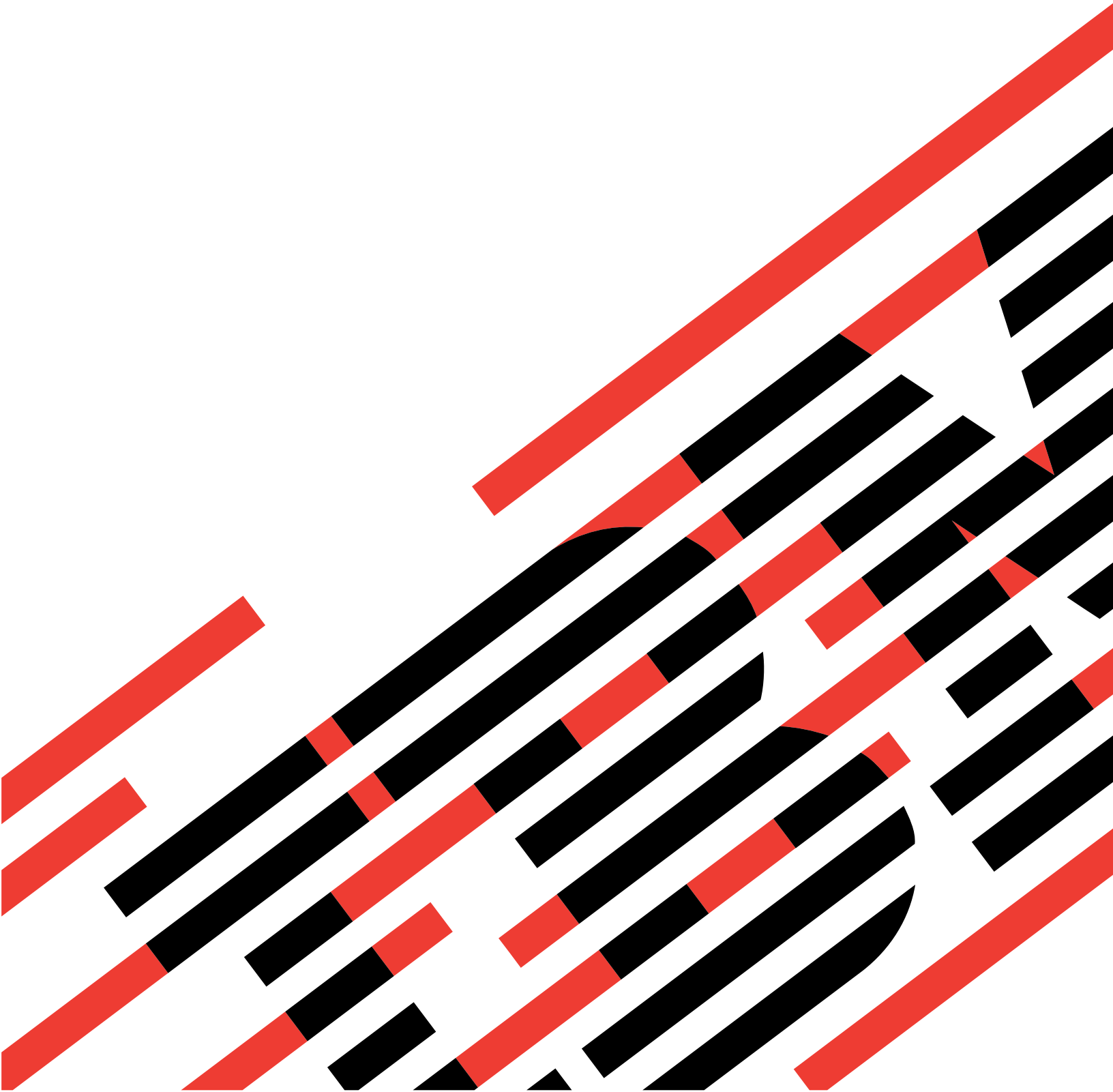
IBM

eserver

iSeries

Serviços de Directório para Funcionamento em Rede (LDAP)



IBM

@server

iSeries

Serviços de Directório para Funcionamento em Rede (LDAP)

Índice

Parte 1. Serviços de Directório (LDAP) 1

Capítulo 1. O que há de novo na V5R2 3

Capítulo 2. Imprimir este tópico 5

Capítulo 3. Como começar com os Serviços de Directório 7
Noções básicas de LDAP 8
Considerações para utilizar o LDAP V2 com o LDAP V3 11
Planear o servidor de directórios de LDAP 11
Migrar para a V5R2 a partir de uma edição anterior dos Serviços de Directório 12
Migrar da V4R3 ou V4R4 dos Serviços de Directório para a V5R2 12
Instalar e configurar os Serviços de Directório 14
Configurar o servidor de directórios de LDAP 14
Configuração assumida dos Serviços de Directório 16
A Ferramenta de Gestão de Directórios IBM SecureWay 17

Capítulo 4. Administrar o servidor de directórios de LDAP 19
Iniciar o servidor de directórios de LDAP 19
Parar o servidor de directórios de LDAP 20
Verificar o estado do servidor de directórios 20
Verificar trabalhos no servidor de directórios de LDAP 20
Activar a notificação de acontecimentos 21
Especificar definições de transacção 21
Alterar a porta ou endereço de IP 21
Mover dados do directório de LDAP entre sistemas 22
Importar um ficheiro de LDIF 22
Exportar um ficheiro de LDIF 22
Configurar uma nova réplica do servidor de directórios 23
Publicar informações no servidor de directórios 27
Especificar um servidor para consultas de directório 29
Adicionar sufixos ao servidor de directórios de LDAP 29
Remover sufixos do servidor de directórios 30
Guardar e restaurar informações dos Serviços de Directório 30
Gerir a propriedade e o acesso a dados de directório 30
Trabalhar com as propriedades de objectos de directório 30
Trabalhar com listas de controlo de acesso (ACLs) 31
Trabalhar com Grupos de ACLs 31
Trabalhar com o acesso administrativo para utilizadores autorizados 31
Registar o acesso e as alterações ao directório de LDAP 32
Activar a auditoria de objectos para o servidor de directórios 33
Ajustar o rendimento do servidor de directórios de LDAP 33

Capítulo 5. Conceitos e informações de consulta dos Serviços de Directório 35
Listas de controlo de acesso (ACLs) de LDAP 35
Formato de troca de dados de LDAP 36
Considerações sobre o suporte de idioma nacional (NLS) 39
Propriedade de objectos do directório de LDAP 39
Consultas do directório de LDAP 39
Transacções 40
Servidores de directórios de LDAP de réplica 40
Segurança dos Serviços de Directório 41

Utilizar Secure Sockets Layer (SSL) e Translation Layer Security com o servidor de directórios de LDAP . . . 41
Utilizar a autenticação de Kerberos com o servidor de directórios de LDAP . . . 42
Programa origem projectado pelo sistema operativo . . . 43
Árvore de informações de directório projectadas pelo utilizador do OS/400 . . . 43
Operações de LDAP . . . 44
DNs do administrador e de ligação de réplicas . . . 48
Esquema projectado pelo utilizador do OS/400 . . . 49
Serviços de Directório e o suporte de registo em diário do OS/400 . . . 49

Capítulo 6. Utilitários de linha de comandos de LDAP . . . 51
Utilitários ldapmodify e ldapadd . . . 51
Exemplos: ldapmodify e ldapadd . . . 53
Utilitário ldapdelete . . . 54
Exemplo: ldapdelete . . . 56
Utilitário ldapsearch . . . 56
Exemplos: ldapsearch . . . 59
Utilitário ldapmodrdn . . . 61
Exemplo: ldapmodrdn . . . 63
Notas sobre a utilização de SSL com os utilitários de linha de comandos de LDAP . . . 63

Capítulo 7. Resolução de problemas dos Serviços de Directório . . . 65
Procedimento básico de resolução de problemas dos Serviços de Directório . . . 65
Supervisionar erros e o acesso com o registo de trabalhos dos Serviços de Directório . . . 66
Utilizar TRCTCPAPP para ajudar a localizar problemas . . . 66
Utilizar a opção LDAP_OPT_DEBUG para rastrear erros . . . 67
Erros comuns do cliente de LDAP . . . 68
ldap_search: Limite de tempo excedido . . . 68
[Falha na operação de LDAP]: Erro nas operações . . . 68
ldap_bind: Não existe nenhum objecto desse tipo . . . 68
ldap_bind: Autenticação incorrecta . . . 68
[Erro no funcionamento de LDAP]: Acesso insuficiente . . . 69
[Falha na operação de LDAP]: Não é possível contactar o servidor de LDAP . . . 69
[Falha na operação de LDAP]: A ligação ao servidor de SSL falhou . . . 69

Parte 1. Serviços de Directório (LDAP)

Os Serviços de Directório fornecem um servidor de Lightweight Directory Access Protocol (LDAP) no 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.

Se já estiver familiarizado com os Serviços de Directório, poderá ter interesse em ler em primeiro lugar o que há de novo nesta edição. Se quiser, pode imprimir ou visualizar uma versão em PDF das informações sobre os Serviços de Directório.

Os tópicos que se seguem apresentam os Serviços de Directório e fornecem-lhe informações para ajudá-lo a administrar o servidor de LDAP no seu iSeries™:

Capítulo 3, “Como começar com os Serviços de Directório” na página 7

Capítulo 4, “Administrar o servidor de directórios de LDAP” na página 19

Capítulo 5, “Conceitos e informações de consulta dos Serviços de Directório” na página 35

Capítulo 6, “Utilitários de linha de comandos de LDAP” na página 51

Capítulo 7, “Resolução de problemas dos Serviços de Directório” na página 65

Para obter mais informações sobre os Serviços de Directório, visite a página da Web dos Serviços de Directório .

O servidor de LDAP fornecido pelos Serviços de Directório é um IBM® SecureWay® Directory .

Capítulo 1. O que há de novo na V5R2

Os Serviços de Directório apresentam os seguintes melhoramentos e novas funções.

- Os Serviços de Directório fazem parte do sistema operativo base a partir da V5R1. A partir da V5R2, a opção 32 deixa de estar disponível.
- Foram efectuados melhoramentos na segurança de modo a proteger quaisquer dados armazenados no servidor de directórios.
- O servidor de directórios de LDAP pode ser, agora, utilizado como controlador de um domínio de Enterprise Identity Mapping (EIM).
- Está disponível uma nova opção para administradores que pode ser utilizada para conceder aos administradores acesso ao servidor de directórios relativamente aos utilizadores aos quais foi concedido acesso ao identificador de função (ID) do Administrador dos Serviços de Directório (QIBM_DIRSRV_ADMIN) do sistema operativo através do suporte de aplicações do iSeries Navigator.
- Pode optar por fazer com que o servidor de directórios utilize endereços de IP específicos ou por utilizar todos os endereços de IP configurados no servidor. Consulte o tópico “Alterar a porta ou endereço de IP” na página 21 para obter mais informações.
- A API **ldap_set_option** tem uma nova função de rastreio de depuração para a V5R2. A opção LDAP_OPT_DEBUG pode ser utilizada para ajudar a diagnosticar problemas com clientes que utilizam as APIs de C de LDAP. Para obter mais informações, consulte o tópico “Utilizar a opção LDAP_OPT_DEBUG para rastrear erros” na página 67 ou as APIs dos Serviços de Directório no Information Center do iSeries  .

Como ver o que é novo ou alterado:

Para o ajudar a encontrar a localização das alterações técnicas, estas informações utilizam:

- O símbolo  para marcar onde é que têm início as informações novas e alteradas.
- O símbolo  para marcar onde é que terminam as informações novas e alteradas.

Capítulo 2. Imprimir este tópico

Para ver ou descarregar a versão em PDF, seleccione os Directory Services (LDAP) (cerca de 323 KB ou 66 páginas).

Outras informações

Também poderá ver ou imprimir qualquer um dos seguintes PDFs:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino* .
- *Implementation and Practical Use of LDAP on the iSeries Server* .

Para guardar um PDF na sua estação de trabalho para consulta ou impressão:
1. Abra o PDF no seu browser (faça clique sobre a ligação acima referida).
2. No menu do seu browser, faça clique sobre **Ficheiro**.
3. Faça clique sobre **Guardar Como...**
4. Navegue até ao directório no qual gostaria de guardar o PDF.
5. Faça clique sobre **Guardar**.

Descarregar o Adobe Acrobat Reader

Se necessitar do Adobe Acrobat Reader para ver ou imprimir estes PDFs, pode descarregar uma cópia a partir do site da Web da Adobe (www.adobe.com/products/acrobat/readstep.html) .

Capítulo 3. Como começar com os Serviços de Directório

Os Serviços de Directório fornecem um servidor de Lightweight Directory Access Protocol (LDAP) no servidor iSeries. O LDAP é executado no Transmission Control Protocol/Internet Protocol (TCP/IP) e está a ganhar popularidade como serviço de directório para aplicações de Internet e sem ser de Internet. Pode efectuar a maior parte das tarefas de configuração e administração do servidor de directórios de LDAP no OS/400 através da interface gráfica do utilizador (GUI) do iSeries Navigator. Para administrar os Serviços de Directório, terá de ter instalado o iSeries Navigator num PC que esteja ligado ao servidor iSeries. Pode utilizar os Serviços de Directório com aplicações activadas por LDAP como, por exemplo, aplicações de correio que procuram endereços de correio electrónico em servidores de LDAP.

