TRACE | LDAP_DEBUG_PACKETS;
ldap_set_option(  ld, LDAP_OPT_DEBUG, &debugvalue);
```

Uma forma alternativa de definir o nível de depuração é configurar o valor numérico da variável de ambiente `LDAP_DEBUG`, para o trabalho em que é executada a aplicação de cliente, como o mesmo valor numérico que o `debugvalue` teria se fosse utilizada a API **ldap_set_option()** .

Um exemplo da activação do rastreio de clientes utilizando a variável de ambiente LDAP_DEBUG é o seguinte:

```
ADDENVVAR ENVVAR(LDAP_DEBUG) VALUE(0x0003)
```

Após executar o cliente que causou o problema, escreva o seguinte na linha de comandos do iSeries:

```
DMPUSRTRC  ClientJobNumber
```

em que `ClientJobNumber` é o número do trabalho do cliente.

Para ver estas informações em modo interactivo, escreva o seguinte na linha de comandos do iSeries:

```
DSPPFM QAPOZDMP QP0Znnnnnn
```

em que `QAP0ZDMP` contém um zero e `nnnnnn` é o número do trabalho.

Para guardar estas informações de modo a enviar as informações para o serviço, execute os seguintes passos:

1. Crie um ficheiro SAVF utilizando o comando Criar SAVF (CRTSAVF).
2. Escreva o que se segue na linha de comandos do iSeries.

   ```
   SAVOBJ OBJ(QAP0ZDMP LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   em que `QAP0ZDMP` contém um zero e *xxx* é o nome que especificou para o ficheiro SAVF.

Erros comuns do cliente de LDAP

Conhecer as causas de erros comuns do cliente de LDAP pode ajudá-lo a resolver problemas com o servidor. Para obter uma lista completa de condições de erro de clientes de LDAP, consulte o tópico “APIs do Directory Server” em Programação, no iSeries Information Center.

As mensagens de erro do cliente têm o seguinte formato:

```
[Operação de LDAP em falha]:[Condições de erro da API do cliente de LDAP]
```

Nota: A explicação destes erros assume que o cliente está a comunicar com um servidor de LDAP no i5/OS. Um cliente que comunique com um servidor numa plataforma diferente pode obter erros semelhantes, mas as causas e soluções seriam, muito provavelmente, diferentes.

As mensagens comuns incluem as seguintes:

- "ldap_search: Limite de tempo excedido"
- "[Falha na operação de LDAP]: Erro nas operações"
- "ldap_bind: Não existe nenhum objecto desse tipo"
- "ldap_bind: Autenticação incorrecta"
- "[Erro no funcionamento de LDAP]: Acesso insuficiente" na página 173
- "[Falha na operação de LDAP]: Não é possível contactar o servidor de LDAP" na página 173
- "[operação de LDAP falhada]: Não foi possível ligar ao servidor de SSL" na página 173

ldap_search: Limite de tempo excedido

Este erro ocorre quando as ldapsearches estão a ser efectuadas muito lentamente. Para corrigir este erro, pode efectuar um ou ambos os procedimentos que se seguem:

- Aumentar o limite de tempo de pesquisa do Directory Server. Consulte"Ajustar definições de rendimento" na página 113 para obter informações sobre como executar esta operação.
- Reduzir a actividade no sistema. Pode igualmente reduzir o número de trabalhos activos do cliente de LDAP que estão a ser executados.

[Falha na operação de LDAP]: Erro nas operações

Este erro pode ter várias causas. Para obter informações sobre a causa deste erro numa ocorrência específica, consulte os registos de trabalhos QDIRSRV (tal como descrito em "Supervisionar erros e acesso com o registo de trabalhos do Directory Server" na página 170) e os registos de trabalhos do servidor de Structured Query Language (SQL) (tal como descrito em Capítulo 8, "Resolução de problemas do Directory Server", na página 169).

ldap_bind: Não existe nenhum objecto desse tipo

Uma causa comum para este erro é o utilizador cometer um erro de escrita ao efectuar uma operação. Outra causa comum acontece quando o cliente de LDAP tenta a ligação com um DN que não existe. Isto acontece com frequência quando o utilizador especifica o que erradamente pensa ser o DN do administrador. Por exemplo, o utilizador pode especificar `QSECOFR` ou `Administrador`, quando, na realidade, o DN do administrador pode ser algo como cn=Administrador.

Para obter detalhes sobre o erro, consulte o registo de trabalhos QDIRSRV tal como descrito em "Supervisionar erros e acesso com o registo de trabalhos do Directory Server" na página 170.

ldap_bind: Autenticação incorrecta

O servidor devolve Credenciais inválidas quando a palavra-passe ou DN de ligação está incorrecto. O servidor devolve Autenticação incorrecta quando o cliente tenta ligar como uma das seguintes opções:

- Uma entrada sem um atributo userpassword
- Uma entrada que represente um utilizador do i5/OS, com um atributo de ID do utilizador e não um atributo userpassword. Esta situação faz com que seja efectuada uma comparação entre a palavra-passe especificada e a palavra-passe de utilizador do i5/OS, que não correspondem.
- Quando tiver sido pedida uma entrada que represente um utilizador projectado e um método de ligação diferente do método simples.

Normalmente, este erro é provocado quando o cliente tenta ligar com uma palavra-passe inválida. Para obter detalhes sobre o erro, consulte o registo de trabalhos QDIRSRV tal como se encontra descrito na secção “Supervisionar erros e acesso com o registo de trabalhos do Directory Server” na página 170.

[Erro no funcionamento de LDAP]: Acesso insuficiente

Normalmente, este erro é provocado quando o DN de ligação não tem autoridade para efectuar a operação (por exemplo, adicionar ou eliminar) solicitada pelo cliente. Para obter informações sobre o erro, consulte o registo de trabalhos QDIRSRV tal como se encontra descrito em “Supervisionar erros e acesso com o registo de trabalhos do Directory Server” na página 170.

[Falha na operação de LDAP]: Não é possível contactar o servidor de LDAP

Entre as causas mais comuns deste erro incluem-se as seguintes:

- Um cliente de LDAP emite um pedido antes de o servidor de LDAP no sistema especificado estar a funcionar e no estado a aguardar selecção.
- O utilizador especifica o número de uma porta que não é válida. Por exemplo, o servidor está activado para a porta 386, mas o pedido do cliente tenta utilizar a porta 387.

Para obter informações sobre o erro, consulte o registo de trabalhos QDIRSRV tal como se encontra descrito em “Supervisionar erros e acesso com o registo de trabalhos do Directory Server” na página 170. Se o Directory Server tiver sido iniciado com êxito, a mensagem Servidor iniciado com êxito aparecerá no registo de trabalhos QDIRSRV.

[operação de LDAP falhada]: Não foi possível ligar ao servidor de SSL

Este erro ocorre quando o servidor de LDAP rejeita a ligação do cliente porque não é possível estabelecer uma ligação protegida ao terminal. Este erro pode ser causado por um dos seguintes:

- O suporte de Gestão de Certificados rejeita a tentativa do cliente para estabelecer ligação com o servidor. Utilize o Digital Certificate Manager para se assegurar de que os seus certificados estão correctamente configurados e, em seguida, reinicie o servidor e tente estabelecer a ligação novamente.
- O utilizador poderá não ter acesso de leitura ao local de armazenamento de certificados *SYSTEM (por valor assumido /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Para aplicações i5/OS C, estão disponíveis informações adicionais de erro de SSL. Consulte “APIs do Directory Server” no tópico Programação, para ver detalhes.

Capítulo 9. Referência

Consulte o seguinte para obter informações de referência adicionais.

- "Utilitários da linha de comandos"
- "Formato de permuta de dados de LDAP (LDIF)" na página 202
- "Esquema de configuração do Directory Server" na página 205

Utilitários da linha de comandos

Esta secção descreve os utilitários que podem ser executados a partir do ambiente de comandos da Qshell no i5/OS. Consulte os seguintes comandos para obter mais informações:

- "ldapmodify e ldapadd"
- "ldapdelete" na página 179
- "ldapexop" na página 181
- "ldapmodrdn" na página 185
- "ldapsearch" na página 188
- "ldapchangepwd" na página 196
- "ldapdiff" na página 198
- "Notas sobre a utilização de SSL com os utilitários da linha de comandos de LDAP" na página 201

Note que certas cadeias têm de estar entre aspas para serem processadas correctamente no ambiente de comandos da Qshell. Geralmente, estas cadeias são DNs, filtros de procura e a lista de atributos a devolver por ldapsearch. Consulte a lista que se segue para ver alguns exemplos.

- Cadeias que contêm espaços: `"cn=João Silva,cn=utilizadores"`
- Cadeias que contêm caracteres globais:`"*"`
- Cadeias que contêm parênteses: `"(objectclass=person)"`

Para obter mais informações sobre o ambiente de comandos da Qshell, consulte o tópico "Qshell".

ldapmodify e ldapadd

As ferramentas modify-entry e add-entry de LDAP

Resumo

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V]
[-w passwd | ?] [-Z]


ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-r] [-R] [-v] [-V] [-w passwd | ?]
[-Z]
```

Descrição

ldapmodify é uma interface da linha de comandos destinada às interfaces de programação de aplicações (APIs)ldap_modify, ldap_add, ldap_delete e ldap_modrdn.**ldapadd** é implementado como uma versão com novo nome de ldapmodify. Quando invocado como ldapadd, o sinalizador **-a** (adicionar nova entrada) é ligado automaticamente.

ldapmodify abre uma ligação a um servidor de LDAP, sendo ligado ao servidor. Pode utilizar**ldapmodify** para modificar ou adicionar entradas. As informações sobre a entrada são lidas do output padrão ou de um ficheiro, com a utilização da opção **-i**.

Se quiser ver ajuda para a sintaxe de **ldapmodify** ou **ldapadd**, escreva

```
ldapmodify -?
```

ou

```
ldapadd -?
```

Opções

-a Adicionar novas entradas. A acção assumida para **ldapmodify** é modificar as entradas existentes. Se invocado como **ldapadd**, este sinalizador está sempre definido.

-b Assuma que todos os valores que comecem por uma `/' são valores binários e que o valor real está num ficheiro cujo caminho está especificado em lugar do valor.

-c Modo de funcionamento contínuo. Os erros são comunicados, mas **ldapmodify** continua a efectuar modificações. Caso contrário, a acção assumida é sair após a comunicação de um erro.

-C *charset*
Especifica que as cadeias fornecidas como input aos utilitários **ldapmodify** e **ldapadd** são representadas num conjunto de caracteres local tal como especificado por charset, e têm de ser convertidas para UTF-8. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver os valores charset suportados.

-d *debuglevel*
Defina o nível de depuração de LDAP como debuglevel.

-D *binddn*
Utilize ***binddn*** para ligar ao directório de LDAP.***binddn*** é um DN representado por cadeia.

-h *ldaphost*
Especifique um sistema central alternativo no qual o servidor de ldap esteja em execução.

-i *file* Leia as informações sobre a modificação de entradas de um ficheiro de LDIF, em vez do input padrão. Se um ficheiro de LDIF não for especificado, tem de utilizar input padrão para especificar os registos de actualização em formato LDIF.

-k Especifica a utilização do controlo de administração do servidor.

-K *keyfile*
Especifique o nome do ficheiro de base de dados de chaves de SSL com a extensão assumida **kdb**. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves. Se não for especificado um nome de ficheiro de base de dados de chaves, este utilitário procurará primeiro a presença da variável de ambiente SSL_KEYRING com um nome de ficheiro associado. Se a variável de ambiente SSL_KEYRING não estiver definida, será utilizado o ficheiro de conjuntos de chaves mistas do sistema, se estiver presente.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-m *mechanism*

Utilize ***mechanism*** para especificar o mecanismo SASL a ser utilizado para estabelecer uma associação com o servidor. É utilizada a API ldap_sasl_bind_s(). O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.Os mecanismos válidos são:

- CRAM-MD5 - protege a palavra-passe enviada para o servidor.
- EXTERNAL - utiliza o certificado de SSL. Requer -Z.
- GSSAPI - utiliza as credenciais de Kerberos do utilizador

-M Gerir objectos de referência como entradas normais.

-N *certificatename*

Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. ***certificatename*** não é necessário se tiver sido designado um par certificado/chave privada como valor assumido para o ficheiro de base de dados de chaves. Do mesmo modo, o parâmetro ***certificatename*** não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-O *maxhops*

Especifique ***maxhops*** para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar ao procurar referências. A contagem de sistemas de passagem assumida é 10.

-p *ldapport*

Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado **-p** e estiver especificado **-Z**, será utilizada a porta de SSL de LDAP assumida 636.

-P *keyfilepw*

Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é necessária para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-r Substituir os valores existentes pelos valores assumidos.

-R Especifica que as consultas não devem ser seguidas automaticamente.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-V Especifica a versão de LDAP a ser utilizada por **ldapmodify** quando for ligado ao servidor de LDAP. Por valor assumido, é estabelecida uma ligação de LDAP V3. Para seleccionar explicitamente o LDAP V3, especifique **-V 3**. Especifique **-V 2** para trabalhar com uma aplicação de LDAP V2.

-w *passwd* | **?**

Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

Formato de input

O conteúdo do ficheiro (ou input padrão se não for indicado nenhum sinalizador **-i** na linha de comandos) deverá ser conforme ao formato LDIF. Consulte “Formato de permuta de dados de LDAP (LDIF)” na página 202 para obter mais informações sobre o formato LDIF.

Exemplos

Partindo do princípio de que o ficheiro /tmp/entrymods existe e tem o seguinte conteúdo:

```
dn: cn=Modificar Utilizador, o=Universidade de Estudos Superiores, c=PO
changetype: modify
replace: mail
mail: modutilizador@estudante.de.arte.edu
-
add: title
title: Grande Mestre
-
add: jpegPhoto
jpegPhoto: /tmp/modutilizador.jpeg
-
delete: description
-
```

o comando:

```
ldapmodify -b -r -i /tmp/entrymods
```

substituirá o conteúdo do atributo mail da entrada Modificar Utilizador pelo valor modutilizador@estudante.de.arte.edu, adicionará um título de Grande Mestre e o conteúdo do ficheiro /tmp/modutilizador.jpeg como jpegPhoto e removerá completamente o atributo description. Estas mesmas modificações podem ser executadas com a utilização do formato de input de ldapmodify mais antigo:

```
cn=Modificar Utilizador, o=Universidade de Estudos Superiores, c=PO
mail=modutilizador@estudante.de.arte.edu
+title=Grande Mestre
+jpegPhoto=/tmp/modutilizador.jpeg
-description
```

e o comando:

```
ldapmodify -b -r -i /tmp/entrymods
```

Partindo do princípio de que o ficheiro /tmp/newentry existe e que tem o seguinte conteúdo:

```
dn: cn=Joaquim Dias, o=Universidade de Estudos Superiores, c=PO
objectClass: person
      cn: Joaquim Dias
cn: Quim
      sn: Dias
title: a pessoa mais misteriosa do mundo
mail: joaquimdias@estudante.de.arte.edu
UID: jdias
```

o comando:

```
 ldapadd -i /tmp/entrymods
```

adiciona uma nova entrada para Joaquim Dias, utilizando os valores do ficheiro /tmp/newentry.

Notas

Se não forem fornecidas informações de entrada pelo ficheiro através da utilização da opção **-i**, o comando **ldapmodify** aguardará para ler entradas do output padrão.

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapdelete

A ferramenta delete-entry de LDAP

Resumo