Para além do servidor de LDAP, os Serviços de Directório incluem igualmente:

- Um cliente de LDAP baseado no OS/400. Este cliente inclui um conjunto de interfaces de programação de aplicações (APIs) que pode utilizar em programas do OS/400® para criar as suas próprias aplicações de cliente. Para obter informações sobre estas APIs, consulte o tópico Directory Services em Programming, no iSeries Information Center.
- Versão 3.2 do IBM SecureWay Directory Client Software Development Kit (SDK). O SDK inclui um cliente de LDAP do Windows® e as seguintes ferramentas:
  - A Ferramenta de Gestão de Directórios IBM SecureWay, que lhe fornece uma interface gráfica de utilizador para a gestão do conteúdo de directórios.
  - utilitários de linha de comandos (ldapsearch, ldapadd, etc.)
  - APIs C de LDAP (ficheiros de biblioteca, ficheiros de cabeçalho e código fonte de exemplo)
  - Fornecedor de serviços de JNDI LDAP da IBM (ibmjndi.jar)
  - documentação online para todos os itens anteriores. Consulte o ficheiro leiame (readme) para obter a localização e nomes destes ficheiros HTML.

Se tiver utilizado os Serviços de Directório com uma edição anterior do OS/400, consulte o tópico “Migrar para a V5R2 a partir de uma edição anterior dos Serviços de Directório” na página 12.

Para ver uma introdução ao LDAP, consulte o tópico “Noções básicas de LDAP” na página 8. Se tiver utilizado servidores de LDAP noutras plataformas, deverá dispor de alguns minutos para ler este tópico, uma vez que contém algumas informações específicas do OS/400.

Quando estiver familiarizado com as informações base, avance para o tópico “Planear o servidor de directórios de LDAP” na página 11.

Para obter informações sobre a instalação e configuração do servidor de directórios, consulte o tópico “Instalar e configurar os Serviços de Directório” na página 14.

Documentação

O tópico Serviços de Directório do Information Center fornece uma descrição geral do LDAP e concentra-se especificamente na gestão do servidor de directórios de LDAP no OS/400. Esta documentação também fornece a documentação completa do SDK do Cliente de SecureWay Directory. Para obter informações de LDAP adicionais, consulte outra documentação de LDAP como, por exemplo:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino* .

- *Implementation and Practical Use of LDAP on the iSeries server*  .
- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol* de Tim Howes e Mark Smith.
- *Understanding and Deploying LDAP Directory Services* de Mark C. Smith, Gordon S. Good e Tim Howes.

Estão disponíveis informações adicionais sobre os Serviços de Directório no servidor iSeries na página inicial dos Serviços de Directório do servidor iSeries  .

Nota: Algumas das informações contidas neste documento provêm da documentação de LDAP fornecida pela Universidade de Michigan. Copyright © 1992-1996, Regents of the University of Michigan, Todos os Direitos Reservados.

Noções básicas de LDAP

O Lightweight Directory Access Protocol (LDAP) é um protocolo de serviço de directório que é executado através do Transmission Control Protocol/Internet Protocol (TCP/IP). O LDAP versão 2 foi formalmente definido no Pedido de Comentários (RFC) 1777 do Internet Engineering Task Force (IETF) como *Lightweight Directory Access Protocol*. O LDAP versão 3 foi formalmente definido no IETF RFC 2251, como *Lightweight Directory Access Protocol (v3)*. Pode ver estes RFCs na Internet, no seguinte URL:

http://www.ietf.org 

O serviço de directório de LDAP segue um modelo de cliente/servidor. Um ou mais servidores de LDAP contêm os dados do directório. Um cliente de LDAP estabelece ligação a um Servidor de LDAP e faz um pedido. O servidor envia uma resposta ou um apontador (uma referência) para outro servidor de LDAP.

Utilizações de LDAP:

Uma vez que o LDAP é um serviço de directório e não uma base de dados, as informações no directório de LDAP são, normalmente, descritivas e baseadas em atributos. Normalmente, os utilizadores de LDAP lêem as informações do directório muito mais frequentemente do que as alteram. As actualizações são alterações simples do tipo tudo ou nada. As utilizações comuns de directórios de LDAP incluem listas de telefones e listas de endereços de correio electrónico online.

Estrutura do directório de LDAP:

O modelo do serviço de directório de LDAP é baseado nas **entradas** (que são também referidas como **objectos**). Cada entrada é composta por um ou mais **atributos** como, por exemplo, um nome ou um endereço e um **tipo**. Normalmente, os tipos são constituídos por cadeias mnemónicas como, por exemplo, `nc` para nome comum ou `correio` para endereço de correio electrónico.

O directório exemplo da Figura 1 na página 10 mostra uma entrada para Tiago Jesus que inclui atributos de *correio* e de *NúmeroTelefone*. Outros atributos possíveis incluem *fax*, *cargo*, *ap* (para apelido) e *jpegPhoto*.

Cada directório tem um **esquema**, que é um conjunto de regras que determinam a estrutura e o conteúdo do directório. Deverá utilizar a Ferramenta de Gestão de Directórios (DTM) IBM SecureWay para editar os ficheiros de esquema do servidor de LDAP. Depois de instalar o Serviços de Directório, os ficheiros encontrar-se-ão no sistema em `/QIBM/UserData/OS400/DirSrv`.

Nota: As cópias originais dos ficheiros de esquema assumidos estão localizadas em `/QIBM/ProdData/OS400/DirSrv`. Se tiver de substituir os ficheiros do directório UserData, poderá copiar esses ficheiros para o directório /QIBM/ProdData/OS400/DirSrv.

Cada entrada de directório tem um atributo especial denominado **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 de esquemas a que a entrada tem de obedecer.

Cada entrada do directório tem também os seguintes **atributos operacionais**, mantidos automaticamente pelo servidor de LDAP:

- `CreatorsName`, que contém o DN associado, utilizado ao criar a entrada.
- `CreateTimestamp`, que contém a hora a que a entrada foi criada.
- `modifiersName`, que contém o DN associado, utilizado quando a entrada foi modificada pela última vez (inicialmente este é o mesmo que `CreatorsName`).
- `modifyTimestamp`, que contém a hora a que a entrada foi modificada pela última vez (inicialmente este é o mesmo que `CreateTimestamp`).

Tradicionalmente, as entradas do directório de LDAP são dispostas numa estrutura hierárquica, que reflecte limites políticos, geográficos ou organizacionais (consultar Figura 1 na página 10). As entradas que representam países são apresentadas 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.

Não está limitado(a) 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 `e=ibm,p=po`.

O LDAP refere-se a entradas com **Nomes Distintos** (DNs). Os Nomes Distintos 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 do canto inferior esquerdo da Figura 1 na página 10 é `nc=Tiago Jesus, e=IBM, p=PO`. Cada entrada tem, pelo menos, um atributo utilizado para atribuir um nome à entrada. Este atributo de nomenclatura é denominado **Nome Distinto Relativo (RDN)** da entrada. A entrada acima de um RDN especificado é designada por **Nome Distinto ascendente**. No exemplo anterior, `nc=Tiago Jesus` dá o nome à entrada, pelo que é o RDN. `e=IBM, p=PO` é o DN ascendente de `nc=Tiago Jesus`.

Para dar a um servidor de LDAP a possibilidade de gerir parte de um directório de LDAP, especifique os nomes distintos ascendentes de nível superior na configuração do servidor. Estes nomes distintos denominam-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 em Figura 1 na página 10, necessitaria do sufixo `e=ibm, p=po` especificado na respectiva configuração para poder responder a consultas do cliente relacionadas com Tiago Jesus.

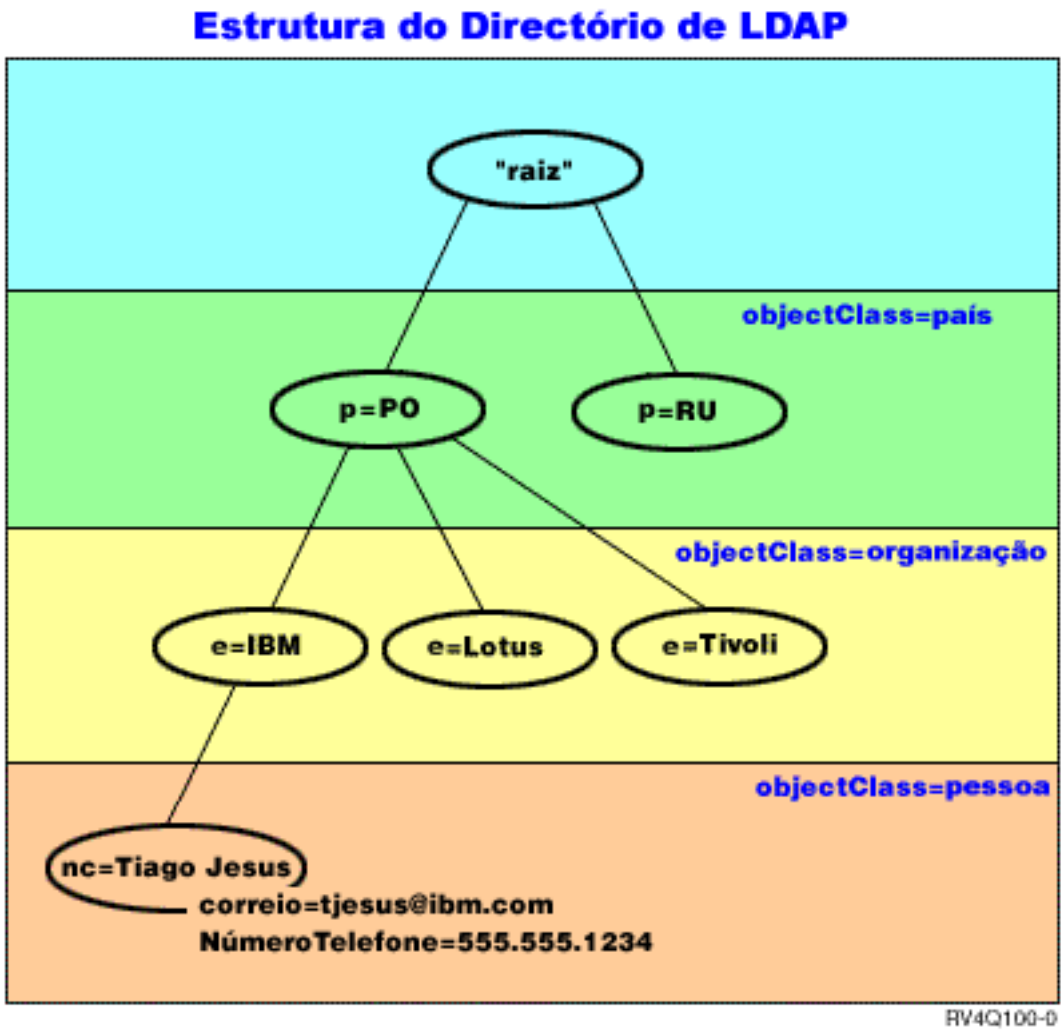


Figura 1. Estrutura básica do directório de LDAP

Notas sobre o LDAP e os Serviços de Directório:

- A partir da V4R5, tanto o servidor de LDAP do OS/400 como o cliente de LDAP do OS/400 se baseiam no LDAP Versão 3. Pode utilizar um cliente da V2 com um servidor da V3. Contudo, não pode utilizar um cliente da V3 com um servidor da V2, a não ser que estabeleça uma associação como cliente da V2 e utilize apenas APIs da V2. Consulte o tópico Considerações da V2/V3 de LDAP para obter mais detalhes.
- O cliente de LDAP do Windows também se baseia no LDAP Versão 3.
- Como o LDAP é um protocolo standard, todos os servidores de LDAP partilham muitas características base. No entanto, devido a diferenças de implementação, não são todos totalmente compatíveis entre si. O servidor de LDAP fornecido pelos Serviços de Directório é bastante compatível com outros servidores de directórios de LDAP do grupo de produtos IBM SecureWay Directory e IBM Directory. No entanto, pode não ser tão compatível com outros servidores de LDAP.
- Os dados do servidor de LDAP fornecidos pelos Serviços de Directório residem numa base de dados do OS/400.

Mais informações:

Para ver exemplos da utilização de directórios de LDAP, consulte:

- Secção 1.6 The Quick Start: A Public LDAP Example, no redbook *Understanding LDAP*.

- Secção 3.3 Example Scenarios, no redbook Understanding LDAP.

Para obter mais informações sobre conceitos de LDAP, consulte o Capítulo 5, “Conceitos e informações de consulta dos Serviços de Directório” na página 35.

Considerações para utilizar o LDAP V2 com o LDAP V3

A partir da V4R5, tanto o servidor de LDAP do OS/400 como o cliente de LDAP do OS/400 baseiam-se no LDAP Versão 3. Não pode utilizar um cliente da V3 com um servidor da V2. Contudo, pode utilizar a API ldap_set_option() para alterar a versão de um cliente V3 para V2. Assim poderá enviar com êxito pedidos de clientes para um servidor V2.

Pode utilizar um cliente V2 com um servidor V3. Tenha em atenção que num pedido de procura o servidor V3 pode devolver dados utilizando o intervalo completo do formato UTF-8, enquanto que um cliente V2 só consegue processar dados no conjunto de caracteres IA5.

Nota: O LDAP versão 2 foi formalmente definido no Pedido de Comentários (RFC) 1777 do Internet Engineering Task Force (IETF) como *Lightweight Directory Access Protocol*. O LDAP versão 3 foi formalmente definido no IETF RFC 2251, como *Lightweight Directory Access Protocol (v3)*. Pode ver estes RFCs na Internet, no seguinte URL:

http://www.ietf.org

Planear o servidor de directórios de LDAP

Antes de instalar os Serviços de Directório 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.
- **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 do directório.
  - O número de entradas do servidor.
  - O tipo de informações que armazena no servidor.

  Por exemplo, um directório vazio que utiliza o esquema do Serviços de Directório 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 objectos grandes, como imagens, no directório.
- **Decidir quais as medidas de segurança que irá tomar**. Os Serviços de Directório suportam a utilização de Secure Sockets Layer (SSL) e Certificados Digitais, bem como Translation Layer Security (TLS) para a segurança de comunicações. A partir da V5R1, a autenticação de Kerberos também é suportada.
- Os Serviços de Directório permitem-lhe controlar o acesso a objectos de directório com listas de controlo de acesso (ACLs). Também pode utilizar a auditoria de segurança do OS/400 para proteger o directório.

Migrar para a V5R2 a partir de uma edição anterior dos Serviços de Directório

A V5R2 do OS/400 apresenta novas funções e capacidades para os Serviços de Directório. Estas alterações afectam tanto o servidor de directórios 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 anterior do iSeries Navigator instalada, deverá actualizar para a V5R2.

A V5R2 do OS/400 suporta actualizações da V4R5 e da V5R1. Quando actualiza para a V5R2 do OS/400, tanto os dados do directório de LDAP, como os ficheiros de esquema de directório são automaticamente migrados para ficarem em conformidade com os formatos da V5R2. Se tiver um servidor de LDAP dos Serviços de Directório em execução sob a V4R3 ou V4R4 do OS/400 e pretende migrar o servidor para a V5R2, terá de executar algumas tarefas de migração adicionais.

Quando actualiza para a V5R2 do OS/400, deverá ter em consideração algumas questões relacionadas com migração:

- Quando actualiza para a V5R2, os Serviços de Directório migram automaticamente os seus ficheiros de esquema para a V5R2 e eliminam os ficheiros de esquema antigos. Contudo, se tiver eliminado ou atribuído outro nome aos ficheiros de esquema, os Serviços de Directório não podem migrá-los. Pode receber um erro ou os Serviços de Directório podem assumir que os ficheiros já foram migrados.
- Os Serviços de Directório migram dados de directório para o formato da V5R2 na primeira vez que inicia o servidor ou importa um ficheiro de LDIF. Reserve algum tempo para a conclusão da migração. Se estiver a actualizar para a V5R2 a partir da V4R4 ou anterior, tenha em consideração que os dados de directório irão requerer aproximadamente o dobro do espaço de memória na V5R2 que requeriam anteriormente. Isto acontece porque na V4R4 ou nas versões anteriores, os Serviços de Directório apenas suportavam o conjunto de caracteres IA5 e guardavam dados em ccsid 37 (formato de byte único). Os Serviços de Directório suportam o conjunto de caracteres completo de ISO 10646.

  Após actualizar para a V5R2, 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.
- A V4R4 e as edições anteriores dos Serviços de Directório não levavam em consideração os fusos horários quando criavam entradas de marcas de hora. A partir da V4R5, o fuso horário é utilizado em todas as adições e modificações feitas no directório. Assim, se actualizar para a V5R2 a partir da V4R4 ou de uma versão anterior, os Serviços de Directório ajustam 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 das 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.
- Após a migração, o servidor de directórios de LDAP será automaticamente iniciado quando o TCP/IP for iniciado. Se não desejar que o servidor de directórios seja iniciado automaticamente, utilize o iSeries Navigator para alterar essa definição.

Migrar da V4R3 ou V4R4 dos Serviços de Directório para a V5R2

A V5R2 do OS/400 não suporta actualizações directas da V4R3. Se pretender migrar um servidor de LDAP da V4R3 ou V4R4 dos Serviços de Directório para a V5R2, pode efectuar um dos seguintes procedimentos:

- Instalação via SLIP do OS/400 da V4R3 ou V4R4 para uma edição intermédia
- Guardar a biblioteca de bases de dados e executar uma instalação de raiz do OS/400 da V4R3 ou V4R4 para a V5R2

Instalação via SLIP do OS/400 da V4R3 ou V4R4 para uma edição intermédia

Embora as actualizações da V4R3 e V4R4 do OS/400 para a V5R2 não sejam suportadas, são suportadas as seguintes actualizações:

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

Uma forma de migrar o servidor dos Serviços de Directório é actualizar para uma versão intermédia (V4R5 ou V5R1) e, em seguida, para a V5R2. Para obter informações detalhadas sobre os procedimentos de instalação do OS/400, consulte o tópico *Instalação de Software*  . Siga estes passos gerais para efectuar a migração:

1. Observer quaisquer alterações que tenha efectuado aos ficheiros de esquema no directório /QIBM/UserData/OS400/DirSrv. Os ficheiros de esquema são migrados automaticamente.
2. No que se refere à V4R4 ou V4R3, efectue a instalação via SLIP da V4R5 ou V5R1 do OS/400.
3. Execute a instalação via SLIP para a V5R2 do OS/400.
4. Inicie o servidor dos Serviços de Directório, se ainda não o tiver feito.
5. Utilize a Ferramenta de Gestão de Directórios para modificar os ficheiros de esquema implementando de novo quaisquer alterações que tenha anotado no passo 1.
6. Reinicie o servidor dos Serviços de Directório.

Guardar a biblioteca de bases de dados e efectuar a instalação de raiz do OS/400 da V4R3 ou V4R4 para a V5R2

A outra forma de migrar o servidor dos Serviços de Directório é guardar a biblioteca de bases de dados utilizada pelos Serviços de Directório na V4R3 ou V4R4 e restaurá-la após a instalação de raiz da V5R2. Este procedimento poupa-lhe o passo da instalação de uma edição intermédia. No entanto, as definições do servidor não são migradas, de modo que terá de as reconfigurar. Para obter informações detalhadas sobre os procedimentos de instalação do OS/400, consulte o tópico *Instalação de Software*  . Siga estes passos gerais para efectuar a migração:

1. Observe quaisquer alterações que tenha efectuado aos ficheiros de esquema no directório /QIBM/UserData/OS400/DirSrv. Os ficheiros de esquema não são migrados automaticamente; por isso, se desejar manter as alterações, terá de as implementar de novo manualmente.
2. Observe as várias definições de configuração nas propriedades do servidor dos Serviços de Directório, incluindo o nome da biblioteca de bases de dados.
3. Guarde a biblioteca de bases de dados que está especificada na configuração do servidor dos Serviços de Directório.
4. Observe a configuração da publicação.
5. Execute uma instalação de raiz do sistema da V5R2 do OS/400.
6. Utilize o EZ-Setup para configurar o servidor dos Serviços de Directório.
7. Restaure a biblioteca de bases de dados que tinha guardado no passo 3.
8. Utilize a Ferramenta de Gestão de Directórios para modificar os ficheiros de esquema implementando de novo quaisquer alterações que tenha anotado no passo 1.
9. Utilize o iSeries Navigator para reconfigurar os Serviços de Directório. Especifique a biblioteca de bases de dados que guardou e restaurou.
10. Utilize o iSeries Navigator para reconfigurar a publicação.
11. Reinicie o servidor dos Serviços e Directório.

Questões Relacionadas com a Actualização

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 Client Access da V3R2 utilizava ficheiros do conjunto de chaves mistas para estabelecer ligações de Secure Sockets Layer (SSL) ao servidor de directórios de LDAP. O iSeries Access para Windows utiliza armazenamentos de certificados, por vezes, designados bases de dados de chaves, para estabelecer ligações de SSL. Se utilizou anteriormente um ficheiro do conjunto de chaves mistas com o servidor de directórios LDAP, esse ficheiro tem de ser convertido para uma base de dados de chaves para poder continuar a utilizar o SSL. A primeira vez que tentar iniciar uma ligação de SSL num servidor de directórios de LDAP, o iSeries Navigator avisá-lo-á desta alteração. Se optar por converter a chave, ser-lhe-á pedido que especifique algumas informações para a base de dados de chaves antes de a conversão poder ser efectuada.

  O servidor de directórios 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 ficheiros de dados contínuos utilizados por Serviços de Directório 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 necessita de tomar qualquer medida com estes ficheiros. Isto só é mencionado para que não se preocupe se reparar que já não estão presentes no sistema.

Tenha também em atenção que podem haver questões adicionais associadas à actualização da edição actual a partir de outras edições.

Instalar e configurar os Serviços de Directório

Os Serviços de Directório (LDAP) são automaticamente instalados quando instala o OS/400. O servidor de directórios inclui uma configuração assumida que inicia automaticamente o servidor de directórios quando o TCP/IP for iniciado. O servidor de directórios também começará a publicar informações do computador a partir do OS/400 no servidor de directórios. Para personalizar as definições dos servidores de directórios de LDAP, execute o Assistente de Configuração dos Serviços de Directório. Tem de ter as autoridades especiais *ALLOBJ e *IOSYSCFG para utilizar o assistente.

Os Serviços de Directório estão integrados no sistema operativo base a partir da V5R1 e a Opção 32 já não está disponível a partir da V5R2.

Configurar o servidor de directórios de LDAP

Se o sistema não tiver sido configurado para publicar informações noutro servidor de LDAP e nenhum servidor de LDAP for conhecido do servidor de DNS de TCP/IP, os Serviços de Directório serão automaticamente instalados com uma configuração assumida limitada. Os Serviços de Directório fornecem um assistente para o ajudar na configuração do servidor de directórios de LDAP 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 servidor de directórios. Pode igualmente utilizar o assistente para reconfigurar o servidor de directórios.

Nota: Quando utiliza o assistente para reconfigurar o servidor de directórios, começa a configuração desde o início. Em vez de ser alterada, a configuração original é eliminada. No entanto, os dados de directório não são eliminados; pelo contrário, permanecem armazenados na biblioteca que seleccionou durante a 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 servidor de directórios, 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.

Para iniciar o Assistente de Configuração dos Serviços de Directório, efectue os seguintes 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 **Configurar**.

Nota: Se já tiver configurado o servidor de directórios, faça clique sobre **Reconfigurar** em vez de fazer clique sobre **Configurar**.

Siga as instruções apresentadas pelo assistente Configurar Servidor de Directórios para configurar o servidor de directórios de LDAP.

Nota: Pode também querer 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.

Quando o assistente terminar, o servidor de directórios de LDAP terá uma configuração base. Se estiver a executar o Lotus® Domino no sistema, a porta 389 (a porta assumida do 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
- Alterar a porta utilizada pelos Serviços de Directório
- Utilizar endereços de IP específicos

Pode iniciar o servidor neste ponto. No entanto, antes de iniciar o servidor, pode desejar executar algumas ou todas as seguintes operações:
- Importar dados para o servidor
- Activar a segurança de Secure Sockets Layer (SSL)
- Activar a autenticação de Kerberos
- Configurar uma consulta

Activar SSL no servidor de directórios de LDAP

Se tiver o Gestor de Certificados Digitais instalado no sistema, poderá utilizar a segurança do Secure Sockets Layer (SSL) para proteger o acesso ao servidor de directórios de LDAP. Antes de activar o SSL no servidor de directórios, poderá considerar útil ler uma descrição geral da utilização do SSL com os Serviços de Directório.

Para utilizar uma ligação de SSL quando administra o servidor de directórios de LDAP a partir do iSeries Navigator, ou para utilizar o SSL com o cliente de LDAP do Windows, tem de ter um dos produtos Client Encryptions (5722CE2 ou 5722CE3) instalados no PC.

Para activar o SSL no servidor de LDAP, utilize a interface do Gestor de Certificados Digitais. Pode iniciar o Gestor de Certificados Digitais a partir do arquivador **Internet** no iSeries Navigator, ou a partir da página **Rede** da caixa de diálogo **Propriedades** dos servidores de directórtios.

Para iniciar a Interface de Certificados Digitais a partir da página **Rede**, 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 **Rede**.
6. Faça clique sobre **Gestor de Certificados Digitais**.

   O Gestor de Certificados Digitais irá iniciar o browser de Internet assumido.

Consulte o tópico Proteger o servidor de directórios de LDAP para os passos específicos que necessita de seguir para atribuir um certificado digital ao servidor de directórios.

Após a activação de SSL, poderá alterar a porta que o servidor de directórios de LDAP utiliza para ligações seguras.

Activar a autenticação de Kerberos no servidor de directórios de LDAP

Se tiver o Serviço de Autenticação de Rede configurado no sistema, pode configurar o servidor de directórios de LDAP para utilizar a autenticação de Kerberos. Antes de activar o Kerberos no servidor de directórios, poderá achar útil ler uma descrição geral da utilização do Kerberos com os Serviços de Directório.

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 as páginas de ajuda online para obter informações sobre campos individuais.

Configuração assumida dos Serviços de Directório

O servidor de directórios de LDAP é automaticamente instalado quando instala o OS/400. Esta instalação inclui uma configuração assumida. O servidor de directórios utilizar a configuração assumida quando todas as seguintes condições forem verdadeiras:

- Os administradores não tiverem executado o Assistente de Configuração dos Serviços de Directório ou alterado as definições de directório com as páginas de propriedades.
- A publicação do Serviços de Directório não estiver configurada.
- O servidor de directórios de LDAP não conseguir encontrar as informações de DNS de LDAP.

Se o servidor de directórios de LDAP utiliza a configuração assumida, ocorrerá o seguinte:

- O servidor de directórios de LDAP será iniciado automaticamente quando o TCP/IP for iniciado.
- O sistema cria um administrador assumido, nc=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 Serviços de Directório.
- É criado um sufixo assumido que é 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 sistema for maria.empresa.com, o sufixo é dc=maria,dc=empresa,dc=com.
- O servidor de directórios de LDAP utiliza a biblioteca de dados assumida QUSRDIRDB. O sistema cria-o 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.