```
ldapdelete [-c] [-C charset] [-d debuglevel][-D binddn][-i file]
[-h ldaphost] [-k] [-K keyfile] [-m mechanism] [-M] [-n] [-N certificatename]
[-O maxops] [-p ldapport] [-P keyfilepw] [-R] [-s][-v] [-V version]
[-w passwd | ?] [-Z] [dn]...
```

Descrição

ldapdelete é uma interface da linha de comandos destinada à interface de programação de aplicações (API)ldap_delete.

ldapdelete abre uma ligação a um servidor de LDAP, liga e elimina uma ou mais entradas. Se for fornecido um ou mais argumentos de Nome exclusivo (DN), as entradas com esses DNs serão eliminadas. Cada DN é um DN representado por cadeia. Se não forem fornecidos argumentos de DN, uma lista de DNs será lida do input padrão ou de um ficheiro, se for utilizado o sinalizador **-i**.

Se quiser ver ajuda para a sintaxe de **ldapdelete** ou **ldapadd**, escreva

```
ldapdelete -?
```

Opções

-c Modo de funcionamento contínuo. Os erros são comunicados, mas **ldapdelete** continua a efectuar modificações. Caso contrário, a acção assumida é sair após a comunicação de um erro.

-C *charset*
Especifica que os DNs fornecidos como input ao utilitário **ldapdelete** estão representados num conjunto de caracteres local, tal como especificado por charset. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver os valores charset suportados.

-d *debuglevel*
Defina o nível de depuração de LDAP como debuglevel.

-D *binddn*
Utilize ***binddn*** para ligar ao directório de LDAP.***binddn*** é um DN representado por cadeia.

-h *ldaphost*
Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.

-i *file* Leia um conjunto de linhas do ficheiro, efectuando uma eliminação de LDAP em cada linha do ficheiro. Cada linha do ficheiro deverá conter um único nome exclusivo.

-k Especifica a utilização do controlo de administração do servidor.

-K *keyfile*
Especifique o nome do ficheiro da base de dados de chaves de SSL. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

Se o utilitário não conseguir localizar uma base de dados de chaves, usará um conjunto de código incorporado de raízes de autoridade de certificados fidedignas assumidas. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (ACs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-m *mechanism*
Utilize ***mechanism*** para especificar o mecanismo SASL a ser utilizado para estabelecer uma associação com o servidor. O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.

-M Gerir objectos de referência como entradas normais.

-n Mostra o procedimento que seria executado, mas, na realidade, não modifica entradas. É útil para efectuar a depuração, conjuntamente com a opção **-v**.

-N *certificatename*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. O parâmetro ***certificatename*** não será necessário se tiver sido designado um certificado assumido/par de chaves privado como o valor assumido. Do mesmo modo, o parâmetro ***certificatename*** não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-O *maxhops*
Especifique ***maxhops*** para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar ao procurar referências. A contagem de sistemas de passagem assumida é 10.

-p *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de LDAP irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado **-p** e estiver especificado **-Z**, será utilizada a porta de SSL de LDAP assumida 636.

-P *keyfilepw*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é obrigatória para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-R Especifica que as consultas não devem ser seguidas automaticamente.

-s Utilize esta opção para eliminar a sub-árvore encaminhada para a entrada especificada.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-V Especifica a versão de LDAP a ser utilizada por **ldapdelete** quando for ligado ao servidor de LDAP. Por valor assumido, é estabelecida uma ligação de LDAP V3. Para seleccionar explicitamente o LDAP V3, especifique **-V 3**. Especifique **-V 2** para trabalhar com uma aplicação de LDAP V2.

-w *passwd* | **?**
Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

dn Especifica um ou mais argumentos de DN. Cada DN deverá ser um DN representado por cadeia.

Exemplos

O comando seguinte,

```
ldapdelete -D cn=administrador -w secreta "cn=Eliminar Utilizador, o=Universidade de Arte, c=PO"
```

tenta eliminar uma entrada com o commonName ″Eliminar Utilizador″ directamente abaixo da entrada organizacional Universidade de Arte.

Notas

Se não forem fornecidos argumentos de DN, o comando **ldapdelete** aguarda para ler uma lista de DNs do input padrão.

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapexop

A ferramenta de operações expandidas de LDAP

Resumo

```
ldapexop [-C charset] [-d debuglevel][-D binddn][-e] [-h ldaphost]
[-help][-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-v] [-w passwd | ?] [-Z]
-op {cascrepl | controlqueue | controlrepl |
quiesce | readconfig}
```

Descrição

O utilitário **ldapexop** é uma interface de linha de comandos que permite estabelecer ligação com um Directory Server e emitir uma única operação expandida juntamente com quaisquer dados que formem o valor da operação expandida.

O utilitário **ldapexop** suporta o sistema central, a porta, SSL e opções de autenticação padrão usados por todos os utilitários de cliente de LDAP. Além disso, está definido um conjunto de opções para especificar a operação a executar e os argumentos para cada operação expandida.

Para ver a ajuda para a sintaxe de **ldapexop**, escreva:

```
ldapexop -?
```

ou

```
ldapexop -help
```

Opções

As opções para o comando ldapexop estão divididas em duas categorias:

1. Opções gerais que especificam como ligar ao Directory Server. Estas opções têm de ser especificadas antes das opções específicas das operações.
2. Opção de operação expandida que identifica a operação expandida a ser executada.

Opções Gerais

Estas opções especificam os métodos de ligação ao servidor e têm de ser especificadas antes da opção **-op**.

-C *charset*
Especifica que os DNs fornecidos como input ao utilitário **ldapexop** estão representados num conjunto de caracteres local, tal como especificado por charset. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver os valores charset suportados.

-d *debuglevel*
Defina o nível de depuração de LDAP como debuglevel.

-D *binddn*
Utilize ***binddn*** para ligar ao directório de LDAP.***binddn*** é um DN representado por cadeia.

-e Apresenta as informações sobre a versão da biblioteca de LDAP e, em seguida, sai.

-h *ldaphost*
Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.

-help Apresenta a sintaxe do comando e informações de utilização.

-K *keyfile*
Especifique o nome do ficheiro da base de dados de chaves de SSL. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

Se o utilitário não conseguir localizar uma base de dados de chaves, será utilizada a base de dados de chaves do sistema. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (ACs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-m *mechanism*
Utilize ***mechanism*** para especificar o mecanismo SASL a ser utilizado para estabelecer uma associação com o servidor. Será utilizada a API ldap_sasl_bind_s(). O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.

-N *certificatename*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. O parâmetro ***certificatename*** não será necessário se tiver sido designado um certificado assumido/par de chaves privado como o valor assumido. Do mesmo modo, o parâmetro ***certificatename*** não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-p *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de LDAP irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado **-p** e estiver especificado **-Z**, será utilizada a porta de SSL de LDAP assumida 636.

-P *keyfilepw*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é obrigatória para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-? Apresenta a sintaxe do comando e informações de utilização.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-w *passwd* **| ?**
Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

Opção de operações expandidas

A opção **-op** de operações expandidas identifica a operação expandida a executar. A operação expandida pode ter um dos seguintes valores:

- **cascrepl**: operação expandida de replicação de controlo em cascata. A acção pedida é aplicada ao servidor especificado e transferida juntamente com todas as réplicas da sub-árvore indicada. Se algumas destas réplicas forem de reencaminhamento, elas passam a operação expandida directamente para as respectivas réplicas. A operação é disposta em cascata sobre toda a topologia de replicação.

  -action quiesce | unquiesce | replnow | wait
  Este é um atributo obrigatório que especifica a acção a executar.

  quiesce
  Não são permitidas actualizações adicionais, excepto por replicação.

  unquiesce
  Retomar a operação normal, sendo aceites replicações de clientes.

  replnow
  Replicar todas as alterações colocadas na fila para todos os servidores de réplica, o mais rapidamente possível, seja qual for a data da marcação.

  wait Aguardar que todas as actualizações sejam replicadas para todas as réplicas.

  -rc *contextDn*
  Este é um atributo obrigatório que especifica a raiz da sub-árvore.

  -timeout *secs*
  Este é um atributo opcional que, se estiver presente, especifica o período de tempo de espera em segundos. Se não estiver, ou se for 0, a operação aguarda indefinidamente.

  Exemplo:

```
ldapexop -op cascrepl -action -quiesce -rc "o=empresa,c=po" -timeout 60
```

- **controlqueue**: operação expandida de replicação de fila de controlo. Esta operação permite eliminar ou remover alterações pendentes da lista de alterações de replicação que se acumularam na fila e que não foram executadas devido a falhas de replicação. Esta operação é útil quando os dados de réplica são corrigidos manualmente. Esta operação deve ser utilizada para não cometer algumas das falhas acumuladas na fila.

  -skip all | change-id
  Este atributo é obrigatório.
  - **all** indica que deverão ser ignoradas todas as alterações pendentes referentes a este acordo.
  - **change-id** identifica a única alteração a ser ignorada. Se o servidor não estiver presentemente a replicar esta alteração, o pedido falhará.

  -ra *agreementDn*
  Este é um atributo obrigatório que especifica o DN do acordo de replicação.

  Exemplos:

```
ldapexop -op controlqueue -skip all -ra "cn=servidor3,
             ibm-replicaSubentry=principal1-id,ibm-replicaGroup=valor assumido,
             o=empresa,c=po"
ldapexop -op controlqueue -skip 2185 -ra "cn=servidor3,
             ibm-replicaSubentry=principal1-id,ibm-replicaGroup=valor assumido,
             o=empresa,c=po"
```

- **controlrepl**: operação expandida de replicação de controlo

  -action suspend | resume | replnow
  Este é um atributo obrigatório que especifica a acção a executar.

  -rc *contextDn* | **-ra** *agreementDn*
  O **-rc** *contextDn* é o DN do contexto de replicação. A acção é executada para todos os acordos para este contexto. O **-ra** *agreementDn* é o DN do acordo de replicação. A acção é executada para o acordo de replicação especificado.

  Exemplo:

```
ldapexop -op controlrepl -action suspend -ra "cn=servidor3,
             ibm-replicaSubentry=principal1-id,ibm-replicaGroup=valor assumido,
             o=empresa,c=po"
```

- **quiesce**: operação expandida de replicação de controlo de desactivação ou activação

  -rc *contextDn*
  Este é um atributo obrigatório que especifica o DN do contexto de replicação (sub-árvore) a desactivar ou activar.

  -end Este é um atributo opcional que, se estiver presente, especifica a activação da sub-árvore. Se não for especificado, o valor assumido é desactivar a sub-árvore.

  Exemplos:

```
ldapexop -op quiesce -rc "o=empresa,c=po"

ldapexop -op quiesce -end -rc "o=ibm,c=po"
```

- **readconfig**: operação expandida do ficheiro de configuração de nova leitura

  -scope entire | single<*DN da entrada***><***atributo***>**
  Este atributo é obrigatório.
  - **entire** indica que todo o ficheiro de configuração deverá ser lido de novo.
  - **single** significa que só deverá ser lida a entrada simples e o atributo especificado.

  Exemplos:

```
ldapexop -op readconfig -scope entire

ldapexop -op readconfig -scope single "cn=configuração" ibm-slapdAdminPW
```

  Nota: As entradas seguintes marcadas com:
  - [1] entram em vigor imediatamente
  - [2] entram em vigor em novas operações
  - [3] entram em vigor assim que a palavra-passe for alterada (não é necessário readconfig)
  - [4] são suportadas pelo utilitário de linha de comandos no i5/OS, mas não são suportadas pelo Directory Server no i5/OS

```
cn=Configuraçãoibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3, 4]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]
cn=Computador Principal, cn=Configuração
```

```
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]
cn=Notificação de Acontecimentos, cn=Configuração
ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]
cn=Transacção, cn=Configuração
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]
cn=ConfigDB, cn=Prog. Emissores Conf., cn=IBM SecureWay, cn=Esquemas, cn=Configuração
ibm-slapdreadonly[2]
cn=Directório, cn=Prog. Emissores de RDBM, cn=IBM SecureWay, cn=Esquemas, cn=Configuração
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapmodrdn

A ferramenta de RDN de modificação de entrada de LDAP

Resumo

```
ldapmodrdn [-c] [-C charset] [-d debuglevel][-D binddn] [-h ldaphost]
[-i file] [-k] [-K keyfile] [-m mechanism] [-M] [-n]
[-N certificatename] [-O hopcount] [-p ldapport] [-P keyfilepw]
[-r] [-R] [-v] [-V] [-w passwd | ?] [-Z] [dn newrdn | [-i file]]
```

Descrição

ldapmodrdn é uma interface da linha de comandos destinada à interface de programação de aplicações (API) ldap_modrdn.

ldapmodrdn abre uma ligação a um servidor de LDAP, liga e modifica o RDN das entradas. As informações sobre a entrada são lidas do input padrão, de um ficheiro através da utilização da opção **- f** ou do par dn e rdn da linha de comandos.

Consulte “Nomes exclusivos (DNs)” na página 11 para obter informações sobre RDNs (Nomes exclusivos relativos) e DNs (Nomes exclusivos).

Se quiser ver ajuda para a sintaxe de **ldapmodrdn**, escreva:

```
ldapmodrdn -?
```

Opções

-c Modo de funcionamento contínuo. Os erros são comunicados, mas **ldapmodrdn** continua a efectuar modificações. Caso contrário, a acção assumida é sair após a comunicação de um erro.

-C *charset*

Especifica que as cadeias fornecidas como input ao utilitário **ldapmodrdn** são representadas num conjunto de caracteres local, tal como especificado porcharset. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver valores charset suportados. Note que os valores suportados para charset são os mesmos que são suportados para o controlo charset que pode ser definido nos ficheiros de LDIF Versão 1.

-d *debuglevel*

Defina o nível de depuração de LDAP como debuglevel.

-D *binddn*

Utilize ***binddn*** para ligar ao directório de LDAP.binddn deverá ser um DN representado por cadeia.

-h *ldaphost*

Especifique um sistema central alternativo no qual o servidor de ldap esteja em execução.

-i *file* Leia as informações de modificação da entrada de um ficheiro em vez do input padrão ou da linha de comandos (especificando rdn e newrdn). O input padrão pode ser fornecido a partir de um ficheiro, bem como ("< ficheiro").

-k Especifica a utilização do controlo de administração do servidor.

-K *keyfile*

Especifique o nome do ficheiro da base de dados de chaves de SSL. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

Se o utilitário não conseguir localizar uma base de dados de chaves, usará um conjunto de código incorporado de raízes de autoridade de certificados fidedignas assumidas. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (ACs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-m *mechanism*

Utilize ***mechanism*** para especificar o mecanismo SASL a ser utilizado para estabelecer uma associação com o servidor. É utilizada a API ldap_sasl_bind_s(). O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.

-M Gerir objectos de referência como entradas normais.

-n Mostra o procedimento que seria executado, mas, na realidade, não modifica entradas. É útil para efectuar a depuração, conjuntamente com a opção **-v**.

-N *certificatename*

Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Note que, se o servidor de LDAP estiver configurado para executar apenas a autenticação do servidor, não será necessário um certificado do cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. O parâmetro ***certificatename*** não será necessário se tiver sido designado um certificado assumido/par de chaves privado como o valor assumido. Do mesmo modo, o parâmetro ***certificatename*** não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-O *hopcount*
Especifique ***hopcount*** para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar ao procurar referências. A contagem de sistemas de passagem assumida é 10.

-p *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificada e a opção -Z tiver sido especificada, será utilizada a porta 636 assumida de SSL de LDAP.

-P *keyfilepw*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é requerida para aceder às informações codificadas existentes no ficheiro de base de dados de chaves (o qual pode incluir uma ou mais chaves privadas). Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-r Remova valores de RDN antigos da entrada. A acção assumida é manter os valores antigos.

-R Especifica que as consultas não devem ser seguidas automaticamente.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-V Especifica a versão de LDAP a ser utilizada por **ldapmodrdn** quando for ligado ao servidor de LDAP. Por valor assumido, é estabelecida uma ligação de LDAP V3. Para seleccionar explicitamente o LDAP V3, especifique **-V 3**. Especifique **-V 2** para trabalhar com uma aplicação de LDAP V2. Uma aplicação, como **ldapmodrdn**, selecciona LDAP V3 como o protocolo preferencial utilizando ldap_init em vez deldap_open.

-w *passwd* **| ?**
Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

dn newrdn
Consulte a seguinte secção, “Formato de input para o dn newrdn” para obter mais informações.