Em seguida, existirão os seguintes valores assumidos para publicação dos Serviços de Directório:

- O sistema publica informações no servidor de directórios de LDAP
- A publicação não utiliza o SSL
- A publicação utiliza contentores sob o sufixo assumido
- Para a autenticação do servidor de directórios, OS/400 utiliza o ID nc=Administrador e a palavra-passe gerada pelo sistema.
- O sistema publica apenas informações do sistema

A Ferramenta de Gestão de Directórios IBM SecureWay

A Ferramenta de Gestão de Directórios IBM SecureWay (DMT) fornece-lhe uma interface gráfica de utilizador para gerir o conteúdo dos directórios de LDAP. As tarefas que pode realizar com a DMT incluem:

- Procurar esquemas de directórios
- Adicionar, editar e eliminar classes de objectos
- Adicionar, editar e eliminar atributos
- Percorrer e procurar a árvore de directórios
- Adicionar, editar, visualizar e eliminar entradas
- Editar RDNs de entrada
- Gerir ACLs

A DMT faz parte do cliente de LDAP do Windows que está incluído nos Serviços de Directório. O cliente é enviado num directório de sistema de ficheiros integrados.

Para instalar o cliente de LDAP do Windows, incluindo a DMT, num PC, siga estes passos:

1. No iSeries Navigator, expanda **Sistemas de Ficheiros**.
2. Expanda **Partilhas de Ficheiros**.
3. Faça duplo clique sobre **Qdirsrv**.
4. Faça duplo clique sobre **UserTools**.
5. Faça duplo clique sobre **Windows**.
6. Faça duplo clique sobre **setup.exe** para iniciar a instalação da DMT. Siga as instruções no ecrã para concluir a instalação.

A documentação da Ferramenta de Gestão de Directórios (DTM) IBM SecureWay encontra-se no ficheiro `dparent.htm`. Este ficheiro é copiado para o arquivador IBM SecureWay Directory do PC quando instala o cliente.

Capítulo 4. Administrar o servidor de directórios de LDAP

Para administrar o servidor de directórios de LDAP, tem de ter os seguintes conjuntos de autoridade:

- 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 servidor de directórios: 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 a integração da autoridade estiver a ser utilizada, um administrador também pode ser um utilizador projectado que tenha autoridade para o ID de função do Administrador de Serviços de Directório.

A administração do servidor de directórios inclui as seguintes tarefas:

- "Iniciar o servidor de directórios de LDAP"
- "Parar o servidor de directórios de LDAP" na página 20
- "Verificar o estado do servidor de directórios" na página 20
- "Verificar trabalhos no servidor de directórios de LDAP" na página 20
- "Activar a notificação de acontecimentos" na página 21
- "Especificar definições de transacção" na página 21
- "Alterar a porta ou endereço de IP" na página 21
- "Mover dados do directório de LDAP entre sistemas" na página 22
- "Especificar um servidor para consultas de directório" na página 29
- "Adicionar sufixos ao servidor de directórios de LDAP" na página 29
- "Remover sufixos do servidor de directórios" na página 30
- "Guardar e restaurar informações dos Serviços de Directório" na página 30
- "Gerir a propriedade e o acesso a dados de directório" na página 30
- "Registar o acesso e as alterações ao directório de LDAP" na página 32
- "Activar a auditoria de objectos para o servidor de directórios" na página 33
- "Ajustar o rendimento do servidor de directórios de LDAP" na página 33

Iniciar o servidor de directórios de LDAP

Para iniciar o servidor de directórios de LDAP, efectue 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** e seleccione **Iniciar**.

   O servidor de directórios pode demorar alguns minutos a ser iniciado, dependendo da velocidade do servidor e da quantidade de memória disponível. A primeira vez que iniciar o servidor de directórios pode demorar mais alguns minutos do que habitualmente porque o servidor tem de criar ficheiros novos. De igual modo, quando inicia o servidor de directórios pela primeira vez depois de fazer a actualização de uma versão anterior de Serviços de Directório, pode levar mais alguns minutos do que o habitual, porque o servidor tem de migrar ficheiros. Pode verificar o estado do servidor periodicamente, para ver se já foi iniciado.

Nota: O servidor de directórios pode igualmente ser iniciado a partir de uma sessão de 5250, escrevendo o comando `STRTCPSVR *DIRSRV`.

Adicionalmente, se o servidor de directórios estiver configurado para ser iniciado quando inicia o TCP/IP, poderá igualmente iniciá-lo escrevendo o comando STRTCP.

Parar o servidor de directórios de LDAP

A paragem do servidor de directórios 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 servidor de directórios para operações de EIM. Todas as aplicações são desligadas do servidor de directórios, embora não sejam impedidas de tentar estabelecer nova ligação com o servidor.

Para parar o servidor de directórios de LDAP, efectue 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** e seleccione **Parar**.

   O servidor de directórios 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 o estado do servidor periodicamente para ver se já está parado.

Nota: O servidor de directórios 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 servidor de directórios

O iSeries Navigator apresenta o estado do servidor de directórios na coluna **Estado** na estrutura da direita.

Para verificar o estado do servidor de directórios, 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 servidor de directórios, 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 servidor de directórios, 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 servidor de directórios sem perder o tempo adicional que é necessário para verificar o estado dos outros servidores de TCP/IP.

Verificar trabalhos no servidor de directórios de LDAP

Por vezes, pode querer monitorizar trabalhos específicos no servidor de directórios de LDAP. 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 **Directório** e seleccione **Trabalhos de Servidor**.

Activar a notificação de acontecimentos

Os Serviços de Directório suportam 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 o Apêndice C: Event Notification do manual IBM SecureWay Directory Version 3.2: Client SDK Programming Reference .

Especificar definições de transacção

Os Serviços de Directório suportam 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 40.

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, de modo que pode desejar fazer algumas experiências com definições diferentes.

Alterar a porta ou endereço de IP

O servidor de directórios de LDAP activado pelos Serviços de Directório utiliza as seguintes portas assumidas:
- 389 para ligações não protegidas.
- 636 para ligações protegidas (se tiver utilizado o Gestor de Certificados Digitais para activar os Serviços de Directório 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, poderá atribuir uma porta diferente aos Serviços de Directório ou utilizar endereços de IP diferentes para os dois servidores, se as aplicações suportarem a ligação a um endereço de IP específico.

Para obter um exemplo dos conflitos entre o servidor de LDAP do Domino e o servidor de LDAP dos Serviços de Directório do iSeries, consulte Domiciliar Domino LDAP e Serviços de Directório no mesmo iSeries

Para alterar as portas utilizadas pelo servidor de directórios de LDAP, 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 **Rede**.
6. Escreva os números das portas adequados e, em seguida, faça clique sobre **OK**.

Para alterar o endereço de IP em que o servidor de directórios 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.

Mover dados do directório de LDAP entre sistemas

O servidor de LDAP dos Serviços de Directório pode funcionar de modo independente de outros servidores. No entanto, pode ser útil se este funcionar com outros servidores. Isto pode incluir:
- “Importar um ficheiro de LDIF”
- “Exportar um ficheiro de LDIF”
- “Configurar uma nova réplica do servidor de directórios” na página 23
- “Publicar informações no servidor de directórios” na página 27

Importar um ficheiro de LDIF

Pode transferir informações entre diferentes servidores de directórios de LDAP utilizando ficheiros do Formato de Permuta de Dados de LDAP (LDIF). 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 servidor de directórios de LDAP, efectue os seguintes passos:
1. Se o servidor de directórios estiver iniciado, pare-o. Consulte “Parar o servidor de directórios de LDAP” na página 20 para obter informações sobre como parar o servidor de directórios.
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**.

Nota: Pode igualmente usar o utilitário ldapadd para importar ficheiros de LDIF.

Exportar um ficheiro de LDIF

Pode transferir informações entre diferentes servidores de directórios de LDAP utilizando ficheiros do Formato de Permuta de Dados (LDIF) de LDAP, consulte “Formato de troca de dados de LDAP” na página 36. Pode exportar a totalidade ou parte do directório de LDAP para um ficheiro de LDIF.

Para exportar um ficheiro de LDIF a partir do servidor de directórios, 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 uma localização para onde o ficheiro LDIF deve ser exportado, será guardado no directório assumido especificado no seu perfil de utilizador do OS/400. Se não o tiver alterado, o directório assumido é o directório raiz.

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 "Utilitário ldapsearch" na página 56. Utilize a opção -L e redireccione o output para um ficheiro.

Configurar uma nova réplica do servidor de directórios

Pode configurar réplicas do servidor de directórios de LDAP para servidores de directórios de outros servidores do iSeries. Os Serviços de Directório utilizam o protocolo standard de LDAP, versão 3, para efectuar a replicação.

Notas:

1. Não é possível fazer a replicação entre os servidores de LDAP, versão 3 e versão 2. Assim, o sistema para o qual efectuar a replicação tem de estar a utilizar a mesma versão do LDAP que o sistema a partir do qual efectua a replicação. As versões V4R3 e V4R4 do OS/400 suportam o LDAP versão 2. A versão V4R5 e posterior suporta o LDAP versão 3.
2. Pode replicar o directório dos Serviços de Directório para servidores IBM SecureWay V3.2 ou posteriores noutras plataformas. Para tal, o servidor de directórios do OS/400 tem de ser configurado de modo a utilizar o mecanismo 3.2 ACI. Se o servidor encontrar um problema quando estiver a tentar replicar, parará a replicação. Se isso acontecer, a sua réplica ficará incompleta.

Siga estes passos para configurar uma nova réplica do servidor de directórios:

1. Se ainda não o tiver feito, configure o servidor principal e o servidor de réplica.

   Nota: Certifique-se de que os esquemas e os sufixos correspondem em ambos os servidores.
2. Pare o servidor principal.
3. (opcional) Configure os dados de LDAP para a replicação inicial. Pode ignorar este passo se não tiver dados iniciais que pretenda transferir do servidor principal para o servidor de réplica.
4. (opcional) Mova os dados de LDAP para o servidor principal. Ignore este passo se uma das seguintes indicações se aplicar ao servidor de réplica:
   - É um novo servidor de directórios de LDAP.
   - Não contém dados que o utilizador pretenda manter.
5. Configurar o novo servidor de réplica.
6. Configurar o servidor principal para ter uma nova réplica.
7. Certifique-se de que o servidor principal está a permitir actualizações:
   a. No iSeries Navigator, expanda o sistema no qual está a ser executado o servidor de directórios principal.
   b. Expanda **Rede**.
   c. Expanda **Servidores**.
   d. Faça clique sobre **TCP/IP**.
   e. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
   f. Se ainda não estiver marcada, marque a opção **Permitir actualizações de directório**.

Nota: Estas instruções presumem que o servidor principal e os servidores de réplica estão nos sistemas que gere a partir do iSeries Navigator no mesmo PC. Se estiver a gerir os sistemas a partir de PCs separados, pode deslocar-se entre dois PCs para efectuar esta tarefa. Se estiver em execução um

servidor principal ou um servidor de réplica num sistema operativo IBM sem ser o OS/400, consulte a documentação referente a essa plataforma para configurar esse servidor.

Configurar dados de LDAP para replicação inicial

Pode ter dados que já existem no servidor de directórios principal de LDAP que pretende adicionar a um novo servidor de réplica. Para o fazer, terá de, em primeiro lugar, exportar o directório para um ficheiro de LDIF. Enquanto o ficheiro de LDIF está a ser exportado, terá de impedir que o servidor principal seja actualizado. Pode fazê-lo de uma das seguintes formas:

- Pare o servidor de directórios de LDAP. Dependendo da quantidade de dados existente no directório, esta operação poderá requerer que o servidor permaneça parado por um período de tempo alargado.
- Altere as propriedades do servidor, de modo a que não seja possível efectuar actualizações. Isto permite que o servidor continue a responder a pedidos de procura enquanto o ficheiro de LDIF está a ser exportado. Para escolher esta opção, siga estes passos:
  1. No iSeries Navigator, expanda o sistema no qual está a ser executado o servidor de directórios principal.
  2. Expanda **Rede**.
  3. Expanda **Servidores**.
  4. Faça clique sobre **TCP/IP**.
  5. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
  6. Se a opção **Permitir actualizações de directório** estiver marcada, desmarque-a. Isto impedirá actualizações ao directório até a replicação estar totalmente configurada.
  7. Faça clique sobre **OK**.
  8. Pare e, em seguida, reinicie o servidor de directórios de LDAP.

Depois de ter parado o servidor ou alterado as propriedades do mesmo para desautorizar as actualizações do directório, realize as seguintes tarefas:

1. Exporte o directório para um ficheiro de LDIF.
2. Transfira o ficheiro de LDIF para o sistema no qual o servidor de réplica será executado.

Após o ficheiro de LDIF ser transferido para o sistema no qual o servidor de réplica será executado, terá de importar os dados para o servidor de réplica:

1. No iSeries Navigator, expanda o sistema no qual está a ser executada a réplica do servidor de directórios.
2. Se o servidor de réplica ainda não estiver parado, pare-o agora. Actualize o estado dos servidores até o estado ser **Parado**.
3. Expanda **Rede**.
4. Expanda **Servidores**.
5. Faça clique sobre **TCP/IP**.
6. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
7. Se a opção **Permitir actualizações de directório** estiver desmarcada, marque-a. Isto permitirá que os dados sejam importados.
8. Faça clique sobre **OK**.
9. Importe o ficheiro de LDIF que transferiu no passo 2.
10. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
11. Desmarque a opção **Permitir actualizações de directório**.

Mover dados de LDAP para o servidor principal

Quando criar um servidor de directórios de LDAP para um servidor de réplica, deixará de poder actualizar os dados contidos nesse servidor. Se existirem dados no servidor que está a configurar para ser um servidor de directórios de LDAP de réplica, provavelmente pretenderá movê-los para o servidor principal para que seja possível continuar a respectiva manutenção. Para o fazer, siga estes passos:

1. No iSeries Navigator, expanda o sistema no qual está a ser executada a réplica do servidor de directórios.
2. Expanda **Rede**.
3. Expanda **Servidores**.
4. Faça clique sobre **TCP/IP**.

5. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
6. Se a opção **Permitir actualizações de directório** estiver marcada, desmarque-a. Isto impedirá actualizações ao directório até a replicação estar totalmente configurada.
7. Faça clique sobre **OK**.
8. Pare o servidor de directórios de LDAP.
9. Exporte o directório para um ficheiro de LDIF.
10. Transfira o ficheiro de LDIF para o sistema no qual o servidor principal será executado.

Após o ficheiro de LDIF ser transferido para o sistema no qual o servidor principal será executado, terá de importar os dados para o servidor principal:

1. No iSeries Navigator, expanda o sistema no qual está a ser executado o servidor de directórios principal.
2. Se o servidor de directórios principal ainda não estiver parado, pare-o agora. Actualize o estado dos servidores até o estado ser **Parado**.
3. Expanda **Rede**.
4. Expanda **Servidores**.
5. Faça clique sobre **TCP/IP**.
6. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
7. Se a opção **Permitir actualizações de directório** estiver desmarcada, marque-a. Isto permitirá que os dados sejam importados.
8. Faça clique sobre **OK**.
9. Importe o ficheiro de LDIF que transferiu no passo 10 do procedimento anterior.
10. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
11. Desmarque a opção **Permitir actualizações de directório**.

Configurar a nova réplica

Siga estes passos para configurar o novo servidor de réplica.

Nota: O servidor de réplica tem de estar configurado e parado para poder efectuar este procedimento.

1. No iSeries Navigator, expanda o sistema no qual está a ser executada a réplica do servidor de directórios.
2. Expanda **Rede**.
3. Expanda **Servidores**.
4. Faça clique sobre **TCP/IP**.
5. Se o servidor ainda não tiver sido parado, pare-o agora. Actualize o estado dos servidores até o estado ser **Parado**.
6. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
7. Faça clique sobre o separador **Replicação**.
8. Seleccione **Utilizar como um servidor de réplica**.
9. No campo **Nome utilizado pelo servidor principal para actualização**, seleccione um nome para o servidor principal a utilizar quando iniciar sessão no servidor de réplica quando efectuar actualizações. Este poderá ser um nome distinto (DN) ou um utilizador de Kerberos.

   Se seleccionar um DN:

   - Faça clique sobre o botão **Palavra-passe** a seguir ao campo **Nome utilizado pelo servidor principal para as actualizações**. Escreva uma palavra-passe para o servidor principal utilizar quando iniciar sessão no servidor de réplica para efectuar actualizações.

     Nota: Deve anotar esta palavra-passe e o nome que introduziu no passo 9. Irá necessitar desses elementos quando configurar o servidor principal para replicação.

   Se seleccionar **Adicionar utilizador de Kerberos** :

   - Ser-lhe-á pedido que introduza um nome de Kerberos (no formato `LDAP/`*`nome de sistema central`*, onde *nome de sistema central* é o nome de sistema central qualificado do servidor principal) e o domínio assumido (como, por exemplo, EMPRESA.COM) do servidor principal.

Nota: Para utilizar Kerberos, terá de ter o Kerberos activo tanto no servidor principal, como no de réplica.

10. No campo **URL do servidor principal**, introduza o nome do servidor principal em formato URL. Se o servidor principal utilizar uma porta diferente da assumida, introduza este número de porta como parte do URL.
11. Faça clique sobre o separador **Base de dados/Sufixos**. Se o sufixo que pretende replicar não estiver na lista, adicione-o.
12. (opcional) Se pretender utilizar o Secure Sockets Layer (SSL) durante a replicação, utilize o Gestor de Certificados Digitais para activar o SSL no servidor. Pode iniciar o Gestor de Certificados Digitais a partir do separador **Rede**. Para obter mais informações sobre a activação do SSL num servidor de directórios, consulte “Activar SSL no servidor de directórios de LDAP” na página 15.
13. Faça clique sobre **OK**.

Configurar o servidor principal para ter uma nova réplica

Siga estes passos de modo a configurar o servidor principal para ter uma nova réplica.

Nota: É necessário que tenha configurado e iniciado o servidor principal antes de executar este procedimento.

1. No iSeries Navigator, expanda o sistema no qual está a ser executado o servidor de directórios principal.
2. Expanda **Rede**.
3. Expanda **Servidores**.
4. Faça clique sobre **TCP/IP**.
5. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
6. Se ainda não estiver marcada, marque a opção **Permitir actualizações de directório**.
7. Faça clique sobre **OK**.
8. Pare e, em seguida, reinicie o servidor de directórios de LDAP. Actualize o estado dos servidores até ser **Iniciado**.
9. Faça novamente clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
10. Faça clique sobre o separador **Replicação**. O iSeries Navigator pode pedir-lhe para escrever informações de ligação. Escreva estas informações e, em seguida, faça clique sobre **OK**.
11. Faça clique sobre **Adicionar**.
12. No campo **Servidor**, introduza o nome do servidor principal em formato URL.
13. Seleccione o método de autenticação.

    Para utilizar um nome distinto (DN) e palavra-passe:

    a. Seleccione **Utilizar DN e palavra-passe**.

    b. No campo **Ligar como**, escreva o nome especificado no passo 9 na página 25 quando configurou o servidor de réplica.

    c. Faça clique sobre **Palavra-passe** e escreva a palavra-passe especificada no passo 9 na página 25 quando configurou o servidor de réplica.

    Para utilizar Kerberos:

    - Seleccione **Utilizar a conta de Kerberos dos servidores principais**. O servidor principal utilizará o respectivo Nome do director de Kerberos para proceder à autenticação.

      Nota: Para utilizar o Kerberos, terá de ter o Kerberos activo tanto no servidor principal como no de réplica.

14. Se pretender utilizar o Secure Sockets Layer (SSL) durante a replicação, utilize o Gestor de Certificados Digitais para activar o SSL no servidor. Pode iniciar o Gestor de Certificados Digitais a partir do separador **Rede**. Para obter mais informações sobre a activação do SSL num servidor de directórios, consulte “Activar SSL no servidor de directórios de LDAP” na página 15.
15. Se o servidor de réplica não utilizar a porta assumida, especifique o número da porta no campo **Porta**.

16. Se não pretender actualizar o servidor de réplica cada vez que for alterada uma entrada no servidor principal, seleccione **Hora**. Em seguida, especifique com que frequência pretende que o servidor principal actualize a réplica.
17. Faça clique sobre **OK**.
18. Faça clique sobre o separador **Base de dados/Sufixos**. Se o sufixo que pretende replicar não estiver na lista, adicione-o.
19. Active actualizações de directório em cada servidor de réplica:
    a. No iSeries Navigator, expanda o sistema no qual está a ser executada a réplica do servidor de directórios.
    b. Expanda **Rede**.
    c. Expanda **Servidores**.
    d. Faça clique sobre **TCP/IP**.
    e. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Propriedades**.
    f. Se a opção **Permitir actualizações de directório** estiver desmarcada, marque-a.
    g. Faça clique sobre **OK**.
20. Se ainda não estiverem iniciados todos os servidores de réplica inicie-os agora.

Nota: Um servidor não pode ser um servidor principal e um servidor de réplica.

Publicar informações no servidor de directórios

Pode configurar o sistema de modo a publicar certas informações num servidor de directórios de LDAP no mesmo ou noutro sistema. O OS/400 publicará automaticamente estas informações no servidor de directórios de LDAP quando utilizar 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 Qualidade do serviço de TCP/IP. Para obter mais informações sobre a Qualidade do serviço, consulte a secção Configuração de LDAP e QoS .

Se o DN ascendente no qual os dados estão a ser publicados não existir, os Serviços de Directório criá-lo-ão automaticamente. Também poderá ter instaladas outras aplicações de OS/400 que publiquem informações num directório de LDAP. Adicionalmente, pode chamar interfaces de programação de aplicações (APIs) dos seus próprios programas para publicar outros tipos de informações no directório de LDAP.

Notas:

1. Quando configurar o OS/400 para publicar informações do tipo Utilizadores no servidor de directórios de LDAP, este exportará automaticamente entradas do directório de distribuição do sistema para o servidor de LDAP. Utiliza a interface de programação de aplicações (API) QGLDSSDD para fazê-lo. Isto 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 o tópico OS/400 Directory Services em Programming, no iSeries Information Center. As informações disponíveis incluem:
   - Como chamar manualmente esta API.
   - Como impedir que utilizadores específicos sejam exportados para o servidor de LDAP.
   - Como exportar os campos de directório de distribuição de sistema.
2. Quando configurar o OS/400 para publicar informações do tipo Sistema para o servidor de directórios de LDAP e seleccionar uma ou mais impressoras para publicar, o sistema manterá automaticamente o directório de LDAP sincronizado com as alterações efectuadas a essas impressoras no sistema. As informações sobre impressoras que podem ser publicadas incluem a localização das impressoras, a velocidade em páginas por minuto, se suportam a impressão em dúplex e a cores, o tipo e modelo e a 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.
3. Também pode publicar informações do OS/400 num servidor de directórios de LDAP que não esteja num OS/400, se configurar esse servidor para utilizar o esquema da IBM.

Para configurar o sistema de modo a publicar automaticamente informações sobre o OS/400 num servidor de directórios de LDAP, 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 **Serviços de Directório**.
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 **Servidor de Directórios (Activo)**. Na caixa de diálogo apresentada, introduza o nome do servidor de directórios de LDAP onde deseja publicar as informações sobre o OS/400 e, em seguida, faça clique sobre **OK**.
8. No campo **Abaixo de DN**, introduza o nome distinto ascendente (DN) onde pretende adicionar informações no servidor de directórios.
9. Preencha os campos na estrutura **Ligação do servidor** adequados para a sua configuração.

   Nota: Para publicar informações sobre o OS/400 para o servidor de directórios utilizando SSL ou Kerberos, primeiro tem de ter um servidor de directórios configurado para utilizar o protocolo adequado. Consulte “Utilizar a autenticação de Kerberos com o servidor de directórios de LDAP” na página 42 para obter informações sobre SSL e Kerberos.
10. Se o servidor de directórios não utilizar a porta assumida, escreva o número da porta correcta 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 OS/400 num servidor de directórios de LDAP que se encontre numa plataforma diferente. Tem de publicar as informações do utilizador e do sistema num servidor de directórios que utilize um esquema compatível com o esquema do Serviços de Directório. As definições de esquema de IBM SecureWay Directory, que incluem os iSeries Serviços de Directório, podem ser encontradas na página da Web dos Serviços de Directório.

Tem de publicar as partilhas de impressão num servidor de directórios que suporte o esquema do Active Directory da Microsoft. A publicação de partilhas de impressão num Active Directory permite aos utilizadores configurar impressoras do iSeries directamente a partir do respectivo ambiente de trabalho de Windows 2000 através do assistente Adicionar Impressora do Windows 2000. Para o fazer com o assistente Adicionar Impressora, especifique que deseja encontrar uma impressora no Active Directory do Windows 2000.

APIs para publicar informações sobre o OS/400 no servidor de directórios

Os Serviços de Directório fornecem suporte incorporado para publicação de informações do utilizador e do sistema. Estes itens estão listados na página **Serviços de Directório** 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 informação aparecem também na página **Serviços de Directório**. Tal como os utilizadores e os sistemas, estão desactivados inicialmente, e podem ser configurados utilizando o mesmo procedimento. O

programa que adiciona dados ao directório de LDAP é designado agente de publicação. O tipo de informação que é publicado, tal como aparece na página **Serviços de Directório**, é designado por nome do agente.

As APIs que se seguem permitem-lhe 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 ir para a página de propriedades dos Serviços de Directório de modo a configurar o agente de publicação. Exemplos de nomes de agente são os nomes de agente dos sistemas e utilizadores que estão disponíveis automaticamente na página **Serviços de Directório**.

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.

Especificar um servidor para consultas de directório

Para atribuir servidores de referência ao servidor de directórios, 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, em seguida, seleccione **Propriedades**.
5. Faça clique sobre **Adicionar**.
6. No pedido de informação, especifique o nome do servidor de referência em 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 consulta não utilizar a porta assumida, especifique o número de porta correcto como parte do URL, tal como a porta 400 está especificada no segundo exemplo anterior.
7. Faça clique sobre **OK**.

Adicionar sufixos ao servidor de directórios de LDAP

O facto de adicionar um sufixo ao servidor de directórios de LDAP 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 `e=ibm, p=po` for um sufixo no servidor, não poderá adicionar `uo=rochester, e=ibm, p=po`.

Para adicionar um sufixo ao servidor de directórios, 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.

Remover sufixos do servidor de directórios

Para remover um sufixo do servidor de directórios de LDAP, efectue 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** 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 servidor de directórios. No entanto, poderá posteriormente readquirir o acesso aos dados adicionando de novo o sufixo.