Formato de input para o dn newrdn

Se forem fornecidos os argumentos de linha de comandos*dn* e *newrdn*, *newrdn* substitui o RDN da entrada especificada pelo DN, *dn*. Caso contrário, o conteúdo do ficheiro (ou input padrão se não for fornecido nenhum sinalizador **- i**) consistirá numa ou mais entradas:

```
Nome exclusivo (DN)

Nome exclusivo relativo (RDN)
```

Pode ser utilizada uma ou mais linhas em branco para separar cada par de DN e RDN.

Exemplos

Partindo do princípio de que o ficheiro /tmp/entrymods existe e tem o seguinte conteúdo:

```
cn=Modificar
Utilizador, o=Universidade de Arte, c=PO
cn=O Novo Utilizador
```

o comando:

```
ldapmodrdn -r -i /tmp/entrymods
```

altera o RDN da entrada `Modificar Utilizador` de `Modificar Utilizador` para `O Novo Utilizador` e o cn antigo, `Modificar Utilizador`, é removido.

Notas

Se não forem fornecidas informações sobre a entrada a partir de ficheiro através da utilização da opção **-i** (ou do par *dn* e *rdn* da linha de comandos), o comando **ldapmodrdn** aguarda para ler entradas do input padrão.

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapsearch

A ferramenta e programa exemplo de procura de LDAP

Resumo

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-F sep] [-h ldaphost] [-i file] [-K keyfile] [-l timelimit] [-L]
[-m mechanism] [-M] [-n] [-N certificatename][-o attr_type] [-O maxhops]
[-p ldapport] [-P keyfilepw] [-q pagesize]  [-R] [-s scope ] [-t] [-T seconds]
[-v] [-V version] [-w passwd | ?] [-z sizelimit] [-Z] filter [attrs...]
```

Descrição

ldapsearch é uma interface de linha de comandos destinada à interface de programação de aplicações (API) ldap_search.

ldapsearch abre uma ligação a um servidor de LDAP, liga e executa uma procura com a utilização do filtro. O filtro deverá estar em conformidade com a representação de cadeia para filtros de LDAP (consulte ldap_search nasAPIs do Directory Server para obter mais informações sobre filtros).

Se **ldapsearch** encontrar uma ou mais entradas, os atributos especificados por attrs serão obtidos e as entradas e valores serão impressos no output padrão. Se não forem mostrados attrs, serão devolvidos todos os atributos.

Para ver ajuda para a sintaxe de**ldapsearch**, escreva `ldapsearch -?`.

Opções

-a deref
Especifique o modo como será feita a remoção de referências a nomes alternativos. deref deverá ser nunca, sempre, procurar ou localizar, para especificar que a referência aos nomes alternativos nunca é retirada, é sempre retirada, é retirada durante a procura ou é retirada apenas ao localizar o objecto base para a procura. O valor assumido é nunca retirar a referência a nomes alternativos.

-A Obtenha apenas atributos (nenhum valor). Isto é útil quando só pretende ver se um atributo existe numa entrada e não está interessado nos valores específicos.

-b searchbase
Utilize searchbase como ponto de partida para a procura, em vez do valor assumido. Se **-b** não for especificado, este utilitário procurará, na variável de ambiente LDAP_BASEDN, uma definição de searchbase. Se nenhum estiver definido, o valor base assumido será definido como "".

-B Não suprima a apresentação de valores não ASCII. Isto é útil para processar valores que apareçam em conjuntos de caracteres alternativos como, por exemplo, ISO-8859.1. Esta opção está implícita na opção **-L**.

-C charset

Especifica que as cadeias fornecidas como input ao utilitário Idapsearch estão representadas num conjunto de caracteres local (tal como especificado por charset). O input de cadeias inclui o filtro, o DN de ligação e o DN base. De modo semelhante, quando está a apresentar os dados, **ldapsearch** converte os dados recebidos do servidor de LDAP para o conjunto de caracteres especificado. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver os valores charset suportados. Além disso, se as opções **-C** e**-L** forem ambas especificadas, assume-se que o input se encontra no conjunto de caracteres especificado, mas o output de **ldapsearch** é sempre preservado na respectiva representação UTF-8 ou numa representação codificada em base-64 dos dados quando são detectados caracteres não imprimíveis. É este o caso, uma vez que os ficheiros de LDIF padrão apenas contêm representações em UTF-8 (UTF-8 codificado em base-64) dos dados de cadeias. Note que os valores suportados para charset são os mesmos que são suportados para o controlo charset que pode ser definido nos ficheiros de LDIF Versão 1.

-d debuglevel

Defina o nível de depuração de LDAP como debuglevel.

-D binddn

Utilize binddn para ligar ao directório de LDAP. binddn deverá ser um DN representado por cadeia DN (consulte Nomes exclusivos de LDAP).

-e Apresenta as informações sobre a versão da biblioteca de LDAP e, em seguida, sai.

-F sep Utilize sep como o separador de campos entre nomes e valores de atributos. O separador assumido é `=', a menos que o sinalizador **-L** tenha sido especificado, caso em que esta opção é ignorada.

-h ldaphost

Especifique um sistema central alternativo no qual o servidor de ldap esteja em execução.

-i file Leia um conjunto de linhas do ficheiro, executando uma procura de LDAP em cada linha do ficheiro. Neste caso, o filtro fornecido na linha de comandos é tratado como um padrão em que a primeira ocorrência de %s é substituída por uma linha do ficheiro. Se o ficheiro for um único carácter "-", as linhas serão lidas no input padrão.

-K keyfile

Especifique o nome do ficheiro da base de dados de chaves de SSL. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

Se o utilitário não conseguir localizar uma base de dados de chaves, usará um conjunto de código incorporado de raízes de autoridade de certificados fidedignas assumidas. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (ACs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-l timelimit

Aguarde, no máximo, os segundos indicados em "timelimit" até que a procura seja concluída.

-L Visualize os resultados da procura no formato de LDIF. Esta opção activa igualmente a opção **-B** e faz com que a opção **-F** seja ignorada.

-m mechanism

Utilize mechanism para especificar o mecanismo de SASL a utilizar para ligar ao servidor. Será utilizada a API ldap_sasl_bind_s(). O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.

-M Gerir objectos de referência como entradas normais.

-n Mostra o procedimento que seria executado, mas, na realidade, não modifica entradas. É útil para efectuar a depuração, conjuntamente com a opção **-v**.

-N certificatename
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves.

Nota: Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. O parâmetro *certificatename* não será necessário se tiver sido designado um certificado assumido/par de chaves privado como o valor assumido.Do mesmo modo, o parâmetro *certificatename* não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado.Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-o *attr_type*
Para especificar um atributo a utilizar para ordenar critérios dos resultados da procura, pode utilizar o parâmetro -o (ordenar). Pode utilizar vários parâmetros -o para definir mais detalhadamente a sequência de ordenação. No exemplo seguinte, os resultados da procura são ordenados primeiro por apelido (sn), depois, por nome indicado, sendo o nome indicado (givenname) ordenado na sequência contrária (descendente), tal como especificado pelo sinal de menos com prefixo (-):

```
-o sn -o -givenname
```

Assim, a sintaxe do parâmetro de ordenação é a seguinte:

```
[-]<nome do atributo>[:<OID da regra de correspondência>]
```

em que

- `nome do atributo` é o nome do atributo pelo qual pretende ordenar.
- `OID da regra de correspondência` é o OID opcional de uma regra de correspondência que pretende utilizar para a ordenação. O atributo OID da regra de correspondência não é suportado pelo Directory Server, embora outros servidores de LDAP possam suportar este atributo.
- O sinal menos (-) indica que os resultados podem ser ordenados no sentido contrário.
- O nível de gravidade é sempre crítico.

A operação ldapsearch assumida é não ordenar os resultados devolvidos.

-O maxhops
Especifique maxhops para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar ao procurar referências. A contagem de sistemas de passagem assumida é 10.

-p ldapport
Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificada e a opção -Z tiver sido especificada, será utilizada a porta 636 assumida de SSL de LDAP.

-P keyfilepw
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é requerida para aceder às informações codificadas existentes no ficheiro de base de dados de chaves (o qual pode incluir uma ou mais chaves privadas). Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-q *pagesize*

Para especificar a paginação dos resultados da procura, podem ser utilizados dois parâmetros: -q (tamanho de página de consulta) e -T (tempo entre procuras em segundos). No exemplo que se segue, os resultados da procura devolvem uma página (25 entradas) de cada vez, de 15 em 15 segundos, até serem devolvidos todos os resultados dessa procura. O cliente de ldapsearch gere toda a continuação da ligação para cada pedido de resultados por página, enquanto durar a operação de procura.

Estes parâmetros podem ser úteis quando o cliente dispõe de recursos limitado ou quando está ligado através de uma ligação de banda estreita.Em geral, permite controlar a velocidade à qual os dados são devolvidos por um pedido de procura. Em vez de receber todos os resultados de uma só vez, pode obtê-los num conjunto de entradas (uma página) de cada vez. Além disso, pode controlar a duração do intervalo de tempo entre cada pedido de página, concedendo ao cliente tempo suficiente para processar os resultados.

```
-q 25  -T 15
```

e o parâmetro -v (verboso) for especificado, ldapsearch mostra uma lista das entradas que foram devolvidas até aqui, após cada página de entradas devolvida pelo servidor como, por exemplo, **foram devolvidas 30 entradas no total.**

São activados vários parâmetros -q, para poder especificar tamanhos de página diferentes ao longo da duração de uma única operação de procura. No exemplo que se segue, a primeira página tem 15 entradas, a segunda página tem 20 e o terceiro parâmetro termina o resultado por página/operação de procura:

```
-q 15 -q 20 -q 0
```

No exemplo que se segue, a primeira página tem 15 entradas e todas as restantes páginas têm 20 entradas, continuando com o último valor **-q** especificado até a operação de procura terminar:

```
-q 15 -q 20
```

A operação ldapsearch assumida é devolver todas as entradas num único pedido. Não é executada a paginação na operação ldapsearch assumida.

-R Especifica que as consultas não devem ser seguidas automaticamente.

-s scope

Especifique o âmbito da procura. scope deve ser base, um ou sub, para especificar uma procura de objecto base, de um nível ou de sub-árvore. O valor assumido é sub.

-t Escreva valores obtidos num conjunto de ficheiros temporários. Isto é útil para processar valores não ASCII, como jpegPhoto ou áudio.

-T *segundos*

Tempo entre procuras (em segundos). A opção **-T** só é suportada quando a opção **-q** é especificada.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-V Especifica a versão de LDAP a ser utilizada por ldapmodify quando for ligada ao servidor de LDAP. Por valor assumido, é estabelecida uma ligação de LDAP V3. Para seleccionar explicitamente LDAP V3, especifique ″-V 3″. Especifique ″-V 2″ para trabalhar com uma aplicação de LDAP V2. Uma aplicação, como ldapmodify, selecciona LDAP V3 como o protocolo preferencial utilizando ldap_init em vez de ldap_open.

-w *passwd* | **?**

Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe. .

-z sizelimit
Limita os resultados da procura a um máximo de entradas com sizelimit. Isto possibilita a colocação de um limite superior ao número de entradas que são devolvidas para uma operação de procura.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

filtro Especifica uma representação de cadeia do filtro a aplicar na procura. Os filtros simples podem ser especificados como attributetype=attributevalue. Os filtros mais complexos são especificados com a utilização de uma notação de prefixo de acordo com o seguinte Backus Naur Form (BNF):

```
<filter> ::='('<filtercomp>')'
<filtercomp> ::= <and>|<or>|<not>|<simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter>|<filter><filterlist>
<simple> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

A construção '~=' é utilizada para especificar correspondências aproximadas. A representação de *<attributetype>* e *<attributevalue>* está descrita no "RFC 2252, LDAP V3 Attribute Syntax Definitions" . Além disso, se o tipo de filtro for '=', *<attributevalue>* pode ser um único *, para se obter um teste de existência de atributo, ou pode conter texto e asteriscos (*) intercalados, para se obter a correspondência de subcadeias.

Por exemplo, o filtro "mail=*" encontra todas as entradas que tenham um atributo mail. O filtro "mail=*@estudante.de.arte.edu" encontra todas as entradas que tenham um atributo mail terminado pela cadeia especificada. Para colocar parênteses num filtro, introduza uma barra invertida (\).

Nota: Um filtro como `"cn=Paulo *"`, onde existe um espaço entre Paulo e o asterisco (*), corresponde a "Paulo Cardoso", mas não a "Paulinho Cardoso" no Directório da IBM. O espaço entre "Paulo" e o carácter global (*) afecta o resultado de uma procura com filtros.

Consulte "RFC 2254, A String Representation of LDAP Search Filters" para obter uma descrição mais completa dos filtros permitidos.

Formato de output

Se for encontrada uma ou mais entradas, cada entrada será escrita no seguinte formato de output padrão:

```
Nome exclusivo (DN)

attributename=valor

attributename=valor

attributename=valor

...
```

Múltiplas entradas são separadas por uma linha em branco simples. Se a opção **-F** for utilizada para especificar um carácter separador, ela será utilizada em vez do carácter `=`. Se for utilizada a opção **-t**, será utilizado o nome de um ficheiro temporário em vez do valor real. Se for fornecida a opção **-A**, só será escrita a parte do "attributename".

Exemplos

O comando seguinte:

```
ldapsearch "cn=joaquim dias" cn telephoneNumber
```

executa uma procura na sub-árvore (utilizando a base de procura assumida) para entradas com um commonName ″joaquim dias″. Os valores commonName e telephoneNumber são obtidos e impressos no output padrão. O output poderá ser semelhante ao seguinte, se forem encontradas duas entradas:

```
  cn=Joaquim Dias, ou="Universidade de Literatura, Ciência e Artes",
ou=Estudantes, ou=Pessoas, o=Universidade de Estudos Superiores, c=PO

  cn=Joaquim Dias

  cn=Joaquim Eduardo Dias

  cn=Joaquim E Dias 1

  cn=Joaquim E Dias

  telephoneNumber=+1 313 555-5432



  cn=Joaquim B Dias, ou=Departamento de Tecnologia de Informações,
ou=Sector e Pessoal, ou=Pessoas, o=Universidade de Estudos Superiores, c=PO

  cn=Joaquim Dias

  cn=Joaquim B Dias 1

  cn=Joaquim B Dias

  telephoneNumber=+1 313 555-1111
```

O comando:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

executa uma procura na sub-árvore com a utilização da base de procura assumida para entradas com o id de utilizador ″jed″. Os valores jpegPhoto e audio são obtidos e escritos em ficheiros temporários. O output pode ser semelhante ao seguinte, se for encontrada uma entrada com um valor para cada um dos atributos pedidos:

```
cn=Joaquim E Dias, ou=Departamento de Tecnologia de Informações,

ou=Sector e Pessoal,

ou=Pessoas, o=Universidade de Estudos Superiores, c=PO

audio=/tmp/ldapsearch-audio-a19924

jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

O comando:

```
ldapsearch -L -s one -b "c=PO" "o=universidade*" o description
```

executa uma procura de um nível no nível c=PO para todas as organizações cujo organizationName comece por universidade. Os resultados da procura serão apresentados no formato LDIF (consulte Formato de Permuta de Dados de LDAP). Os valores de atributo organizationName e description serão obtidos e impressos no output padrão, o que resulta num output semelhante a:

```
dn:
o=Universidade de Viseu, c=PO

o: Universidade de Viseu

description: Preparar Viseu para os desafios do amanhã

description: apenas nó de folhas


dn: o=Universidade de Lisboa em Faro, c=PO

o: Universidade de Lisboa em Faro

description: Não existem informações sobre o pessoal

description: Instituição de educação e pesquisa


dn: o=Universidade de Lisboa em Faro, c=PO

o: Universidade de Lisboa em Faro

o: ULF

o: UL/Faro

o: CU-Faro

description: Instituto de Estudos Superiores e Pesquisa


dn: o=Universidade de Évora, c=PO

o: Universidade de Évora

o: UEl

description: Orientador de mentes jovens


 ...
```

O comando:

```
ldapsearch -b "c=PO" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

executa uma procura ao nível da sub-árvore, no nível c=PO, para todas as pessoas. Este atributo especial (ibm-slapdDN), quando utilizado para procuras ordenadas, ordena os resultados da procura pela representação de cadeia do Nome exclusivo (DN). O output poderá ser semelhante a:

```
cn=Gil Esteves,ou=Departamento de Mecânica,ou=Almada,o=IBM,c=PO

cn=Alberto Garcia,ou=Entretenimento Doméstico,ou=Almada,o=IBM,c=PO

cn=Ana Gomes,ou=Sistemas de Voo,ou=Almada,o=IBM,c=PO

cn=Artur Eduardo,ou=Departamento de Mecânica,ou=Almada,o=IBM,c=PO

cn=Berta Garcia,ou=Sistemas de Voo,ou=Almada,o=IBM,c=PO

cn=Rui Crato,ou=Sistemas de Voo,ou=Almada,o=IBM,c=PO
```

```
cn=Rui Garcia Jr,ou=Entretenimento Doméstico,ou=Almada,o=IBM,c=PO

cn=Bruno Chelas Jr.,ou=Sistemas de Voo,ou=Almada,o=IBM,c=PO

cn=Rui Campos,ou=Sistemas de Voo,ou=Almada,o=IBM,c=PO
```

O comando:

```
ldapsearch –h hostname –o sn –b "o=ibm,c=po" "title=engenheiro"
```

devolve todas as entradas de um directório de empregados da IBM cujo título seja″engenheiro″, com os resultados ordenados por apelido.

O comando:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=po" "title=engenheiro"
```

devolve todas as entradas de um directório de empregados da IBM cujo título seja ″engenheiro″, com os resultados ordenados por apelido (por ordem descendente) e, em seguida, por nome comum (por ordem ascendente).

O comando:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=po "title=engenheiro"
```

devolve cinco entradas por página, com um intervalo de 3 segundos entre páginas, para todas as entradas do directório de empregados da IBM cujo título seja ″engenheiro″.

Este exemplo apresenta procuras em que está envolvido um objecto de consulta. Tal como foi explicado no “Consultas do directório de LDAP” na página 42, os directórios de LDAP do Directory Server podem conter objectos de referência, desde que apenas contenham:

- Um nome exclusivo (`dn`).
- Uma classe de objecto (`objectClass`).
- Um atributo de referência (`ref`).

Assuma que o ’Sistema_A’ contém a entrada de referência:

```
dn: cn=Bárbara Jorge, ou=Coimbra, o=Empresa Principal, c=PO
ref: ldap://Sistema_B:389/cn=Bárbara Jorge,
  ou=Coimbra, o=Empresa Principal, c=PO objectclass: referência
```

Todos os atributos associados à entrada deverão residir no ’Sistema_B’.

O Sistema_B contém uma entrada:

```
dn: cn=Bárbara Jorge, ou=Coimbra, o=Empresa Principal, c=PO
cn: Bárbara Jorge
objectclass: organizationalPerson
sn: Jorge
telephonenumber: (800) 555 1212
```

Quando um cliente emite um pedido para o ’Sistema_A’, o servidor de LDAP no Sistema_A responde ao cliente com o URL:

```
ldap://Sistema_B:389/cn=Bárbara Jorge,
  ou=Coimbra, o=Empresa Principal, c=PO
```

O cliente utiliza estas informações para emitir um pedido ao Sistema_B. Se a entrada no Sistema_A contiver atributos para além de`dn`, `objectclass` e `ref`, o servidor ignorará esses atributos (a menos que especifique o sinalizador **-R** para indicar que não deverão ser procuradas referências).

Quando um cliente receber uma resposta de referência de um servidor, enviará o pedido de novo, desta vez para o servidor ao qual se refere o URL devolvido. O novo pedido tem o mesmo âmbito que o pedido original. Os resultados desta procura variam dependendo do valor que especificar para o âmbito da procura (**-b**).

Se especificar `-s base`, como neste exemplo:

```
ldapsearch -h Sistema_A -b 'ou=Coimbra, o=Empresa principal, c=PO'
     -s base 'sn=Jorge'
```

a procura devolverá todos os atributos de todas as entradas com 'sn=Jorge' que residam em`'ou=Coimbra, o=Empresa Principal, c=PO'` tanto no Sistema_A, como no Sistema_B.

Se especificar `-s sub`, como neste exemplo:

```
ldapsearch -h Sistema_A -b 'ou=Coimbra, o=Empresa Principal, c=PO'
     -s sub 'sn=Jorge'
```

a procura devolverá todos os atributos de todas as entradas com 'sn=Jorge' que residam no ou abaixo de`'ou=Coimbra, o=Empresa Principal, c=PO'` tanto no Sistema_A, como no Sistema_B.

Se especificar `-s one`, como neste exemplo:

```
ldapsearch -h Sistema_A -b 'ou=Coimbra, o=Empresa principal, c=PO'
     -s one 'sn=Jorge'
```

a procura não devolve nenhuma entrada em nenhum sistema. Em vez disso, o servidor devolve ao cliente o URL de consulta:

```
ldap://Sistema_B:389/cn=Bárbara Jorge,
  ou=Coimbra, o=Empresa Principal, c=PO
```

Por sua vez, o cliente submete um pedido:

```
 ldapsearch -h Sistema_B -b 'ou=Coimbra, o=Empresa Principal, c=PO'
     -s one 'sn=Jorge'
```

Este pedido também não devolve resultados, uma vez que a entrada

```
dn: cn=Bárbara Jorge, ou=Coimbra, o=Empresa Principal, c=PO
```

reside em

```
  ou=Coimbra, o=Empresa Principal, c=PO
```

Uma procura com `-s one` tenta encontrar entradas no nível imediatamente abaixo

```
  ou=Coimbra, o=Empresa Principal, c=PO
```

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapchangepwd

A ferramenta de modificação de palavras-passe de LDAP.

Resumo

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel][-h ldaphost] [-K keyfile]
[-m mechanism] [-M]  [-N certificatename] [-O maxhops]
[-p ldapport] [-P keyfilepw]  [-R] [-v] [-V version]
[-Z] [-?]
```

Descrição

Envia pedidos de modificação de palavras-passe para um servidor de LDAP. Permite que a palavra-passe de uma entrada de directório seja alterada.

Opções

-C *charset*
Especifica que os DNs fornecidos como input ao utilitário **ldapdelete** estão representados num conjunto de caracteres local, tal como especificado por charset. Utilize a opção **-C** *charset*, se a página de códigos da cadeia de input for diferente do valor da página de códigos do trabalho. Consulte a API ldap_set_iconv_local_charset() para ver os valores charset suportados.

-d *debuglevel*
Defina o nível de depuração de LDAP como debuglevel.

-D *binddn*
Utilize ***binddn*** para ligar ao directório de LDAP.***binddn*** é um DN representado por cadeia.

-h *ldaphost*
Especifique um sistema central alternativo no qual o servidor de ldap esteja em execução.

-K *keyfile*
Especifique o nome do ficheiro da base de dados de chaves de SSL. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

Se o utilitário não conseguir localizar uma base de dados de chaves, usará um conjunto de código incorporado de raízes de autoridade de certificados fidedignas assumidas. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (ACs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas.

Este parâmetro activa efectivamente o comutador **-Z**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-m *mechanism*
Utilize ***mechanism*** para especificar o mecanismo SASL a ser utilizado para estabelecer uma associação com o servidor. Será utilizada a API ldap_sasl_bind_s(). O parâmetro **-m** será ignorado se estiver definido **-V 2**. Se **-m** não for especificado, é utilizada a autenticação simples.

-M Gerir objectos de referência como entradas normais.

-n *newpassword* | **?**
Especifica a nova palavra-passe. Utilize o ? para gerar um pedido de palavra-passe.

-N *certificatename*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. O parâmetro ***certificatename*** não será necessário se tiver sido designado um certificado assumido/par de chaves privado como o valor assumido. Do mesmo modo, o parâmetro ***certificatename*** não será necessário se existir um único par certificado/chave privada no ficheiro de conjunto de base de dados designado. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-O *maxhops*
Especifique ***maxhops*** para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar ao procurar referências. A contagem de sistemas de passagem assumida é 10.

-p *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado **-p** e estiver especificado **-Z**, será utilizada a porta de SSL de LDAP assumida 636.

-P *keyfilepw*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é obrigatória para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-P** não é necessário. Este parâmetro será ignorado se não for especificado **-Z** nem **-K**.

-R Especifica que as consultas não devem ser seguidas automaticamente.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

-V *version*
Especifica a versão de LDAP a ser utilizada por **ldapdchangepwd** quando for ligado ao servidor de LDAP. Por valor assumido, é estabelecida uma ligação de LDAP V3. Para seleccionar explicitamente o LDAP V3, especifique **-V 3**. Especifique **-V 2** para trabalhar com uma aplicação de LDAP V2. Uma aplicação, como **ldapdchangepwd**, selecciona LDAP V3 como o protocolo preferencial utilizando ldap_init em vez de ldap_open.

-w *passwd* **| ?**
Utilize ***passwd*** como a palavra-passe de autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-Z Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. Para o Directory Server no i5/OS, se utilizar -Z e não utilizar -K ou -N, será utilizado o certificado associado ao ID da aplicação do Cliente dos Serviços de Directório.

-? Apresenta a ajuda para a sintaxe de ldapchangepwd.

Exemplos

O comando seguinte,

```
ldapchangepwd -D cn=Joaquim Dias -w a1b2c3d4 -n wxyz9876
```

altera a palavra-passe da entrada com o commonName ″Joaquim Dias″ de a1b2c3d4 para wxyz9876

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

ldapdiff

A ferramenta de sincronização de réplicas de LDAP.

Nota: A execução deste comando pode ser demorada dependendo do número de entradas (e atributos para essas entradas) que são replicadas.

Resumo

(Compara e sincroniza entradas de dados entre dois servidores num ambiente de réplicas.)

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
 [-cD dn] [-cK keyStore] [-cw password] -[cN keyLabel]
 [-cp port] [-cP keyStorePwd]  [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
 [-sw password] -[sN keyLabel] [-sp port] [-sP keyStorePwd]
 [-sZ] [-v]
```

ou

(Compara o esquema entre dois servidores.)

```
 ldapdiff -S -sh host -ch host [-a] [-C countnumber][-cD dn]
 [-cK keyStore] [-cw password] -[cN keyLabel] [-cp port]
 [-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
 [-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
 [-sP keyStorePwd] [-sZ] [-v]
```

Descrição

Esta ferramenta sincroniza um servidor de réplica com o respectivo servidor principal. Se quiser consultar a ajuda para a sintaxe de **ldapdiff**, escreva:

```
ldapdiff -?
```

Opções

As opções que se seguem aplicam-se ao comando **ldapdiff**. Existe dois sub-agrupamentos que se aplicam especificamente ao servidor fornecedor ou ao servidor consumidor.

-a Especifica a utilização do controlo de administração do servidor para operações de escritas numa réplica só de leitura.

-b *baseDN*
Utilize searchbase como ponto de partida para a procura, em vez do valor assumido. Se não for especificado **-b**, este utilitário procura, na variável de ambiente LDAP_BASEDN, uma definição de searchbase.

-C *countnumber*
Conta o número de entradas a corrigir. Se forem encontradas mais discordâncias do que o número especificado, significa que a ferramenta existe.

-F Esta é a opção de correcção. Se especificado, o conteúdo da réplica do consumidor é modificado de modo a corresponder ao conteúdo do servidor fornecedor. Não poderá ser utilizado se **-S** também for especificado.

-L Se a opção **-F** não for especificada, utilize esta opção para gerar um ficheiro de LDIF para output. O ficheiro de LDIF pode ser utilizado para actualizar o consumidor para eliminar as diferenças.

-S Especifica a comparação do esquema em ambos os servidores.

-v Utilize o modo verboso, com muitos diagnósticos escritos no output padrão.

Opções para um fornecedor de replicação

As opções que se seguem aplicam-se ao servidor consumidor e estão identificadas por um 's' inicial no nome da opção.

-sD *dn* Utilize ***dn*** para ligar ao directório de LDAP. ***dn*** é um DN representado por cadeia.

~-sh *host*
Especifica o nome do sistema central.

-sK *keyStore*
Especifique o nome do ficheiro de base de dados de chaves de SSL com a extensão assumida **kdb**. Se este parâmetro não for especificado, ou se o valor for uma cadeia vazia (-sK""), será

utilizado o armazenamento de chaves do sistema. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

-sN *keyLabel*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se for especificada uma etiqueta sem ser especificado um armazenamento de chaves, a etiqueta é um identificador de aplicação no Gestor de Certificados Digitais (DCM - Digital Certificate Manager). A etiqueta assumida (id da aplicação) é QIBM_GLD_DIRSRV_CLIENT. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, será necessário um certificado de cliente. ***keyLabel*** não será necessário se tiver sido designado um par certificado/chave privada assumido. De modo semelhante, ***keyLabel*** não é necessário se existir um único par certificado/chave privada no ficheiro de base de dados de chaves designado. Este parâmetro será ignorado se não for especificado **-sZ** nem **-sK**.

-sp *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não for especificado **-sp** e for especificado **-sZ**, será utilizada a porta de SSL de LDAP assumida 636.

-sP *keyStorePwd*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é obrigatória para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-sP** não é necessário. Este parâmetro será ignorado se não for especificado **-sZ** nem **-sK**. A palavra-passe não será utilizada se existir um ficheiro de ocultação da palavra-passe para o armazenamento de chaves que está a ser utilizado.

-st *trustStoreType*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados fidedigno. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, poderá ser necessário um certificado de cliente. ***trustStoreType*** não é necessário se tiver sido designado um par certificado/chave privada como valor assumido. De modo semelhante, ***trustStoreType*** não é necessário se existir um único par certificado/chave privada no ficheiro de base de dados de chaves designado. Este parâmetro será ignorado se não for especificado **-sZ** nem **-sT**.

-sZ Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP.

Opções para um consumidor de replicação

As opções que se seguem aplicam-se ao servidor conmsumidor e estão identificadas por um 'c' inicial no respectivo nome. Por uma questão de conveniência, se for especificado -cZ sem serem especificados valores para -cK, -cN ou -cP, estas opções utilizarão o mesmo valor especificado para as opções de SSL do fornecedor. Para substituir as opções do fornecedor e utilizar a definição assumida, especifique -cK "" -cN "" -cP "".

-cD *dn* Utilize ***dn*** para ligar ao directório de LDAP. ***dn*** é um DN representado por cadeia.

-ch *host*
Especifica o nome do sistema central.

-cK *keyStore*
Especifique o nome do ficheiro de base de dados de chaves de SSL com a extensão assumida kdb. Se o valor for uma cadeia vazia (-sK""), será utilizado o armazenamento de chaves do sistema. Se o ficheiro da base de dados de chaves não se encontrar no directório actual, especifique o nome de ficheiro completo da base de dados de chaves.

-cN *keyLabel*
Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Se o servidor de LDAP estiver configurado para efectuar apenas a autenticação do servidor, não será necessário um certificado de cliente. Se for especificada uma etiqueta sem ser especificado um armazenamento de chaves, a etiqueta é um identificador de aplicação no Gestor de Certificados Digitais (DCM - Digital Certificate Manager). A etiqueta assumida (id da aplicação) é QIBM_GLD_DIRSRV_CLIENT. Se o servidor de LDAP estiver configurado para efectuar a autenticação do cliente e servidor, será necessário um certificado de cliente. ***keyLabel*** não será necessário se tiver sido designado um par certificado/chave privada assumido. De modo semelhante, ***keyLabel*** não é necessário se existir um único par certificado/chave privada no ficheiro de base de dados de chaves designado. Este parâmetro será ignorado se não for especificado **-cZ** nem **-cK**.