Guardar e restaurar informações dos Serviços de Directório

Os Serviços de Directório guardam informações nas seguintes localizações:

- Biblioteca de bases de dados (QUSRDIRDB por valor assumido), que inclui o conteúdo dos servidores de directórios.
- 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 servidor de directórios 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 o manual Cópia de Segurança e Recuperação, SC17-5326  para obter informações sobre como guardar e restaurar dados do OS/400.

Gerir a propriedade e o acesso a dados de directório

A gestão de propriedade e o acesso a dados de directório inclui as seguintes tarefas:
- “Trabalhar com as propriedades de objectos de directório”
- “Trabalhar com listas de controlo de acesso (ACLs)” na página 31
- “Trabalhar com Grupos de ACLs” na página 31

Trabalhar com as propriedades de objectos de directório

Para definir as características de propriedade de objectos de directório, efectue 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** e seleccione **Autoridade**.

   Se não estiver já ligado ao servidor de directórios, é apresentada a caixa de diálogo **Estabelecer Ligação ao Servidor de Directórios**. Estabeleça a ligação como administrador do servidor ou como proprietário do objecto que tem as propriedades com as quais pretende trabalhar.
5. Na árvore de directórios, seleccione o objecto que tenha as propriedades com as quais pretende trabalhar e, em seguida, faça clique sobre **OK**.

Trabalhar com listas de controlo de acesso (ACLs)

Trabalhar com listas de controlo de acesso (ACLs) inclui atribuir ACLs explícitas e implícitas a objectos de directórios, adicionar utilizadores a ACLs, remover utilizadores de ACLs e procurar objectos de directórios. Note que, a partir da V5R1, os Serviços de Directório suportam um novo modelo de ACLs, de modo que, mesmo que tenha utilizado ACLs anteriormente, poderá considerar útil voltar a familiarizar-se com as mesmas.

Para trabalhar com ACLs, efectue 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** e seleccione **Autoridade**.

   Se não estiver já ligado ao servidor de directórios, é apresentada a caixa de diálogo **Estabelecer Ligação ao Servidor de Directórios**. Estabeleça a ligação como administrador do servidor ou como proprietário do objecto com a ACL com a qual pretende trabalhar.
5. Seleccione, na árvore de directórios, o objecto que tenha a ACL com a qual pretende trabalhar e, em seguida, faça clique sobre **OK**.
6. Faça clique sobre o separador **ACL**.

Trabalhar com Grupos de ACLs

Para trabalhar com grupos de ACLs, efectue os seguintes procedimentos:
1. No iSeries Navigator, seleccione **Rede**.
2. Seleccione **Servidores**.
3. Faça clique sobre **TCP/IP**.
4. Faça clique com o botão direito do rato sobre **Directório** e seleccione **Grupos de ACL**.

Trabalhar com o acesso administrativo para utilizadores autorizados

A partir da V5R2, é possível conceder aos administradores acesso a perfis de utilizador aos quais foi concedido acesso ao identificador de função (ID) Administrador dos Serviços de Directório (QIBM_DIRSRV_ADMIN).

Por exemplo, se for concedido ao perfil de utilizador JOAOSILVA acesso ao ID da função Administrador dos Serviços de Directório e a opção Conceder acesso de administrador a utilizadores autorizados estiver seleccionada na caixa de diálogo Propriedade de directório, o perfil de utilizador JOAOSILVA terá a autoridade de administrador de LDAP. Quando este perfil é utilizado para ligar ao servidor de directórios utilizando o DN que se segue, os400-profile=JOAOSILVA,nc=contas,os400-sys=sistemaA.empresa.com, o utilizador terá 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 a secção “Programa origem projectado pelo sistema operativo” na página 43.

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 dos Serviços de Directório 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 dos Serviços de Directório** 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**.

Registar 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 do directório de LDAP para manter o controlo das alterações ao directório. O registo de alterações está localizado no sufixo especial `nc=changelog`. 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 **Base de dados/Sufixos**.
6. Seleccione **Alterações no directório de registo**.
7. (opcional) Em **Entradas máximas** especifique o número máximo de entradas a serem mantidas pelo registo de alterações.

   Nota: Apesar deste parâmetro ser opcional, deverá considerar seriamente especificar um número máximo de entradas. Se não especificar um número máximo de entradas, o registo de alterações irá registar todas as entradas e tornar-se demasiado extenso.

A classe de objectos `changeLogEntry` é utilizada para representar as alterações aplicadas ao servidor de directórios. 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 esteja na Lista de Controlo de Acesso para o sufixo `nc=changelog` pode fazer uma procura das entradas do registo de alterações. Execute procuras apenas no sufixo do registo de alterações `nc=changelog`. Não tente adicionar, alterar ou eliminar no sufixo do registo de alterações, mesmo que tenha autoridade para o fazer. Esta acção terá resultados inesperados.

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 nc=admininistrator -w password -b nc=changelog  (changetype=*)
```

Activar a auditoria de objectos para o servidor de directórios

Os Serviços de Directório suportam a auditoria de segurança do 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 os Serviços de Directório:
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 servidor de directórios de LDAP. Para obter mais informações, consulte a secção “Segurança dos Serviços de Directório” na página 41.

Ajustar o rendimento do servidor de directórios de LDAP

Pode ajustar o rendimento do servidor de directórios de LDAP alterando um dos seguintes elementos:
- O tamanho das procuras.
- O tempo máximo permitido para procuras
- As definições de transacção do servidor
- Número de ligações de base de dados e módulos do servidor

Para ajustar os valores de rendimento do servidor de directórios, 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 **Rendimento**.

Pode também ajustar o rendimento do servidor de directórios 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**.

Capítulo 5. Conceitos e informações de consulta dos Serviços de Directório

As informações sobre conceitos e de consulta que se seguem ajudá-lo-ão a compreender e a executar o servidor de LDAP dos Serviços de Directório:

- "Listas de controlo de acesso (ACLs) de LDAP"
- "Formato de troca de dados de LDAP" na página 36
- "Considerações sobre o suporte de idioma nacional (NLS)" na página 39
- "Propriedade de objectos do directório de LDAP" na página 39
- "Consultas do directório de LDAP" na página 39
- "Transacções" na página 40
- "Servidores de directórios de LDAP de réplica" na página 40
- "Segurança dos Serviços de Directório" na página 41
- "Programa origem projectado pelo sistema operativo" na página 43
- "Serviços de Directório e o suporte de registo em diário do OS/400" na página 49

Para obter informações sobre os princípios básicos de LDAP e planear o servidor de LDAP, consulte também o Capítulo 3, "Como começar com os Serviços de Directório" na página 7.

Listas de controlo de acesso (ACLs) de LDAP

Em muitos casos, provavelmente não gostaria de limitar o acesso a dados existentes no servidor de directórios de LDAP. Por exemplo, um servidor de LDAP existente na Intranet da empresa poderia conter uma lista telefónica dos empregados da empresa. É provável que gostasse que todos os empregados pudessem ver os dados desta lista telefónica.

No entanto, imagine que o presidente da empresa não quer que todos os empregados tenham acesso ao seu número de telefone. Nesse caso, poderia criar uma **lista de controlo de acesso (ACL)**. Com esta ACL, poderia limitar o acesso a essa entrada do servidor apenas aos empregados cujas chamadas o presidente estivesse interessado em receber.

Com as ACLs, pode controlar os utilizadores que têm autoridade para adicionar e eliminar objectos de directório. Pode igualmente especificar se os utilizadores podem ou não ler, escrever, procurar e comparar atributos de directório. As ACLs podem ser herdadas ou explícitas. Ou seja, pode utilizar ACLs de uma das seguintes formas:

- Configurar explicitamente uma ACL para um objecto específico.
- Especificar que os objectos herdam ACLs de objectos que se encontrem em níveis superiores da hierarquia de directórios de LDAP.

Talvez o presidente do exemplo anterior não pretendesse que todos os empregados tivessem acesso ao seu número de telefone. No entanto, gostaria que todos os gestores lhe pudessem ter acesso. Nesse caso, poderia utilizar um **Grupo de ACL** para simplificar a concessão de autoridade aos gestores. Os grupos de ACL permitem-lhe conceder acesso a grupos específicos de utilizadores em vez de conceder autoridade individualmente. Isto é particularmente útil se o mesmo grupo de pessoas necessitar de ter acesso a mais do que um conjunto de objectos. Se, por exemplo, os mesmos gestores que tinham acesso ao número de telefone do presidente necessitassem, mais tarde, de aceder a entradas relativas a salários, poderia reutilizar o grupo de ACL.

Modelos de ACL

Todas as versões dos Serviços de Directório suportam um modelo de permissões de nível de classe de acesso. Neste modelo, cada tipo de atributo de LDAP tem uma classificação de ″Normal″, ″Sensível″ ou ″Crítica″. São os ficheiros esquemas de atributos que controlam estas classificações. Ao adicionar um utilizador a uma ACL de objectos, especifica as classificações que o utilizador pode ler, escrever, procurar

e comparar. Na maior parte dos esquemas, o número de telefone seria classificado como um atributo ″Normal″. Deste modo, para permitir o acesso dos gestores do exemplo anterior ao número de telefone do presidente, atribuir-lhes-ia acesso de leitura aos atributos ″Normal″ do objecto lista telefónica do presidente. Continuariam a não ter acesso a informações ″Sensíveis″ e ″Críticas″. Todas as versões dos Serviços de Directório suportam a definição de permissões de nível de classe de acesso.

Os Serviços de Directório também suportam o modelo de permissões de nível de atributo. Neste modelo, poderá especificar as autoridades de leitura, escrita, pesquisa e comparação para atributos específicos, independentemente da sua classe de acesso. Considere novamente o exemplo anterior. No modelo de permissões de nível de atributo, poderia atribuir aos gestores acesso de leitura para o atributo `númerotelefone`, mesmo que eles, normalmente, não tenham acesso aos atributos ″Normais″.

O modelo de permissão de nível de atributo só é compatível com servidores de Serviços de Directório SecureWay versão 3.2 e superiores. Por valor assumido, não está activado. Tem a possibilidade de o activar quando trabalha com ACLs. Depois de activado, o modelo só poderá ser desactivado através da reconfiguração do servidor e do restauro da base de dados do directório. Antes de se decidir a activar este modelo, lembre-se de que não o poderá administrar a partir de qualquer cliente LDAP V2 (incluindo as versões pré-V5R1 do iSeries Navigator) e que tentar fazê-lo poderá danificar as entradas da ACL.

Valores especiais da ACL

Inicialmente, todos os objectos do servidor de directórios dos Serviços de Directório têm uma ACL que contém um grupo de ACL especial, `NC=Qualquer`, que inclui todos os utilizadores do directório. Por valor assumido, este grupo tem acesso de leitura, procura e comparação aos atributos de classe normal de todos os objectos.

Pode desejar que alguns objectos tenham as mesmas permissões de acesso para todos os utilizadores ligados ao servidor de directórios através de uma ligação que não seja anónima. Para o fazer, utilize o grupo especial de listas de controlo de acesso (ACL) `nc=Authenticated`.

Para especificar quais as permissões de acesso que um objecto pode ter, utilize o DN especial `nc=this`. Isto permite que as entradas descendentes que herdem as suas ACLs sejam autorizadas automaticamente a efectuar operações nos respectivos objectos.

Informações adicionais

Para administrar ACLs através do iSeries Navigator, não necessita de saber os detalhes sobre o modo como os Serviços de Directório implementam as ACLs. No entanto, se pretender especificar atributos relacionados com ACLs quando utilizar ficheiros de LDIF ou pretender utilizar ACLs com os utilitários de linha de comandos de LDAP, terá de se familiarizar com os atributos utilizados pelas ACLs. Para obter informações sobre atributos de ACL, consulte o documento de referência Listas de Controlo de Acesso da documentação A Ferramenta de Gestão de Directórios IBM SecureWay.

Para obter informações sobre como configurar e alterar ACLs e grupos de ACL, siga estas ligações:
“Trabalhar com listas de controlo de acesso (ACLs)” na página 31
“Trabalhar com Grupos de ACLs” na página 31

Formato de troca de dados de LDAP

O formato de troca de dados de LDAP (LDIF) fornece-lhe uma forma simples de transferir informações de directório entre servidores de directórios de LDAP. Os ficheiros de LDIF guardam entradas do directório de LDAP num formato de texto simples. O formato dos ficheiros de LDIF utilizados pelo servidor de directórios foi alterado ligeiramente, a partir da V4R5 dos Serviços de Directório. Os ficheiros de LDIF são constituídos por uma sequência de linhas que descreve uma entrada de directório ou um conjunto de alterações feitas numa entrada de directório. Não pode descrever ambas.

O formato geral de uma entrada de LDIF é o seguinte:

```
version: 1
dn: nome distinto
attrtype1: valoratrib1
...
```

em que:

- *versão* mostra a versão do formato do ficheiro de LDIF. O número da versão tem de ser 1. Se o número da versão estiver ausente, o ficheiro de LDIF é considerado como estando num formato de ficheiro de LDIF mais antigo. Quando o ficheiro de LDIF tem a versão 1, o conteúdo TEM de ser em código UTF-8.
- *nome distinto* é o nome distinto da entrada de directório
- *attrtype1* é um tipo de atributo de LDAP (como, por exemplo, nc ou uo)
- *valoratrib1* é o valor do atributo

Cada entrada pode ter vários atributos. Cada atributo aparece numa linha em separado. Se o valor de um atributo ocupar mais do que uma linha, pode continuar na linha seguinte e é precedido de um espaço em branco ou de uma tabulação.

As linhas em branco separam múltiplas entradas do mesmo ficheiro de LDIF. Todas as linhas que comecem com um cardinal (#) são linhas de comentário e têm de ser ignoradas durante a análise de um ficheiro de LDIF.

Qualquer nome distinto ou valor de atributo que satisfaça uma das seguintes condições deve ser codificado em base64:

- Contém retornos de linha ou mudanças de linha.
- Começa por dois pontos (:), ESPAÇO ou sinal de menor que (<).
- Termina com um espaço.

Os atributos codificados em base64 são designados através da utilização de um sinal de dois pontos entre o nome de atributo e o valor.

As referências externas estão no ficheiro:// formato URL. Deverão existir sinais de dois pontos e menor que (:<) entre o tipo de atributo e o valor de referência externo.

Eis alguns exemplos de ficheiros de LDIF:

Exemplo 1: Um ficheiro de LDAP simples com duas entradas