-cp *ldapport*
Especifique uma porta de TCP alternativa em que o servidor de ldap irá aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado **-cp** e estiver especificado **-cZ**, será utilizada a porta de SSL de LDAP assumida 636.

-cP *keyStorePwd*
Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é obrigatória para aceder às informações codificadas existentes no ficheiro de base de dados de chaves, o qual pode incluir uma ou mais chaves privadas. Se um ficheiro de ocultação da palavra-passe estiver associado ao ficheiro de base de dados de chaves, a palavra-passe será obtida a partir do ficheiro de ocultação da palavra-passe e o parâmetro **-cP** não é necessário. Este parâmetro será ignorado se não for especificado **-cZ** nem **-cK**.

-cw *password* | **?**
Utilize ***password*** como a palavra-passe para autenticação. Utilize o ? para gerar um pedido de palavra-passe.

-cZ Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP.

Exemplos

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> [opções]
```

ou

```
ldapdiff -S  -sh <supplierhostname> -ch <consumerhostname> [opções]
```

Diagnósticos

O estado de saída é 0 se não ocorrerem erros. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro padrão.

Notas sobre a utilização de SSL com os utilitários da linha de comandos de LDAP

Para utilizar as funções do Secure Sockets Layer (SSL) dos utilitários da linha de comandos, tem de ter instalado um dos produtos do Cryptographic Access Provider (5722-ACx).

O “Secure Sockets Layer (SSL) e Transport Layer Security com o Directory Server” na página 44 explica a utilização de SSL com o servidor de LDAP do Directory Server. Estas informações incluem a gestão e a criação de Autoridades de Certificação fidedignas com o Gestor de Certificados Digitais.

Alguns dos servidores de LDAP acedidos pelo cliente utilizam apenas a autenticação do servidor. Para estes servidores, só tem de definir um ou mais certificados de raiz fidedigna no arquivo de certificados. Com a autenticação do servidor, o cliente pode ter a certeza de que foi emitido um certificado ao servidor de LDAP destino através de uma das Autoridades de Certificação fidedignas (ACs). Para além disso, todas as transacções de LDAP estabelecidas através da ligação de SSL com o servidor são codificadas. Isto

inclui as credenciais de LDAP fornecidas nas interfaces de programação de aplicação (APIs) utilizadas para estabelecer associações ao Directory Server.Por exemplo, se o servidor de LDAP estiver a utilizar um certificado Verisign de alta segurança, deverá efectuar o seguinte procedimento:

1. Peça um certificado da AC ao Verisign.
2. Utilize o DCM para o importar para o seu arquivo de certificados.
3. Utilize o DCM para o marcar como fidedigno.

Se o servidor de LDAP estiver a utilizar um certificado de servidor emitido em privado, o administrador do servidor pode fornecer-lhe uma cópia do ficheiro de pedido de certificado do servidor. Importe o ficheiro de pedido de certificado para o arquivo de certificados e marque-o como fidedigno.

Se usar os utilitários da interface para aceder a servidores de LDAP que utilizem a autenticação do cliente e a autenticação do servidor, terá de efectuar o seguinte procedimento:

- Defina um ou mais certificados de raiz fidedigna no arquivo de certificados do sistema. Isto permite que o cliente tenha a certeza de que foi emitido um certificado ao servidor de LDAP destino através de uma das ACs fidedignas. Para além disso, todas as transacções de LDAP estabelecidas através da ligação de SSL com o servidor são codificadas. Isto inclui as credenciais de LDAP fornecidas nas interfaces de programação de aplicação (APIs) utilizadas para estabelecer associações ao Directory Server.
- Crie um par de chaves e peça um certificado de cliente a uma AC. Depois de receber o certificado assinado de uma AC, receba o certificado no ficheiro do conjunto de chaves mistas do cliente.

Formato de permuta de dados de LDAP (LDIF)

Esta documentação descreve o Formato de Permuta de Dados de LDAP (LDIF) tal como usado pelos utilitários ldapmodify, ldapsearch e ldapadd. O LDIF aqui especificado também é suportado pelos utilitários do servidor fornecidos com o DirectórioIBM.

O LDIF é utilizado para representar entradas de LDAP em formato de texto. O formato base de uma entrada de LDIF é:

```
dn: <nome exclusivo>
<attrtype> : <attrvalue>
<attrtype> : <attrvalue>
...
```

Uma linha pode ser continuada se iniciar a linha seguinte for iniciada com um espaço em branco ou tabulação como, por exemplo:

```
dn: cn=Joaquim E Dias, o=Universidade de Estudos       Superiores, c=PO
```

Os valores de atributo múltiplos são especificados em linhas separadas como, por exemplo:

```
cn: Joaquim E Dias
cn: Joaquim Dias
```

Se um <*attrvalue*> contiver um carácter não ASCII dos EUA, ou começar por um espaço ou dois pontos (:), o <*attrtype*> será seguido de dois sinais de dois pontos e o valor será codificado na notação base-64. Por exemplo, o valor ″ começa por um espaço″ seria codificado do seguinte modo:

```
cn:: IGJlZ2luciaB3aXRoIGEgc3BhY2U=
```

Múltiplas entradas no mesmo ficheiro de LDIF são separadas por uma linha em branco. Múltiplas linhas em branco são consideradas como um fim de ficheiro lógico.

Para obter mais informações, consulte:

- “Exemplo de LDIF” na página 203
- “Suporte de LDIF Versão 1” na página 203
- “Exemplos de LDIF Versão 1” na página 204

Exemplo de LDIF

Segue-se um exemplo de um ficheiro de LDIF com três entradas.

```
dn: cn=Joaquim E Dias, o=Universidade de Estudos
 Superiores, c=PO
cn: Joaquim E Dias
cn: Joaquim Dias
objectclass: person
sn: Dias

dn: cn=Bruno L Dias, o=Universidade de Estudos
 Superiores, c=PO
cn: Bruno L Dias
cn: Bruno Dias
objectclass: person
sn: Dias

dn: cn=Joaquina K. Dias, o=Universidade de Estudos
 Superiores, c=PO
cn: Joaquina K. Dias
cn: Joaquina Dias
objectclass: person
sn: Dias
jpegPhoto:: /9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD
 A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQ
 ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

O jpegPhoto na entrada de Joaquina Jorge tem a codificação base-64. Os valores de atributo textuais também podem ser especificados no formato base-64. No entanto, se for este o caso, a codificação base-64 tem de estar na página de códigos do formato comum do protocolo (ou seja, para LDAP V2, o conjunto de caracteres IA5 e, para LDAP V3, a codificação UTF-8).

Suporte de LDIF Versão 1

Os utilitários de cliente (ldapmodify e ldapadd) foram melhorados de modo a reconhecerem a versão de LDIF mais recente, que é identificada pela presença do controlo ″versão: 1″ no título do ficheiro. Ao contrário da versão de LDIF original, a versão mais recente de LDIF suporta valores de atributo representados em UTF-8 (em vez do mais limitado US-ASCII).

No entanto, a criação manual de um ficheiro de LDIF contendo valores de UTF-8 pode ser difícil. Para simplificar este processo, é suportada uma extensão charset para o formato LDIF. Esta extensão permite que seja especificado um nome de conjunto de caracteres IANA no cabeçalho do ficheiro de LDIF (juntamente com o número da versão.É suportado um grupo limitado de conjuntos de caracteres IANA.

O formato de LDIF versão 1 também suporta URLs de ficheiro. Este fornece uma forma mais flexível de definir uma especificação de ficheiro. Os URLs de ficheiro assumem o seguinte formato:

```
atributo:< ficheiro:///caminho          (em que a sintaxe de caminho depende da plataforma)
```

Por exemplo, seguem-se endereços da Web válidos de ficheiros:

```
jpegphoto:< ficheiro:///d:\temp\photos\minhafoto.jpg    (Caminhos de estilo DOS/Windows)
     jpegphoto:< ficheiro:///etc/temp/photos/minhafoto.jpg   (Caminhos de estilo Unix)
```

Nota: Os utilitários do IBM Directory suportam a nova especificação de URL de ficheiro, bem como o estilo mais antigo (″jpegphoto: /etc/temp/minhafoto″), seja qual for a especificação da versão. Por outras palavras, o novo formato de URL de ficheiro pode ser utilizado sem a adição do controlo de versão aos seus ficheiros de LDIF.

Exemplos de LDIF Versão 1

Pode utilizar o controlo charset opcional para que os utilitários sejam convertidos automaticamente do conjunto de caracteres especificado para UTF-8, tal como no seguinte exemplo:

```
versão: 1
 charset: ISO-8859-1

 dn: cn=João Grego, o=Universidade de Faro, c=PO
 cn: João Grego
 sn: Grego
 description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvd
 title: Director Associado
 title: [Vice-director]
 jpegPhoto:> ficheiro:///usr/local/photos/jgrego.jpg
```

Nesta ocorrência, todos os valores a seguir a um nome de atributo e a um único sinal de dois pontos são convertidos do conjunto de caracteres ISO-8859-1 para UTF-8. Os valores a seguir a um atributo e a dois sinais de dois pontos (tais como a descrição:: V2hhdCBhIGNhcm...) têm de ter a codificação base-64 e espera-se que sejam cadeias de caracteres binárias ou UTF-8. Também se espera que os valores lidos de um ficheiro, como o atributo jpegPhoto especificado pelo endereço da Web do exemplo anterior sejam binários ou UTF-8. Não efectuada qualquer conversão do ″charset″ especificado para UTF-8 nesses valores.

Neste exemplo de um ficheiro de LDIF sem o controlo charset, espera-se que o conteúdo esteja em dados UTF-8, em dados UTF-8 codificados com base-64 ou em dados binários codificados com base-64:

```
# Ficheiro de LDIF ExemploDirectório da IBM
 #
 # O sufixo "o=IBM, c=PO" deverá ser definido antes de qualquer tentativa de
 # carregamento destes dados.

versão: 1

 dn: o=IBM, c=PO
objectclass: superior
objectclass: organização
 o: IBM

 dn: ou=Almada, o=IBM, c=PO
 ou: Almada
 objectclass: organizationalUnit
 seealso: cn=Grupo Carlesberg, ou=Almada, o=IBM, c=PO
```

Este mesmo ficheiro poderia ser utilizado sem a informação do cabeçalho versão: 1, tal como na edição anterior do Directório IBM:

```
 # Ficheiro de LDIF ExemploDirectório da IBM
 #
 # O sufixo "o=IBM, c=PO" deverá ser definido antes de qualquer tentativa de
 # carregamento destes dados.

 dn: o=IBM, c=PO
objectclass: superior
objectclass: organização
 o: IBM

 dn: ou=Almada, o=IBM, c=PO
 ou: Almada
 objectclass: organizationalUnit
 seealso: cn=Grupo Carlesberg, ou=Almada, o=IBM, c=PO
```

Nota: Os valores de atributo textuais podem ser especificados no formato base-64.

Esquema de configuração do Directory Server

Estas informações descrevem a Árvore de Informações de Directórios(DIT) e os atributos utilizados para configurar o ficheiro ibmslapd.conf. Nas edições anteriores, as definições da configuração do directório eram armazenadas num formato exclusivo no ficheiro de configuração. As definições do directório são agora armazenadas com a utilização do formato LDIF no ficheiro de configuração.

O ficheiro de configuração chama-se ibmslapd.conf. O esquema utilizado pelo ficheiro de configuração também está actualmente disponível. Podem ser encontrados tipos de atributo no ficheiro v3.config.at, enquanto que as classes de objecto se encontram no ficheiro v3.config.oc. Os atributos podem ser modificados com a utilização do comando ldapmodify. Para obter mais informações sobre o comando ldapmodify, consulte "ldapmodify e ldapadd" na página 175.

- "Árvore de informações de directório"
- "Atributos" na página 214

Árvore de informações de directório

cn=Configuração

- cn=Admin
- cn=Notificação de Acontecimentos
- cn=Computador Principal
- cn=Kerberos
- cn=Servidor Principal
- cn=Reenvio
- cn=Esquema
  - cn=IBM Directory
    - cn=Programas Emissores de Config
      - cn=ConfigDB
    - cn=Programas Emissores de RDBM
      - cn=Directório
      - cn=RegistoAlterações
    - cn=Programas Emissores de LDCF
      - cn=BDEsquema
- cn=SSL
  - cn=CRL
- cn=Transacção

cn=Configuração

DN cn=Configuração

Descrição
Esta é a entrada de nível superior na DIT de configuração. Contém dados de interesse geral para o servidor, embora, na prática, também contenha itens diversos. Todos os atributos desta entrada provêm da primeira secção (sub-rotina global) de ibmslapd.conf.

Número
1 (obrigatório)

Classe de Objecto
ibm-slapdTop

Atributos Obrigatórios

- cn

- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Atributos Opcionais

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuração

Descrição
Definições da configuração global para o IBM Admin Daemon

Número
1 (obrigatório)

Classe de Objecto
ibm-slapdAdmin

Atributos Obrigatórios

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Atributos Opcionais

- ibm-slapdSecurePort

cn=Notificação de Acontecimentos

DN cn=Notificação de Acontecimentos, cn=Configuração

Descrição
Definições globais de notificação de acontecimentos para o Directory Server

Número
0 ou 1 (opcional; só é necessário se pretender activar a notificação de acontecimentos)

Classe de Objecto
ibm-slapdEventNotification

Atributos Obrigatórios

- cn
- ibm-slapdEnableEventNotification

- objectClass

Atributos Opcionais

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Computador Principal

DN cn=Computador Principal, cn=Configuração

Descrição
Definições globais de ambiente que o servidor aplica no arranque.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdFrontEnd

Atributos Obrigatórios

- cn
- objectClass

Atributos Opcionais

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuração

Descrição
Definições globais da autenticação de Kerberos para o Directory Server.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdKerberos

Atributos Obrigatórios

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Atributos Opcionais

- Nenhum

cn=Servidor Principal

DN cn=Servidor Principal, cn=Configuração

Descrição
Ao configurar uma réplica, esta entrada contém as credenciais de ligação e o URL de referência do servidor principal.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdReplication

Atributos Obrigatórios

- cn
- ibm-slapdMasterPW (Obrigatório se não estiver a ser utiliza da a autenticação de Kerberos.)

Atributos Opcionais

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Opcional se estiver a ser utilizada a autenticação de Kerberos.)
- ibm-slapdMasterReferral
- objectClass

cn=Reenvio

DN cn=Reenvio, cn=Configuração

Descrição
Esta entrada contém todas as entradas de referência a partir da primeira secção (sub-rotina global) de ibmslapd.conf. Se não existirem referências (não existe nenhum por valor assumido), esta entrada é opcional.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdReferral

Atributos Obrigatórios

- cn
- ibm-slapdReferral
- objectClass

Atributos Opcionais

- Nenhum

cn=Esquemas

DN cn=Esquemas, cn=Configuração

Descrição
Esta entrada serve de contentor para os esquemas. Esta entrada não é realmente necessária porque os esquemas podem ser distinguidos pela classe de objecto ibm-slapdSchema. É incluída para melhorar a capacidade de leitura da DIT.

Só é permitida actualmente uma entrada de esquema: cn=IBM Directory.

Número
1 (obrigatório)

Classe de Objecto
Container

Atributos Obrigatórios

- cn
- objectClass

Atributos Opcionais

- Nenhum

cn=IBM Directory

DN cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Esta entrada contém todos os dados de configuração do esquema a partir da primeira secção (sub-rotina global) de ibmslapd.conf. Também serve de contentor para todos os computadores secundários que utilizem o esquema. Actualmente, não são suportados múltiplos esquemas, mas, se fossem, existiria uma entrada ibm-slapdSchema por esquema. Note que múltiplos esquemas são considerados como incompatíveis. Deste modo, um computador secundário só pode ser associado a um único esquema.

Número
1 (obrigatório)

Classe de Objecto
ibm-slapdSchema

Atributos Obrigatórios

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Atributos Opcionais

- ibm-slapdSchemaAdditions

cn=Programas Emissores de Config

DN cn=Prog. Emissores de Config, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Esta entrada serve de contentor para os Programas Emissores de Configuração.

Número
1 (obrigatório)

Classe de Objecto
Container

Atributos Obrigatórios

- cn
- objectClass

Atributos Opcionais
Nenhum

cn=ConfigDB

DN cn=ConfigBD, cn=Prog. Emissores de Config, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Computador secundário de configuração para configuração do IBM Directory Server.

Número
0 - n (opcional)

Classe de Objecto
ibm-slapdConfigBackend

Atributos Obrigatórios
- ibm-slapdSuffix
- ibm-slapdPlugin

Atributos Opcionais
- ibm-slapdReadOnly

cn=Programas Emissores de RDBM

DN cn=Prog. Emissores de RDBM, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Esta entrada serve de contentor para os programas emissores de RDBM. Com efeito, substitui a linha rdbm da base de dados de ibmslapd.conf identificando todas as sub-entradas como programas emissores da DB2. Esta entrada não é realmente necessária porque os programas emissores de RDBM podem ser distinguidos pela classe de objecto ibm-slapdRdbmBackend. É incluída para melhorar a capacidade de leitura da DIT.

Número
0 ou 1 (opcional)

Classe de Objecto
Container

Atributos Obrigatórios
- cn
- objectClass

Atributos Opcionais
- Nenhum

cn=Directório

DN cn=Directório, cn=Programas Emissores de RDBM, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Esta entrada contém todas as definições de configuração da base de dados para o sistema origem da base de dados de RDBM assumido.

Embora possam ser criados vários programas emissores com nomes arbitrários, a Administração do Servidor assume que ″cn=Directório″ é o sistema origem de directórios principal e que ″cn=Registo de Alterações é o sistema origem de changelog opcional. Só os sufixos apresentados em ″cn=Directório″ são configuráveis através da Administração do Servidor (excepto o sufixo changelog, que é definido de forma transparente por meio da activação de changelog).

Número
0 - n (opcional)

Classe de Objecto
ibm-slapdRdbmBackend

Atributos Obrigatórios

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atributos Opcionais

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Nota: Se estiver a utilizar **ibm-slapdUseProcessIdPw**, terá de modificar o esquema de modo a tornar **ibm-slapdDbUserPW** opcional.

cn=Registo de Alterações

DN cn=Registo de Alterações, cn=Programas Emissores de RDBM, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição
Esta entrada contém todas as definições de configuração da base de dados para o sistema origem do registo de alterações.

Número
0 - n (opcional)

Classe de Objecto
ibm-slapdRdbmBackend

Atributos Obrigatórios

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atributos Opcionais

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Nota: Se estiver a utilizar **ibm-slapdUseProcessIdPw**, terá de modificar o esquema de modo a tornar **ibm-slapdDbUserPW** opcional.

cn=Programas Emissores de LDCF

DN cn=Programas Emissores de LDCF, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição

Esta entrada serve de contentor para os programas emissores de LDCF. Com efeito, substitui a linha ldcf da base de dados de ibmslapd.conf identificando todas as sub-entradas como programas emissores de LDCF. Esta entrada não é realmente necessária porque os programas emissores de LDCF podem ser distinguidos pela classe de objecto ibm-slapdLdcfBackend. É incluída para melhorar a capacidade de leitura da DIT.

Número

1 (obrigatório)

Classe de Objecto

Container

Atributos Obrigatórios

- cn
- objectClass

Atributos Opcionais

- ibm-slapdPlugin

cn=EsquemaBD

DN cn=EsquemaBD, cn=Programas Emissores de LDCF, cn=IBM Directory, cn=Esquemas, cn=Configuração

Descrição

Esta entrada contém todos os dados de configuração da base de dados desde a secção de base de dados de ldcf de ibmslapd.conf.

Número
1 (obrigatório)

Classe de Objecto
ibm-slapdLdcfBackend

Atributos Obrigatórios

- cn
- objectClass

Atributos Opcionais

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuração

Descrição
Definições globais da ligação de SSL para o Directory Server.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdSSL

Atributos Obrigatórios

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Atributos Opcionais

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Nota: **ibm-slapdSslCipherSpecs** é pedido agora. Utilize **ibm-slapdSslCipherSpec** como alternativa. Se utilizar **ibm-slapdSslCipherSpecs**, o servidor será convertido para o atributo suportado.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuração

Descrição
Esta entrada contém dados da lista de revogação de certificados a partir da primeira secção (sub-rotina global) de ibmslapd.conf. Só é necessária se ″ibm-slapdSslAuth = serverclientauth″ na entrada cn=SSL e os certificados do cliente tiverem sido emitidos para validação de CRL.

Número
0 ou 1 (opcional)

Classe de Objecto
ibm-slapdCRL

Atributos Obrigatórios

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Atributos Opcionais

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transacção

DN cn = Transacção, cn = Configuração

Descrição

Especifica Definições globais do suporte de transacções. O suporte de transacções é fornecido com a utilização do suplemento:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

O servidor (**slapd**) carrega automaticamente este plugin no arranque se **ibm-slapdTransactionEnable = TRUE**. O plugin não necessita de ser explicitamente adicionado a **ibmslapd.conf**.

Número

0 ou 1 (opcional; só é necessário se pretender utilizar transacções)

Classe de Objecto

ibm-slapdTransaction

Atributos Obrigatórios

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Atributos Opcionais

- Nenhum

Atributos

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW

- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck

- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- objectClass

cn

Descrição
Este é o atributo Nome comum de X.500, que contém o nome de um objecto.

Sintaxe
Cadeia de directórios

Comprimento Máximo
256

Valor Vários valores

ibm-slapdACIMechanism

Descrição
Determina qual o modelo de ACL utilizado pelo servidor. (Suportado apenas no i5/OS a partir da versão v3.2, ignorado nas outras plataformas.)
- Modelo de ACL 1.3.18.0.2.26.1 = IBM SecureWay® v3.1
- Modelo de ACL 1.3.18.0.2.26.2 = IBM SecureWay v3.2

Valor Assumido
Modelo de ACL 1.3.18.0.2.26.2 = IBM SecureWay v3.2

Sintaxe
Cadeia de directórios

Comprimento Máximo
256

Valor Com vários valores.

ibm-slapdACLAccess

Descrição
Controla se o acesso às ACLs é activado. Se definido como TRUE, o acesso a ACLs está activado. Se definido como FALSE, o acesso a ACLs está desactivado.

Valor Assumido
TRUE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdACLCache

Descrição
Controla se o servidor guarda informações de ACLs na memória cache.

- Se definido como TRUE, o servidor guarda informações de ACLs na memória cache.
- Se definido como FALSE, o servidor não guarda informações de ACLs na memória cache.

Valor Assumido
TRUE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdACLCacheSize

Descrição
Número máximo de entradas a manter na Memória Cache de ACLs.

Valor Assumido
25000

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdAdminDN

Descrição
O DN de ligação do administrador para o Directory Server.

Valor Assumido
cn=raiz

Sintaxe
DN

Comprimento Máximo
Ilimitado

Valor Valor único

ibm-slapdAdminPW

Descrição
A Palavra-passe de ligação do administrador para o Directory Server.

Valor Assumido
secreta

Sintaxe
Binária

Comprimento Máximo
128

Valor Valor único

ibm-slapdBulkloadErrors

Descrição
Caminho de ficheiro ou dispositivo na máquina sistema central de ibmslapd para o qual serão enviadas mensagens de erro de sobrecarga.

Valor Assumido
/var/bulkload.log

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdChangeLogMaxEntries

Descrição
Este atributo é utilizado por um plug-in de changelog para especificar o número máximo de entradas de changelog permitidas na base de dados de RDBM. Cada changelog tem o seu próprio atributo changeLogMaxEntries.

```
Mínimo = 0 (ilimitado)
Máximo = 2,147,483,647 (número inteiro assinado de 32 bits)
```

Valor Assumido
0

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdCLIErrors

Descrição
Caminho de ficheiro ou dispositivo na máquina sistema central de ibmslapd para o qual serão enviadas mensagens de erro de CLI.

Valor Assumido
/var/db2cli.log

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdConcurrentRW

Descrição
Definir este valor como TRUE permite que as procuras continuem simultaneamente com actualizações. Permite a existência de 'leituras imprecisas', ou seja, resultados que podem não ser consistentes com o estado consolidado da base de dados.

Aviso: Este atributo é pedido.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdDB2CP

Descrição
Especifica a página de códigos da base de dados de directórios. 1208 é a página de códigos para bases de dados UTF-8.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
11

Valor Valor único

ibm-slapdDBAlias

Descrição
O nome alternativo da base de dados DB2.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
8

Valor Valor único

ibm-slapdDbConnections

Descrição
Especifique o número de ligações à DB2 que o servidor irá dedicar ao sistema origem da DB2. O valor tem de estar entre 5 & 50 (inclusive).

Nota: A variável de ambiente ODBCCONS substitui o valor desta directiva.
Se ibm-slapdDbConnections (ou ODBCCONS) for menor que 5 ou maior que 50, o servidor utilizará 5 ou 50 respectivamente. Será criada 1 ligação adicional para replicação (mesmo que não esteja definida replicação). Serão criadas 2 ligações adicionais para o registo de alterações (se o registo de alterações estiver activado).

Valor Assumido
15

Sintaxe
Número Inteiro

Comprimento Máximo
50

Valor Valor único

ibm-slapdDbInstance

Descrição
Especifica a ocorrência da base de dados DB2 para este sistema origem.

Valor Assumido
ldapdb2

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
8

Valor Valor único

Nota: Todos os objectos ibm-slapdRdbmBackend têm de utilizar o mesmo conjunto de caracteres de ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW e da DB2.

ibm-slapdDbLocation

Descrição
O caminho do sistema de ficheiros onde se encontra a base de dados do sistema origem.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdDbName

Descrição
Especifica o nome da base de dados DB2 para este sistema origem.

Valor Assumido
ldapdb2

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
8

Valor Valor único

ibm-slapdDbUserID

Descrição
Especifica o nome de utilizador usado para estabelecer ligação com a base de dados DB2 para este sistema origem.

Valor Assumido
ldapdb2

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
8

Valor Valor único

Nota: Todos os objectos ibm-slapdRdbmBackend têm de utilizar o mesmo conjunto de caracteres de ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW e DB2.

ibm-slapdDbUserPW

Descrição
Especifica a palavra-passe de utilizador usada para estabelecer ligação com a base de dados DB2 para este sistema origem. A palavra-passe pode ser escrita em texto normal ou codificada por imask.

Valor Assumido
ldapdb2

Sintaxe
Binária

Comprimento Máximo
128

Valor Valor único

Nota: Todos os objectos ibm-slapdRdbmBackend têm de utilizar o mesmo conjunto de caracteres de ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW e da DB2.

ibm-slapdEnableEventNotification

Descrição
Especifica se a Notificação de Acontecimentos deve ou não ser activada. Tem de ser definido como TRUE ou FALSE.

Se for definido como FALSE, to servidor rejeitará todos os pedidos de cliente relativos ao registo de notificações de acontecimentos com o resultado expandido LDAP_UNWILLING_TO_PERFORM.

Valor Assumido
TRUE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdEntryCacheSize

Descrição
Número máximo de entradas a manter na memória cache de entradas.

Valor Assumido
25000

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdErrorLog

Descrição
Especifica o caminho de ficheiro ou dispositivo na máquina do Directory Server para o qual são enviadas mensagens de erro.

Valor Assumido
/var/ibmslapd.log

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdFilterCacheBypassLimit

Descrição
Os filtros de procura correspondentes a mais do que este número de entradas não serão adicionados à memória cache de Filtros de Procura. Uma vez que a lista de IDs de entrada correspondentes ao filtro é incluída nesta memória cache, esta definição ajuda a limitar a utilização da memória. Um valor igual 0 indica que não existe limite.

Valor Assumido
100

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdFilterCacheSize

Descrição
Especifica o número máximo de entradas a manter na Memória Cache de Filtros de Procura.

Valor Assumido
25000

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdIdleTimeOut

Descrição
Tempo máximo durante o qual uma ligação de LDAP deverá ser mantida aberta quando não existe actividade na ligação. O tempo de inactividade para uma ligação de LDAP é o

tempo (em segundos) decorrido entre a última actividade na ligação e a hora actual. Se a ligação tiver expirado, com base no facto de o tempo de inactividade ser superior ao valor deste atributo, o servidor de LDAP limpará e terminará a ligação de LDAP, tornando-a disponível para outros pedidos de entrada.

Valor Assumido
300

Sintaxe
Número Inteiro

Comprimento
11

Contagem
Simples

Utilização
Funcionamento do directório

Modificação pelo Utilizador
Sim

Classe de Acesso
Crítica

Obrigatório
Não

ibm-slapdIncludeSchema

Descrição
Especifica um caminho de ficheiro na máquina do Directory Server que contém definições de esquema.

Valor Assumido
/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Vários valores

ibm-slapdKrbAdminDN

Descrição
Especifica o ID de Kerberos do administrador de LDAP (por exemplo, ibm-kn=admin1@realm1). Utilizado quando a autenticação de Kerberos é utilizada para

autenticar o administrador quando tiver iniciado sessão na interface da Administração do Servidor. Pode ser especificado em vez de, ou em adição a adminDN e adminPW.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
128

Valor Valor único

ibm-slapdKrbEnable

Descrição
Especifica se o servidor suporta Kerberos. Tem de ser definido como TRUE ou FALSE.

Valor Assumido
TRUE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdKrbIdentityMap

Descrição
Especifica se deverá ser utilizada a definição de correspondências de identidade de Kerberos. Tem de ser definido como TRUE ou FALSE. Se for definido como TRUE, quando um cliente é autenticado com um ID de Kerberos, o servidor procura todos os utilizadores locais com credenciais de Kerberos correspondentes e adiciona-as às credenciais da ligação. Permite que as ACLs baseadas em DNs de utilizador de LDAP continuem a ser utilizáveis com Kerberos.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdKrbKeyTab

Descrição
Especifica o ficheiro de separadores de chaves de Kerberos do servidor de LDAP. Este ficheiro contém a chave privada do servidor de LDAP, que está associada à respectiva conta de Kerberos. Este ficheiro deverá ser protegido (tal como o ficheiro de base de dados de chaves de SSL do servidor).

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdKrbRealm

Descrição
Especifica o domínio de Kerberos do servidor de LDAP. É utilizado para publicar o atributo ldapservicename no DSE raiz. Note que um servidor de LDAP pode funcionar como repositório de informações sobre contas de vários KDCs (e domínios), mas o servidor de LDAP, enquanto servidor "kerberizado", só pode ser membro de um domínio.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
256

Valor Valor único

ibm-slapdLdapCrlHost

Descrição
Especifica o nome de sistema central do servidor de LDAP que contém as Listas de Revogação de Certificados (CRLs) para validação de certificados x.509v3 de cliente. Este parâmetro é necessário quando tiverem sido emitidos ibm-slapdSslAuth=serverclientauth e os certificados de cliente para validação de CRLs.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
256

Valor Valor único

ibm-slapdLdapCrlPassword

Descrição
Especifica a palavra-passe que o SSL do lado do servidor utiliza para ligar ao servidor de LDAP que contém as Listas de Revogação de Certificados (CRLs) para validação de certificados x.509v3 de cliente. Este parâmetro pode ser necessário quando tiverem sido emitidos ibm-slapdSslAuth=serverclientauth e os certificados de cliente para validação de CRLs.

Nota: Se o servidor de LDAP que contém as CRLs permitir o acesso não autenticado às CRLs (ou seja, acesso anónimo), ibm-slapdLdapCrlPassword não é necessário.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Binária

Comprimento Máximo
128

Valor Valor único

ibm-slapdLdapCrlPort

Descrição
Especifica a porta utilizada para ligar ao servidor de LDAP que contém as Listas de Revogação de Certificados (CRLs) para validação de certificados x.509v3 de cliente. Este parâmetro é necessário quando tiverem sido emitidos ibm-slapdSslAuth=serverclientauth e os certificados de cliente para validação de CRLs. (As portas de IP não são assinadas, os números inteiros de 16 bits estão no intervalo de 1 a 65535.)