```
versão: 1
   dn: nc=Bárbara Jorge, uo=Porto, e=Grande Empresa, p=PO
   objectclass: topo
   objectclass: pessoa
   objectclass: organizationalPerson
   cn: Bárbara Jorge
   cn: Bárbara J Jorge
   cn: Babs Jorge
   sn: Jorge
   uid: bjorge
   númerotelefone: +351 21 855 1212
   descrição: Uma grande adepta da vela.

   dn: nc=Bernardo Jorge, uo=Porto, e=Grande Empresa, p=PO
   objectclass: topo
   objectclass: pessoa
   objectclass: organizationalPerson
   cn: Bernardo Jorge
   sn: Jorge
```

```
   númerotelefone: +351 21 855 1212
   descrição:Babs é uma grande adepta da vela e viaja bastante por mar
   à procura de condições perfeitas para velejar.
   cargo:Gestor de Produto, Divisão Audiovisual
```

Exemplo 2: Um ficheiro que contém um valor codificado em base64

```
versão: 1
   dn: nc=Guilherme Jorge, uo=Porto, e=Grande Empresa, p=PO
   objectclass: topo
   objectclass: pessoa
   objectclass: organizationalPerson
   cn: Guilherme Jorge
   cn: Guilherme Jorge
   sn: Jorge
   uid: gernj
   númerotelefone: +351 21 855 1212
   descrição:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Exemplo 3: Um ficheiro que contém uma série de registos de alterações e comentários

Nota: Os ficheiros de LDIF com registos de alterações não podem ser importados directamente para o servidor. Contudo, são suportados pelas funções de interface de LDAP.

```
versão: 1
   # Adicionar uma nova entrada
   dn: nc=Filipa Jorge, uo=Porto, e=Grande Empresa, p=PO
   alterartipo: adicionar
   objectclass: topo
   objectclass: pessoa
   objectclass: organizationalPerson
   cn: Filipa Jorge
   ap: Jorge
   uid: filipa
   númerotelefone: +351 21 855 1212
   jpegphoto:< ficheiro:///usr/local/directory/photos/filipa.jpg

   # Eliminar uma entrada existente
   dn: nc=Ricardo Jorge, uo=Porto, e=Grande Empresa, p=PO
   alterartipo: eliminar

   # Modificar um nome distinto relativo de uma entrada
   dn: nc=Paulo Jorge, uo=Porto, e=Grande Empresa, p=PO
   alterartipo: modrdn
   newrdn: nc=Paula Jorge
   deleteoldrdn: 1
```

A ordem das entradas no ficheiro de LDIF é importante. Para adicionar com êxito uma entrada que seja especificada no ficheiro de LDIF a um directório de LDAP, primeiro, a respectiva entrada ascendente tem de existir no espaço de nome do directório. No exemplo anterior, não seria possível adicionar a segunda nem a terceira entradas se a primeira entrada não existisse.

Igualmente, para importar um ficheiro de LDIF para um servidor que suporta certos sufixos, o ficheiro de LDIF tem de ter entradas para aqueles sufixos. Por exemplo, se o seu servidor tivesse o sufixo `uo=Porto, e=Grande Empresa, p=PO`, o ficheiro de LDIF mostrado acima podia ser importado. Mas, se no entanto, o servidor tivesse o sufixo `e=Grande Empresa, p=PO`, teria de ter uma entrada para esse sufixo especificado em primeiro lugar no ficheiro de LDIF, como é mostrado a seguir:

```
dn: e=Grande Empresa, p=PO
classe de objecto: organização
o: Grande Empresa
```

O formato específico e o conteúdo dos ficheiros de LDIF são determinados pelo esquema do servidor a partir do qual são exportados. Pode importar um ficheiro de LDIF para qualquer servidor de LDAP que utilize o esquema idêntico como o servidor a partir do qual o ficheiro foi exportado. Servidores de LDAP de fornecedores diferentes utilizam um esquema diferente (com classes e atributos de objecto diferentes). Deste modo, pode não conseguir importar para um servidor um ficheiro de LDIF que tenha sido criado por outro servidor.

Também está disponível um Pedido de Comentário (RFC) sobre especificações de ficheiro LDIF no seguinte URL:

http://www.ietf.org/rfc/rfc2849.txt 

Procedimentos relacionados:

“Importar um ficheiro de LDIF” na página 22
“Exportar um ficheiro de LDIF” na página 22

Considerações sobre o suporte de idioma nacional (NLS)

A partir da V4R5, tanto o servidor de LDAP dos Serviços de Directório do OS/400, como o cliente de LDAP dos Serviços de Directório do OS/400 se baseiam no LDAP Versão 3. Tenha em atenção as seguintes considerações de NLS:

- Os dados são transferidos entre os servidores e clientes de LDAP no formato UTF-8. São permitidos todos os caracteres ISO 10646.
- O servidor de LDAP dos Serviços de Directório utiliza o método de definição 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 o UCS-2, consulte o tópico Globalization em Planning, no iSeries Information Center.

Propriedade de objectos do directório de LDAP

Cada objecto no seu 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 superiores na hierarquia de directórios de LDAP.

Os Serviços de Directório permitem-lhe 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=this` na lista de proprietários de objectos. Por exemplo, suponha que o objecto `nc=A` tem o proprietário `nc=this`. Qualquer utilizador terá acesso de proprietário ao objecto `nc=A` se este se ligar ao servidor como `nc=A`.

Procedimento relacionado:

“Trabalhar com as propriedades de objectos de directório” na página 30

Consultas do directório de LDAP

As consultas permitem que os servidores de directório de LDAP funcionem em equipas. Se o DN pedido por um cliente não estiver num directório, o servidor pode enviar (consultar) automaticamente o pedido para qualquer outro servidor de LDAP.

Os Serviços de Directório permitem-lhe utilizar tipos de referências diferentes. Pode especificar servidores de referência assumidos, onde o servidor de LDAP refere clientes sempre que cada DN não se encontra no directório. Também pode utilizar o seu cliente de LDAP para adicionar entradas ao servidor de directórios que tenham a consulta objectClass. Isto permite-lhe especificar consultas baseadas nesse DN específico pedido por um DN.

Nota: Com os Serviços de Directório, os objectos de referência têm de conter apenas um nome distinto (`dn`), uma classe de Objecto (`objectClass`) e um atributo de referência (`ref`). Consulte o “Utilitário ldapsearch” na página 56 para ver um exemplo que ilustra esta restrição.

Os servidores de consulta estão intimamente relacionados com os servidores de réplicas. Uma vez que não é possível os clientes alterarem dados dos servidores de réplicas, a réplica envia todos os pedidos para alterar dados do directório para o servidor principal.

Transacções

Pode configurar o servidor de directórios de LDAP do sistema para permitir aos clientes utilizar transacções. 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 teria de reiniciar a transacção, em vez de ter de verificar quais as entradas que tinham sido eliminadas com sucesso.

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

- adicionar
- modificar
- modificar RDN
- eliminar

Nota: Não inclua as alterações ao esquema do directório (o sufixo nc=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 servidor de directórios.

Para obter informações adicionais sobre transacções, consulte o apêndice Limited Transaction Support do manual IBM SecureWay Directory Client SDK Programming Reference .

Servidores de directórios de LDAP de réplica

As informações armazenadas em servidores de directórios de LDAP de réplica são idênticas às informações do servidor de directórios de LDAP principal. Existem duas vantagens principais em ter uma ou mais réplicas do directório de LDAP:

- As réplicas tornam mais rápidas as procuras no directório. Em vez de ter todos os pedidos de procura directa dos clientes num único servidor principal, pode dividir os pedidos entre o servidor principal e os servidores de réplica.
- As réplicas constituem uma cópia de segurança do servidor principal. Se o servidor principal não estiver disponível, uma réplica pode responder aos pedidos de procura e fornecer o acesso a dados do directório.

Os servidores de réplica são só de leitura. Quando um utilizador autorizado tenta alterar uma entrada de um servidor de réplica, este envia o pedido para o servidor de directórios principal.

Procedimento relacionado:

"Configurar uma nova réplica do servidor de directórios" na página 23

Segurança dos Serviços de Directório

Auditoria de segurança

A partir da V5R1, os Serviços de Directório suportam a auditoria de segurança do OS/400. Os itens passíveis de auditoria incluem:

- Ligações e separações do servidor de directórios.
- 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 suas definições de auditoria doOS/400 antes de 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 a auditoria, consulte *Security - Reference*  ou o tópico Security auditing no iSeries Information Center.

Autenticação e segurança da ligação

Os Serviços de Directório fornecem os seguintes mecanismos que poderá utilizar para melhorar a segurança das comunicações entre os clientes de LDAP e o servidor de directórios de LDAP:

- Ligações de Secure Sockets Layer (SSL)
- Autenticação de Kerberos
- Encriptação de palavras-passe CRAM-MD5

Utilizar Secure Sockets Layer (SSL) e Translation Layer Security com o servidor de directórios de LDAP

Para tornar as comunicações com o servidor de directórios de LDAP mais protegidas, o Serviços de Directório pode utilizar a segurança do Secure Sockets Layer (SSL).

Para utilizar o SSL com o Serviços de Directório, tem de ter um dos produtos do Fornecedor de Acesso Criptográfico (5722-ACx) instalado no sistema. Se pretende utilizar o SSL de iSeries Navigator, terá de ter instalado no seu PC um dos produtos de Codificação do Cliente (5722-CEx). Necessitará deste software se pretender efectuar o seguinte:

- Configurar e administrar o Serviços de Directório a partir da estação de trabalho utilizando uma ligação com SSL. Isto inclui tarefas que pode efectuar a partir do iSeries Navigator.
- Para utilizar uma ligação de SSL com aplicações criadas por si com interfaces de programação de aplicações (APIs) de cliente do Windows.

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), opção 34 do OS/400, instalado no sistema. O DCM fornece-lhe uma interface para criar e gerir certificados digitais e arquivos de certificados.

Consulte a documentação sobre o Gestor de Certificados Digitais para obter informações sobre os certificados digitais e sobre como utilizar o DCM. Para obter informações sobre o SSL no iSeries, consulte Proteger as aplicações com o SSL. Para obter informações sobre TLS no servidor iSeries, consulte Protocolos SSL e Transport Layer Security (TLS) suportados.

Utilizar a autenticação de Kerberos com o servidor de directórios de LDAP

Os Serviços de Directório permitem-lhe configurar o servidor de directórios de LDAP para 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 Fornecedor de Acesso Criptográfico (5722AC2 ou 5722AC3) instalado no sistema. Também terá de ter configurado um serviço de autenticação de rede.

O suporte Kerberos dos Serviços de Directório fornece suporte ao mecanismo GSSAPI SASL. Este facto permite que tanto os clientes de LDAP do SecureWay como do Windows 2000 utilizem a autenticação de Kerberos com o servidor de directórios de LDAP.

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

`nome de serviço/nome do sistema central@domínio`

`nome de serviço` é o LDAP, `nome do sistema central` é o nome de TCP/IP totalmente qualificado do sistema e `domínio` é o domínio assumido especificado na configuração de Kerberos do sistema.

Por exemplo, para um sistema denominado `o meu as400` no domínio de TCP/IP `empresa.com`, com um domínio de Kerberos assumido `EMPRESA.COM`, o nome principal do servidor de LDAP Kerberos será `LDAP/o 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). Por convenção, os nomes de domínio Kerberos utilizam apenas maiúsculas e os nomes de sistema central apenas minúsculas. LDAP/ tem de estar em maiúsculas. O servidor de directórios não pode ser configurado para utilizar a autenticação de Kerberos se o domínio assumido não tiver sido configurado.

Quando a autenticação de Kerberos for utilizada, o servidor de directórios de LDAP associa um nome distinto (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=principal@domínio″. ibm-kn= é equivalente a ibm-kerberosName=.
- O servidor poderá procurar no directório um nome distinto (DN) que contenha uma entrada do principal e domínio Kerberos. Quando seleccionar esta opção, o servidor pesquisará o directório procurando uma entrada que especifique esta identidade Kerberos da seguinte forma:
  - O servidor procura um objectokrbRealm-V2 no directório que tem um atributo krbRealmName-V2 que corresponde ao domínio de Kerberos. Se encontrar esta entrada, irá procurar nos DNs que estão especificados no atributo princSubtree uma entrada com o atributo krbPrincipalName que corresponda ao nome do director e ao nome do domínio.Se o DN configurado em krbAliasedObjectName contém o DN da entrada anteriormente encontrada, será utilizado o DN configurado em krbAliasedObjectName. Caso contrário, será utilizado o DN da entrada. Este método é normalmente utilizado quando um KDC de Kerberos está a guardar as informações principais de Kerberos no directório de LDAP.
  - Se a procura descrita anteriormente falhar, o servidor procurará uma entrada de directório que utilize a classe auxiliar ibm-securityIdentities e que tenha um valor de atributo altSecurityIdentities

KERBEROS:director@domínio. Este método pode ser utilizado para associar identidades Kerberos com as entradas de directório quando o KDC não estiver a guardar directores no directório.