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdLdapCrlUser

Descrição
Especifica o bindDN que o SSL do lado do servidor utiliza para ligar ao servidor de LDAP que contém as Listas de Revogação de Certificados (CRLs) para validação de certificados x.509v3 de cliente. Este parâmetro pode ser necessário quando tiverem sido emitidos ibm-slapdSslAuth=serverclientauth e os certificados de cliente para validação de CRLs.

Nota: Se o servidor de LDAP que contém as CRLs permitir o acesso não autenticado às CRLs (ou seja, acesso anónimo), ibm-slapdLdapCrlUser não é necessário.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
DN

Comprimento Máximo
1000

Valor Valor único

ibm-slapdMasterDN

Descrição
Especifica o DN de ligação do servidor principal. O valor tem de corresponder ao replicaBindDN no replicaObject definido para o servidor principal. Quando o Kerberos é utilizado para autenticação na réplica, ibm-slapdMasterDN tem de especificar a representação do DN do ID do Kerberos (por exemplo, ibm-kn=freddy@domínio1). Quando o Kerberos é utilizado, MasterServerPW é ignorado.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
DN

Comprimento Máximo
1000

Valor Valor único

ibm-slapdMasterPW

Descrição
Especifica a palavra-passe de ligação de um servidor de réplica principal. O valor tem de corresponder a replicaBindDN no replicaObject definido para o servidor principal. Quando o Kerberos é utilizado para autenticação na réplica, ibm-slapdMasterDN tem de especificar a representação do DN do ID do Kerberos (por exemplo, ibm-kn=freddy@domínio1). Quando o Kerberos é utilizado, MasterServerPW é ignorado.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Binária

Comprimento Máximo
128

Valor Valor único

ibm-slapdMasterReferral

Descrição
Especifica o URL do servidor de réplica principal. Por exemplo:

```
ldap://master.us.ibm.com
```

Quando a segurança está definida apenas como SSL:

```
ldaps://master.us.ibm.com:636
```

Quando a segurança está definida como nenhuma e ao utilizar uma porta não padrão:

```
ldap://master.us.ibm.com:1389
```

Valor Assumido
nenhum

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
256

Valor Valor único

ibm-slapdMaxEventsPerConnection

Descrição
Especifica o número máximo de notificações de acontecimentos que podem ser registadas por ligação.

```
Mínimo = 0 (ilimitado)
Máximo = 2.147.483.647
```

Valor Assumido
100

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdMaxEventsTotal

Descrição
Especifica o número máximo total de notificações de acontecimentos que podem ser registadas para todas as ligações.

```
Mínimo = 0 (ilimitado)
Máximo = 2.147.483.647
```

Valor Assumido
0

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdMaxNumOfTransactions

Descrição
Especifica o número máximo de transacções por servidor.

```
Mínimo = 0 (ilimitado)
Máximo = 2.147.483.647
```

Valor Assumido
20

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdMaxOpPerTransaction

Descrição
Especifica o número máximo de operações por transacção.

```
Mínimo = 0 (ilimitado)
Máximo = 2.147.483.647
```

Valor Assumido
5

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdMaxPendingChangesDisplayed

Descrição
Número máximo de alterações pendentes a apresentar.

Valor Assumido
200

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdMaxTimeLimitOfTransactions

Descrição
Especifica o valor de tempo de espera máximo de uma transacção pendente em segundos.

```
Mínimo = 0 (ilimitado)
Máximo = 2.147.483.647
```

Valor Assumido
300

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdPagedResAllowNonAdmin

Descrição
Especifica se o servidor deverá ou não permitir uma ligação sem ser pelo Administrador para pedidos de resultados por página num pedido de procura. Se o valor lido no ficheiro ibmslapd.conf for FALSE, o servidor processará apenas os pedidos de cliente submetidos por um utilizador com autoridade de Administrador. Se um cliente pedir resultados por página para uma operação de procura, não tiver autoridade de Administrador e o valor lido no ficheiro ibmslapd.conf para este atributo for FALSE, o servidor regressará ao cliente com o código de retorno insufficientAccessRights; não será executada qualquer procura ou paginação.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento
5

Contagem
Simples

Utilização
directoryOperation

Modificação pelo Utilizador
Sim

Classe de Acesso
crítica

Objectclass
ibm-slapdRdbmBackend

Obrigatório
Não

ibm-slapdPagedResLmt

Descrição
Número máximo de pedidos de procura com resultados por página pendentes permitidos activos simultaneamente. Intervalo = 0.... Se um cliente pedir uma operação de resultados por página e estiver activo o número máximo de resultados por página pendentes, o servidor regressará ao cliente com o código de retorno ocupado; não será executada qualquer procura ou paginação.

Valor Assumido
3

Sintaxe
Número Inteiro

Comprimento
11

Contagem
Simples

Utilização
directoryOperation

Modificação pelo Utilizador
Sim

Classe de Acesso
crítica

Obrigatório
Não

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Descrição
Número máximo de entradas a devolver pela procura de uma página individual quando for especificado o controlo de resultados por página, independentemente do tamanho de página que possa ter sido especificado no pedido de procura do cliente. Intervalo = 0.... Se um cliente tiver ultrapassado um tamanho de página, será utilizado o valor mais baixo dos valores do cliente e o valor lido em ibmslapd.conf.

Valor Assumido
50

Sintaxe
Número Inteiro

Comprimento
11

Contagem
Simples

Utilização
directoryOperation

Modificação pelo Utilizador
Sim

Classe de Acesso
crítica

Obrigatório
Não

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Descrição
Um plugin é uma biblioteca carregada dinamicamente que expande as capacidades do servidor. Um atributo ibm-slapdPlugin especifica ao servidor como carregar e inicializar uma biblioteca plug-in. A sintaxe é:

```
palavra-chave nome do ficheiro init_function [args...]
```

A sintaxe é ligeiramente diferente para cada plataforma devido a convenções de nomenclatura de bibliotecas.

A maioria dos plug-ins é opcional, mas o plug-in do sistema origem de RDBM é obrigatório para todos os programas emissores de RDBM.

Valor Assumido
base de dados /bin/libback-rdbm.dll rdbm_backend_init

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
2000

Valor Vários valores

ibm-slapdPort

Descrição
Especifica a porta de TCP/IP utilizada para ligações sem ser de SSL. Não pode ter o mesmo valor que ibm-slapdSecurePort. (As portas de IP não são assinadas, os números inteiros de 16 bits estão entre 1 - 65535.)

Valor Assumido
389

Sintaxe
Número Inteiro

Comprimento Máximo
5

Valor Valor único

ibm-slapdPWEncryption

Descrição
Especifica o mecanismo de codificação para as palavras-passe de utilizador antes de serem armazenadas no directório. Tem de ser especificado como nenhum, imask, crypt ou sha (tem de utilizar a palavra-chave **sha** para poder obter a codificação SHA-1). O valor tem de ser definido como nenhum para que a ligação SASL cram-md5 tenha êxito.

Valor Assumido
nenhum

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
5

Valor Valor único

ibm-slapdReadOnly

Descrição
Este atributo é, normalmente, aplicado apenas ao sistema origem do Directório.Especifica se é ou não possível escrever no sistema origem. Tem de ser especificado como TRUE ou FALSE. Assume o valor FALSE, se não for especificado. Se for definido como TRUE, o servidor devolverá LDAP_UNWILLING_TO_PERFORM (0x35) em resposta a qualquer pedido de cliente que alterar os dados da base de dados readOnly.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdReferral

Descrição
Especifica o URL de LDAP de referência a transferir de novo quando os sufixos locais não correspondem ao pedido. É utilizado para referência superior (ou seja, quando o sufixo não se encontra no contexto de nomenclatura do servidor).

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
32700

Valor Vários valores

ibm-slapdReplDbConns

Descrição
Número máximo de ligações à base de dados para utilização pela replicação.

Valor Assumido
4

Sintaxe
Número Inteiro

Comprimento Máximo
11

Valor Valor único

ibm-slapdReplicaSubtree

Descrição
Identifica o DN de uma sub-árvore replicada

Sintaxe
DN

Comprimento Máximo
1000

Valor Valor único

ibm-slapdSchemaAdditions

Descrição
O atributo ibm-slapdSchemaAdditions é utilizado para identificar explicitamente o ficheiro que contém novas entradas de esquema. Este é definido por valor assumido como/etc/V3.modifiedschema. Se este atributo não for definido, o servidor reverterá para a utilização do último ficheiro ibm-slapdIncludeSchema tal como nas edições anteriores.

Antes da Versão 3.2, a última entrada includeSchema de **slapd.conf** era o ficheiro ao qual eram adicionadas todas as novas entradas de esquema pelo servidor, caso 0 recebesse um pedido de adição de um cliente. Normalmente, o último includeSchema é o ficheiro V3.modifiedschema, que é um ficheiro vazio instalado apenas para esta finalidade.

Nota: O nome modificado é enganador, uma vez que só armazena novas entradas. As alterações a entradas de esquema existentes são efectuadas nos respectivos ficheiros originais.

Valor Assumido
/etc/V3.modifiedschema

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdSchemaCheck

Descrição
Especifica o mecanismo de verificação do esquema para a operação adicionar/modificar/eliminar. Tem de ser especificado como V2, V3 ou V3_lenient.

- V2 - Reter verificação da v2 e v2.1. Recomendado para fins de migração.
- V3 - Executar verificação da v3.
- V3_lenient - Nem todas as classes de objecto ascendentes são necessárias.Só é necessária a classe de objecto imediata ao adicionar entradas.

Valor Assumido
V3_lenient

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
10

Valor Valor único

ibm-slapdSecurePort

Descrição
Especifica a porta de TCP/IP utilizada para ligações de SSL. Não pode ter o mesmo valor que ibm-slapdPort. (As portas de IP não são assinadas, os números inteiros de 16 bits estão entre 1 - 65535.)

Valor Assumido
636

Sintaxe
Número Inteiro

Comprimento Máximo
5

Valor Valor único

ibm-slapdSecurity

Descrição
Activa ligações de SSL. Tem de ser nenhuma, SSL ou SSLOnly.

- nenhuma - o servidor aguarda resposta apenas na porta não ssl.
- SSL - o servidor aguarda resposta tanto na porta de ssl, como na porta não ssl.
- SSLOnly - o servidor só aguarda resposta na porta de ssl.

Valor Assumido
nenhum

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
7

Valor Valor único

ibm-slapdServerId

Descrição
Identifica o servidor a utilizar na replicação.

Sintaxe
Cadeia IA5 com correspondência de maiúsculas e minúsculas

Comprimento Máximo
240

Valor Valor único

ibm-slapdSetenv

Descrição
O servidor executa **putenv()** para todos os valores de ibm-slapdSetenv no arranque de modo a modificar o respectivo ambiente de tempo de execução. As variáveis de interface (como %PATH% ou $LANG) não são expandidas.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
2000

Valor Vários valores

ibm-slapdSizeLimit

Descrição
Especifica o número máximo de entradas a devolver pela procura, independentemente do tamanho de página que possa ter sido especificado no pedido de procura do cliente (Intervalo = 0...). Se um cliente tiver ultrapassado um limite, serão utilizados o valor mais baixo dos valores do cliente e o valor lido em **ibmslapd.conf**. Se um cliente não tiver ultrapassado um limite e tiver estabelecido ligação como DN admin, o valor será considerado como ilimitado. Se o cliente não tiver ultrapassado um limite e não tiver estabelecido ligação como DN de administração, o limite será o mesmo que foi lido no ficheiro **ibmslapd.conf**. 0 = ilimitado.

Valor Assumido
500

Sintaxe
Número Inteiro

Comprimento Máximo
12

Valor Valor único

ibm-slapdSortKeyLimit

Descrição
O número máximo de condições de ordenação (chaves) que podem ser especificadas num único pedido de procura. Intervalo = 0.... Se um cliente tiver transmitido um pedido de procura com mais chaves de ordenação do que as permitidas pelo limite e o nível de gravidade do controlo de procura ordenada for FALSE, o servidor respeitará o valor lido no ficheiro ibmslapd.conf e ignorará quaisquer chaves de ordenação encontradas após ter sido atingido o limite - a procura e a ordenação serão executadas. Se um cliente tiver transmitido um pedido de procura com mais chaves do que as permitidas pelo limite e o nível de gravidade do controlo de procura ordenada for TRUE, o servidor regressará ao cliente com um código de retorno **adminLimitExceeded** - não será executada a procura, nem a ordenação.

Valor Assumido
3

Sintaxe
cis

Comprimento
11

Contagem
Simples

Utilização
directoryOperation

Modificação pelo Utilizador
Sim

Classe de Acesso
crítica

Objectclass
ibm-slapdRdbmBackend

Obrigatório
Não

ibm-slapdSortSrchAllowNonAdmin

Descrição
Especifica se o servidor deverá ou não permitir uma ligação sem ser pelo Administrador para fins de procura num pedido de procura. Se o valor lido no ficheiro ibmslapd.conf for FALSE, o servidor processará apenas os pedidos de cliente submetidos por um utilizador com autoridade de Administrador. Se um cliente pedir a ordenação para uma operação de procura, não tiver autoridade de Administrador e o valor lido no ficheiro ibmslapd.conf para este atributo for FALSE, o servidor regressará ao cliente com o código de retorno insufficientAccessRights- não será executada a procura, nem a ordenação.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento
5

Contagem
Simples

Utilização
directoryOperation

Modificação pelo Utilizador
Sim

Classe de Acesso
crítica

Objectclass
ibm-slapdRdbmBackend

Obrigatório
Não

ibm-slapdSslAuth

Descrição
Especifica o tipo de autenticação para a ligação de ssl, quer seja serverauth, ou serverclientauth.

- serverauth - suporta a autenticação do servidor no cliente. Este é o valor assumido.
- serverclientauth - suporta a autenticação do servidor e do cliente.

Valor Assumido
serverauth

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
16

Valor Valor único

ibm-slapdSslCertificate

Descrição
Especifica a etiqueta que identifica o Certificado Pessoal do servidor no ficheiro de base de dados de chaves. Esta etiqueta é especificada quando a chave privada e o certificado do servidor são criados com a aplicação **gsk4ikm**. Se ibm-slapdSslCertificate não estiver definido, a chave privada assumida, tal como definida no ficheiro de base de dados de chaves, é utilizada pelo servidor de LDAP para ligações de SSL.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
128

Valor Valor único

ibm-slapdSslCipherSpec

Especifica o método de codificação de SSL para os clientes que acederem ao servidor. Tem de ser definido como um dos seguintes:

Tabela 5. Métodos de codificação de SSL

Atributo	Nível de codificação
TripleDES-168	Codificação DES tripla com uma chave de 168 bits e um MACSHA-1
DES-56	Codificação DES com uma chave de 56 bits e um MAC SHA-1
RC4-128-SHA	Codificação RC4 com uma chave de 128 bits e um MACSHA-1
RC4-128-MD5	Codificação RC4 com uma chave de 128 bits e um MAC MD5
RC2-40-MD5	Codificação RC4 com uma chave de 40 bits e um MAC MD5
RC4-40-MD5	Codificação RC4 com uma chave de 40 bits e um MAC MD5
AES	Codificação AES

Sintaxe
Cadeia IA5

Comprimento Máximo
30

ibm-slapdSslKeyDatabase

Descrição
Especifica o caminho para o ficheiro de base de dados de chaves de SSL do servidor de LDAP. Este ficheiro de base de dados é utilizado para o tratamento de ligações de SSL a partir de clientes de LDAP, bem como para a criação de ligações de SSL seguras a servidores de LADP de réplica.

Valor Assumido
/etc/key.kdb

Sintaxe
Cadeia de directórios com correspondência exacta de maiúsculas e minúsculas.

Comprimento Máximo
1024

Valor Valor único

ibm-slapdSslKeyDatabasePW

Descrição
Especifica a palavra-passe associada ao ficheiro de base de dados de chaves de SSL do servidor de LDAP, tal como especificada no parâmetro ibm-slapdSslKeyDatabase. Se o ficheiro de base de dados de chaves do servidor de LDAP tiver um ficheiro de ocultação de palavras-passe associado, o parâmetro ibm-slapdSslKeyDatabasePW pode ser omitido ou definido como nenhum.

Nota: O ficheiro de ocultação de palavras-passe tem de se encontrar no mesmo directório, e ter o mesmo nome, que o ficheiro de base de dados de chaves, mas com uma extensão .sth em vez de .kdb.

Valor Assumido
nenhum

Sintaxe
Binária

Comprimento Máximo
128

Valor Valor único

ibm-slapdSslKeyRingFile

Descrição
Caminho para o ficheiro de base de dados de chaves de SSL do servidor de LDAP. Este ficheiro de base de dados é utilizado para o tratamento de ligações de SSL a partir de clientes de LDAP, bem como para a criação de ligações de SSL seguras a servidores de LADP de réplica.

Valor Assumido
key.kdb

Sintaxe
Cadeia de Directórios com correspondência de maiúsculas e minúsculas

Comprimento Máximo
1024

Valor Valor único

ibm-slapdSuffix

Descrição
Especifica o contexto de nomenclatura a ser armazenado neste sistema origem.

Nota: Tem o mesmo nome que a classe de objecto.

Valor Assumido
Não está estabelecido nenhum valor predefinido.

Sintaxe
DN

Comprimento Máximo
1000

Valor Vários valores

ibm-slapdSupportedWebAdmVersion

Descrição
Este atributo define a versão mais antiga da ferramenta de administração da Web que suporta este servidor de cn=configuração.

Valor Assumido

Sintaxe
Cadeia de Directórios

Comprimento Máximo

Valor Valor único

ibm-slapdSysLogLevel

Descrição
Especifica o nível em que as estatísticas de depuração e funcionamento são registadas no ficheiro slapd.errors. Tem de ser especificado como l, m ou h.

- h - alto (fornece o máximo de informações)
- m - médio (o valor assumido)
- l - low (fornece o mínimo de informações)

Valor Assumido
m

Sintaxe
Cadeia de directórios sem correspondência de maiúsculas e minúsculas.

Comprimento Máximo
1

Valor Valor único

ibm-slapdTimeLimit

Descrição
Especifica o número máximo de segundos despendidos num pedido de procura, independentemente do limite de tempo que possa ter sido especificado no pedido do cliente. Se um cliente tiver ultrapassado um limite, serão utilizados o valor mais baixo dos valores do cliente e o valor lido em **ibmslapd.conf**. Se um cliente não tiver ultrapassado um limite e tiver estabelecido ligação como DN admin, o valor será considerado como ilimitado. Se o cliente não tiver ultrapassado um limite e não tiver estabelecido ligação como DN de administração, o limite será o mesmo que foi lido no ficheiro **ibmslapd.conf**. 0 = ilimitado.

Valor Assumido
900

Sintaxe
Número Inteiro

Comprimento Máximo

Valor Valor único

ibm-slapdTransactionEnable

Descrição
Se o plugin da transacção estiver carregado, mas ibm-slapdTransactionEnable estiver definido como FALSE, o servidor rejeitará todos os pedidos StartTransaction com a resposta LDAP_UNWILLING_TO_PERFORM.

Valor Assumido
TRUE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdUseProcessIdPw

Descrição
Se for definido como TRUE, o servidor ignorará os atributos ibm-slapdDbUserID e ibm-slapdDbUserPW e utilizará as suas próprias credenciais de processo para se autenticar na DB2.

Valor Assumido
FALSE

Sintaxe
Booleano

Comprimento Máximo
5

Valor Valor único

ibm-slapdVersion

Descrição

Valor Assumido

Sintaxe
Cadeia de Directórios com correspondência de maiúsculas e minúsculas

Comprimento Máximo

Valor Valor único

objectClass

Descrição

Sintaxe
Cadeia de directórios

Comprimento Máximo
128

Valor Vários valores

Capítulo 10. Informações relacionadas

A seguir, poderá encontrar o Redbooks IBM (em formato PDF), sítios da Web e tópicos do centro de informações relacionados com o tópico Directory Server. Pode ver ou imprimir qualquer um destes PDFs.

Redbooks (www.redbooks.ibm.com)

- *Understanding LDAP*, SG24-4986  .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*, SG24-6163. 
- *Implementation and Practical Use of LDAP on the iSeries Server*, SG24-6193  .

Sítios da Web

- Sítio da Web do IBM Directory Server para iSeries (www.ibm.com/servers/eserver/iseries/ldap) 
- Sítio da Web The Java Naming and Directory Interface (JNDI) Tutorial (java.sun.com/products/jndi/tutorial/). 

Outras informações

"APIs do Directory Server" no tópico Programação.

Apêndice. Informações especiais

Estas informações foram desenvolvidas para produtos e serviços disponibilizados nos E.U.A.

Os produtos, serviços ou componentes descritos neste documento poderão não ser disponibilizados pela IBM noutros países. Consulte o representante da IBM para obter informações sobre os produtos e serviços actualmente disponíveis na sua área. Quaisquer referências, nesta publicação, a produtos, programas ou serviços da IBM, não significam que apenas esses produtos, programas ou serviços da IBM possam ser utilizados. Qualquer outro produto, programa ou serviço, funcionalmente equivalente, poderá ser utilizado em substituição daqueles, desde que não infrinja qualquer direito de propriedade intelectual da IBM. No entanto, é da inteira responsabilidade do utilizador avaliar e verificar o funcionamento de qualquer produto, programa ou serviço de terceiros.

Nesta publicação, podem ser feitas referências a patentes ou a pedidos de patente pendentes da IBM. O facto de este documento lhe ser fornecido não lhe confere quaisquer direitos sobre essas patentes. Todos os pedidos de informação sobre licenças deverão ser endereçados a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Para endereçar os seus pedidos de informação sobre licenças relacionados com informações de conjunto de caracteres de duplo byte (DBCS - Double Byte Character Set), contacte o Departamento de Propriedade Intelectual da IBM no seu país ou envie-os, por escrito, para:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

O parágrafo seguinte não se aplica ao Reino Unido nem a qualquer outro país onde estas cláusulas sejam incompatíveis com a lei local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "TAL COMO ESTÁ", SEM GARANTIA DE QUALQUER ESPÉCIE, QUER EXPLÍCITA QUER IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRACÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO FIM. Alguns Estados não permitem a exclusão de garantias, quer explícitas quer implícitas, em determinadas transacções; esta declaração pode, portanto, não se aplicar ao seu caso.

É possível que estas informações contenham imprecisões técnicas ou erros de tipografia. A IBM permite-se fazer alterações periódicas às informações aqui contidas; essas alterações serão incluídas nas posteriores edições desta publicação. A IBM pode introduzir melhorias e/ou alterações ao(s) produto(s) e/ou programa(s) descrito(s) nesta publicação em qualquer altura, sem aviso prévio.

Quaisquer referências, nesta publicação, a sítios da Web de terceiros são fornecidas apenas para conveniência e não deverão nunca servir como aprovação desses sítios da Web. Os materiais existentes nesses sítios da Web não fazem parte dos materiais destinados a este produto da IBM e a utilização desses sítios da Web será da exclusiva responsabilidade do utilizador.

A IBM pode utilizar ou distribuir quaisquer informações que lhe sejam fornecidas pelo utilizador, de qualquer forma que julgue apropriada, sem incorrer em qualquer obrigação para com o autor dessas informações.

Os possuidores de licenças deste programa que pretendam obter informações sobre o mesmo com o objectivo de permitir: (i) a troca de informações entre programas criados de forma independente e outros programas (incluindo este) e (ii) a utilização recíproca das informações que tenham sido trocadas, deverão contactar:

IBM
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Tais informações poderão ser disponibilizadas, sujeitas a termos e condições apropriados, incluindo nalguns casos, ao pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível para o programa são fornecidos pela IBM de acordo com os termos do IBM Customer Agreement, do IBM International Program License Agreement, do IBM License Agreement for Machine Code ou qualquer acordo equivalente entre ambas as partes.

Quaisquer dados de desempenho aqui contidos foram obtidos num ambiente controlado. Assim sendo, os resultados obtidos noutros ambientes operativos podem variar significativamente. Algumas medições podem ter sido efectuadas em sistemas de nível do desenvolvimento, pelo que não existem garantias de que estas medições sejam iguais nos sistemas normalmente disponíveis. Para além disso, algumas medições podem ter sido calculadas por extrapolação. Os resultados reais podem variar. Os utilizadores deste documento devem verificar os dados aplicáveis ao seu ambiente específico.

A informação relativa a produtos de terceiros foi obtida junto dos fornecedores desses produtos, dos seus comunicados ou de outras fontes de divulgação ao público. A IBM não testou esses produtos e não pode confirmar a exactidão do desempenho, da compatibilidade ou de quaisquer outras afirmações relacionadas com produtos produzidos por terceiros. Todas as questões sobre as capacidades dos produtos de terceiros deverão ser endereçadas aos fornecedores desses produtos.

Todas as declarações relativas às directivas ou intenções futuras da IBM estão sujeitas a alterações ou descontinuação sem aviso prévio, representando apenas metas e objectivos.

Todos os preços mostrados são os actuais preços de retalho sugeridos pelaIBM e estão sujeitos a alterações sem aviso prévio. Os preços dos concessionários podem variar.

Estas informações destinam-se apenas a planeamento. As informações estão sujeitas a alterações antes de os produtos descritos ficarem disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados em operações comerciais diárias. Para ilustrá-los o melhor possível, os exemplos incluem nomes de indivíduos, firmas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e moradas reais é mera coincidência.

LICENÇA DE DIREITOS DE AUTOR:

Esta publicação contém programas de aplicação exemplo em linguagem-fonte, que ilustram técnicas de programação em diversas plataformas operativas. Pode copiar, modificar e distribuir estes programas exemplo de qualquer forma, sem encargos para com a IBM, com a finalidade de desenvolver, utilizar, comercializar ou distribuir programas de aplicação conformes à interface de programação de aplicações e destinados à plataforma operativa para a qual os programas exemplo são escritos. Estes exemplos não foram testados exaustivamente sob todas as condições. Deste modo, a IBM não garante nem se responsabiliza pela fiabilidade, assistência ou funcionamento destes destes programas.

SUJEITA A QUAISQUER GARANTIAS LEGAIS QUE NÃO POSSAM SER EXCLUÍDAS, A IBM, OS RESPECTIVOS PROGRAMADORES E FORNECEDORES DO PROGRAMA NÃO FORNECEM

GARANTIAS OU CONDIÇÕES DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS QUER IMPLÍCITAS, INCLUINDO MAS NÃO SE LIMITANDO À GARANTIA OU CONDIÇÕES IMPLÍCITAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM DETERMINADO FIM E NÃO INFRACÇÃO, RELATIVAS AO PROGRAMA OU SUPORTE TÉCNICO, SE APLICÁVEL.

EM CIRCUNSTÂNCIA ALGUMA A IBM, OS RESPECTIVOS PROGRAMADORES OU OS FORNECEDORES DO PROGRAMA SE RESPONSABILIZAM PELO INDICADO ABAIXO, AINDA QUE TENHAM SIDO NOTIFICADOS DA RESPECTIVA POSSIBILIDADE DE OCORRÊNCIA:

1. PERDA OU DANOS DE DADOS;
2. PREJUÍZOS ESPECIAIS, ACIDENTAIS, INDIRECTOS OU QUALQUER OUTRO TIPO DE DANOS COM CONSEQUÊNCIAS FINANCEIRAS; OU
3. PERDA DE LUCRO, NEGÓCIO, RENDIMENTOS, BOA-FÉ OU POUPANÇAS PREVISTAS.

ALGUMAS JURISDIÇÕES NÃO PERMITEM A EXCLUSÃO OU LIMITAÇÃO DE RESPONSABILIDADE POR DANOS ACIDENTAIS OU CONSEQUENTES, PELO QUE ALGUMAS OU TODAS AS EXCLUSÕES OU LIMITAÇÕES PODERÃO NÃO SE APLICAR AO SEU CASO.

Cada cópia, qualquer parte destes programas exemplo ou qualquer trabalho derivado, deve incluir uma notificação de direitos de autor, conforme é mostrado a seguir:

© (nome da empresa) (ano). Partes deste código derivam da IBM Corp. Programas exemplo. © Copyright IBM Corp. _introduzir o ano ou os anos_. Todos os direitos reservados.

Se estiver a consultar estas informações em documentos electrónicos, é possível que as fotografias e as ilustrações a cores não estejam visíveis.

Marcas comerciais

Os termos seguintes são marcas comerciais da International Business Machines Corporation nos Estados Unidos e/ou noutros países:

AIX
AIX 5L
e(logótipo)server
eServer
i5/OS
IBM
iSeries
pSeries
xSeries
zSeries

Intel, Intel Inside (logótipos), MMX e Pentium são marcas comerciais da Intel Corporation nos Estados Unidos e/ou noutros países.

Microsoft, Windows, Windows NT e o logótipo do Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou noutros países.

Java e todas as marcas comerciais baseadas em Java são marcas comerciais da Sun Microsystems, Inc. nos Estados Unidos e/ou noutros países.

Linux é uma marca comercial da Linus Torvalds nos Estados Unidos e/ou noutros países.

UNIX é uma marca comercial registada de The Open Group nos Estados Unidos e noutros países.

Outros nomes de empresas, produtos ou serviços podem ser marcas comerciais ou marcas de serviços de terceiros.

Termos e condições para descarregamento e impressão de informações

As permissões de utilização das informações seleccionadas para descarregamento são concedidas sujeitas aos seguintes termos e condições e à respectiva indicação de aceitação por parte do utilizador.

Utilização pessoal: Pode reproduzir estas informações para uso pessoal e não comercial, desde que mantenha todas as informações de propriedade. Não pode realizar, distribuir ou apresentar qualquer trabalho derivado destas informações, nem qualquer parte das mesmas, sem o expresso consentimento da IBM.

Utilização comercial: Pode reproduzir, distribuir e apresentar estas informações exclusivamente no âmbito da sua empresa, desde que mantenha todas as informações de propriedade. Não pode realizar qualquer trabalho derivado destas informações, nem reproduzir, distribuir ou apresentar estas informações, ou qualquer parte das mesmas, fora das instalações da empresa, sem o expresso consentimento da IBM.

À excepção das concessões expressas nesta permissão, não são concedidos outros direitos, permissões ou licenças, quer explícitos, quer implícitos, sobre as informações ou quaisquer dados, software ou outra propriedade intelectual contidos nesta publicação.

A IBM reserva-se o direito de retirar as permissões concedidas nesta publicação sempre que considerar que a utilização das informações pode ser prejudicial aos seus interesses ou, tal como determinado pela IBM, sempre que as instruções acima referidas não estejam a ser devidamente cumpridas.

Não pode descarregar, exportar ou reexportar estas informações, excepto quando em total conformidade com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação em vigor nos Estados Unidos. A IBM NÃO FORNECE QUAISQUER GARANTIAS RELATIVAMENTE AO CONTEÚDO DESTAS INFORMAÇÕES. AS INFORMAÇÕES SÃO FORNECIDAS "TAL COMO ESTÃO" E SEM GARANTIAS DE QUALQUER ESPÉCIE, QUER EXPLÍCITAS, QUER IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRACÇÃO E ADEQUAÇÃO A UM DETERMINADO FIM.

Todo o material está protegido por direitos de autor da IBM Corporation.

Ao descarregar ou imprimir informações a partir deste sítio da Web, o utilizador indica que concorda com estes termos e condições.