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

Programa origem projectado pelo sistema operativo

O programa origem projectado pelo sistema operativo tem capacidade para definir objectos do OS/400 como entradas na árvore de directórios acessível por LDAP. Os objectos projectados são representações de LDAP de objectos do OS/400 em vez de entradas reais armazenadas na base de dados do servidor de LDAP. Com a V5R2, os perfis de utilizador do OS/400 são os únicos objectos que são definidos ou projectados como entradas na árvore de directórios. A definição de objectos perfis de utilizador é referida como programa origem projectado pelo utilizador do OS/400.

As operações de LDAP são definidas como os objectos subjacentes do OS/400 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 informações mais detalhadas sobre o programa origem projectado pelo sistema operativo,consulte o seguinte:

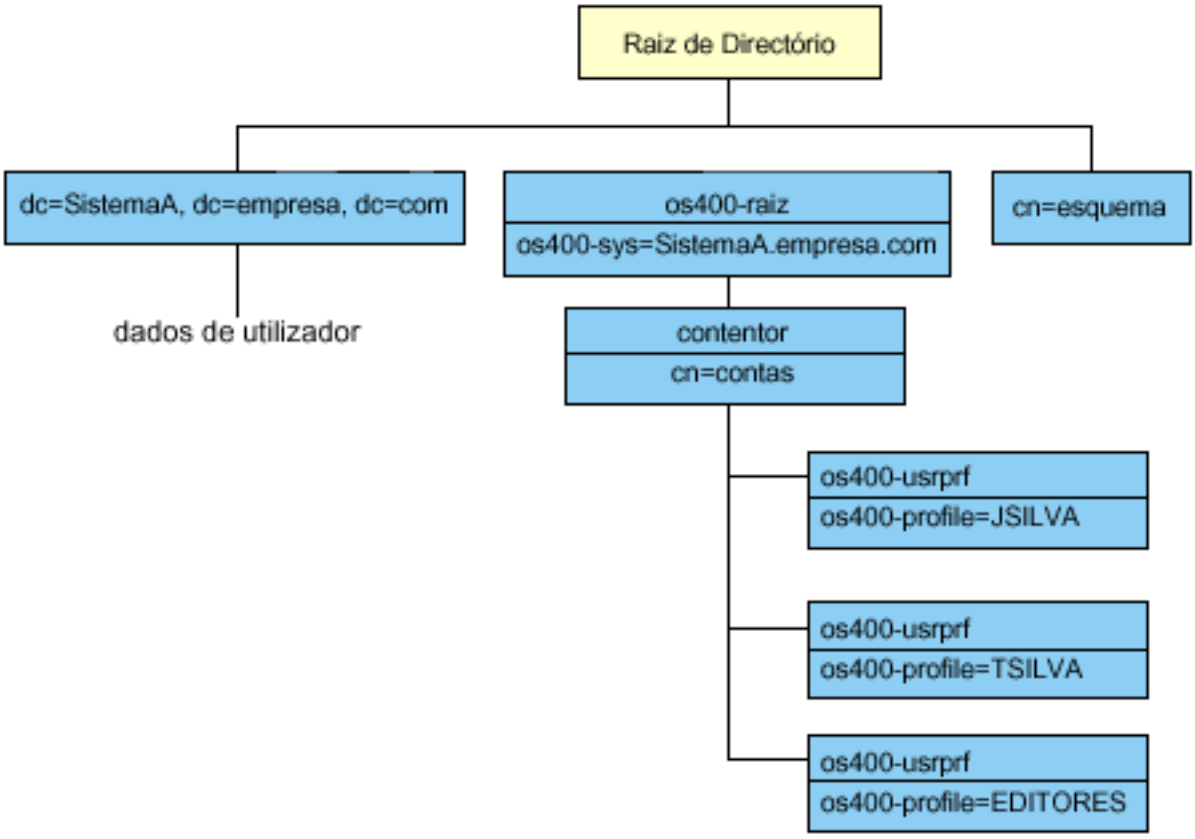
- “Árvore de informações de directório projectadas pelo utilizador do OS/400”
- “Operações de LDAP” na página 44
- “DNs do administrador e de ligação de réplicas” na página 48
- “Esquema projectado pelo utilizador do OS/400” na página 49

Árvore de informações de directório projectadas pelo utilizador do OS/400

A figura que se segue mostra uma árvore de informações de directório (DIT) exemplo para o programa origem projectado pelo utilizador. A figura mostra perfis de grupo e individuais. 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 deLDAP. O sufixo nc=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 ou eliminada, poderá reconfigurar o sufixo dos objectos do sistema. No entanto, terá de se certificar de que o sufixo actual não está a ser utilizado nas ACLs ou noutro lado do sistema em que seria necessário modificar entradas caso o sufixo tivesse de ser alterado.

Na figura anterior, o contentor, nc=contas, é mostrado abaixo da raiz. Este objecto não pode ser modificado. É colocado um contentor neste nível em antecipação a outros tipos de informações ou objectos que poderão ser projectados pelo sistema operativo no futuro. Abaixo do contentor nc=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,nc=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 ao (autenticar o) servidor de LDAP utilizando o perfil de utilizador projectado. Para tal, especifique o nome distinto (DN) do perfil de utilizador projectado (DN) para o DN da ligação e a palavra-passe correcta do perfil de utilizador do OS/400 para autenticação. Um exemplo de um DN utilizado num pedido de ligação seria `os400-profile=jsilva,nc=contas,os400-sys=sistemaA.empresa.com`.

Um cliente tem de ligar como um utilizador projectado a informações de acesso no programa origem projectado pelo sistema. 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 que é permitido quando é especificado um perfil de utilizador projectado num pedido de ligação.

Procura

O programa origem projectado pelo 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 programa origem projectado pelo sistema para operações de procura.

Tabela 1. Comportamento do programa origem projectado pelo 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 no filtro especificados. Os atributos de código incorporado e os respectivos valores são devolvidos para o sufixo de objecto do sistema e para o contentor sob o mesmo.
Devolver todos os perfis de utilizador.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	os400-gid=0	Só são devolvidos os valores de nome distinto (DN), objectclass e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_ TO_PERFORM.

Tabela 1. Comportamento do programa origem projectado pelo sistema para operações de procura (continuação)

Procura pedida	Base da procura	Âmbito da procura	Filtro de procura	Comentários
Devolver todos os perfis de grupo.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	(!(os400-gid=0))	Só são devolvidos os valores de nome distinto (DN), objectclass 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.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	os400-profile=*	Só são devolvidos os valores de nome distinto (DN), objectclass 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.	nc=contas, os400-sys= SistemaA.empresa.com	um 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, nc=contas, os400-sys= SistemaA.empresa.com	bas, sub ou um	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.
Devolver todos os perfis de utilizador e de grupo começados por A.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	os400-profile=A*	Só são devolvidos os valores de nome distinto (DN), objectclass e os400-profile para perfis de utilizador projectados. Se for especificado qualquer outro filtro, será devolvido LDAP_UNWILLING_ TO_PERFORM.

Tabela 1. Comportamento do programa origem projectado pelo sistema para operações de procura (continuação)

Procura pedida	Base da procura	Âmbito da procura	Filtro de procura	Comentários
Devolver todos os perfis de grupo começados por G.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	(&(!(os400-gid=0)) (os400-profile=G*))	Só são devolvidos os valores de nome distinto (DN), objectclass 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.	nc=contas, os400-sys= SistemaA.empresa.com	um ou sub	(&(os400-gid=0) (os400-profile=A*))	Só são devolvidos os valores de nome distinto (DN), objectclass 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

  Segue-se o valor de controlo:
  - 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:

    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 aos 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 programa origem projectado 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 Servidor de Directórios (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 31.

Esquema projectado pelo utilizador do OS/400

Poderá encontrar as classes e atributos de objecto do programa origem projectado no esquema de servidor abrangente. Os nomes dos atributos de LDAP encontram-se no formato `os400–nnn`, em que *nnn* é, normalmente, a palavra-chave do atributo (como CRTUSRPRF ou CHGUSRPRF) nos comandos do perfil de utilizador. Consulte a secção “Árvore de informações de directório projectadas pelo utilizador do OS/400” na página 43 para obter mais informações.

Serviços de Directório e o suporte de registo em diário do OS/400

Os Serviços de Directório utilizam o suporte de base de dados do OS/400 para armazenar informações de directório. Os Serviços de Directório utilizam o controlo de consolidações para arquivar entradas de directório na base de dados. Isto requer o suporte de registo em diário do OS/400.

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 que configurou. O receptor de diário QSQJRN0001 é criado inicialmente na biblioteca de base de dados que configurou.

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 de comandos para a criação de 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 pretender manter receptores antigos, execute o seguinte comando numa linha de comandos do OS/400:

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

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

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

Para obter informações sobre os comandos de registo em diário, consulte o tópico OS/400 commands em Programming, no iSeries Information Center.

Capítulo 6. Utilitários de linha de comandos de LDAP

Os Serviços de Directório incluem cinco utilitários que lhe permitem efectuar acções no servidor de directórios de LDAP a partir do Ambiente de comandos Qshell no OS/400. Estes utilitários utilizam as APIs de LDAP. Pode utilizar estes utilitários a partir da linha de comandos qsh ou chamá-los a partir dos programas. Podem ser igualmente úteis como exemplos de programação. Quando instalar o cliente de LDAP do Windows que está incluído nos Serviços de Directório, também instalará um código que é muito semelhante ao código origem dos utilitários de interface.

Seguem-se os utilitários:
- "Utilitários ldapmodify e ldapadd", que adiciona e altera entradas do directório de LDAP.
- "Utilitário ldapdelete" na página 54, que remove entradas do directório de LDAP.
- "Utilitário ldapsearch" na página 56, que procura entradas no directório de LDAP.
- "Utilitário ldapmodrdn" na página 61, que modifica o Nome Distinto Relativo (RDN) de entradas do directório de LDAP.

Consulte "Notas sobre a utilização de SSL com os utilitários de linha de comandos de LDAP" na página 63 para obter informações sobre a utilização do SSL com os utilitários de linha de comandos.

Utilitários ldapmodify e ldapadd

O utilitário ldapmodify permite-lhe alterar ou adicionar entradas ao servidor de directórios de LDAP a partir da interface de comandos QSH no sistema. Utiliza as interfaces de programação de aplicações (APIs) ldap_modify, ldap_add e ldap_delete. O utilitário ldapadd funciona de forma idêntica ao utilitário ldapmodify, com a excepção de que o sinalizador -a é ligado automaticamente.

Formato:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd* **] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn* **] [-w** *passwd***] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

Nota: Se não fornecer informações de entrada a partir do *ficheiro* utilizando a opção **-f**, o utilitário irá aguardar até ler entradas de input standard. Para deixar de aguardar, prima a tecla SysReq e, em seguida, seleccione `2. Terminar pedido anterior`.

Diagnóstico:

Se não ocorrerem erros, o estado de saída será 0. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro standard.

Faça clique aqui para ver exemplos de utilização destes utilitários.

Parâmetros:

-V	Especifica a versão de LDAP utilizada pelo utilitário para ligar ao servidor de LDAP. Por valor assumido, utiliza uma ligação V3 LDAP. Para seleccionar explicitamente o LDAP V3, especifique -V 3. Especifique -V 2 para o executar como uma aplicação de LDAP V2.

-a	Este parâmetro só é utilizado pelo utilitário ldapmodify. Indica que o utilitário adicionará entradas por valor assumido em vez de as modificar. Utilizar este parâmetro produz os mesmos efeitos que utilizar o ldapadd.
-b	Assume que todos os valores começados por uma`/' são binários e que o valor real se encontra num ficheiro cujo caminho é especificado no local em que os valores aparecem normalmente.
-c	Modo de funcionamento contínuo. Os erros são comunicados, mas o ldapmodify ou o ldapadd continua a proceder a modificações ou adições. O valor assumido é sair depois de comunicar um erro.
-r	Substituir os valores existentes pelos valores assumidos.
-M	Gerir objectos de referência como entradas normais.
-n	Mostrar o procedimento que seria efectuado mas, na realidade, não modificar as entradas. É útil para depurar em conjunto com a opção -v.
-v	Utilize o modo verboso, com muitos diagnósticos escritos no output standard.
-F	Forçar a aplicação de todas as alterações independentemente do conteúdo das linhas de input começadas por réplica: (por valor assumido, réplica: as linhas são comparadas em relação ao sistema central e à porta do servidor de LDAP que em utilização para decidir se se deverá aplicar um registo de replicação).
-R	Especifica que as consultas não devem ser seguidas automaticamente.
-C *charset*	Especifica que as cadeias fornecidas como input ao utilitário estão representadas num conjunto de caracteres local (*charset*) e têm de ser convertidas para UTF-8. Utilize a opção charset -C se a página de códigos das cadeias de input for diferente do valor da página de códigos de trabalhos. Consulte a documentação para a API ldap_set_iconv_local_charset() para ver os valores *charset* .
-d *debuglevel*	Define o nível de depuração *debuglevel*.
-D *binddn*	Utilize *binddn* para ligar ao directório de LDAP. A opção *binddn* deve ser um DN representado por uma cadeia.
-w *passwd*	Utilize *passwd* como a palavra-passe de autenticação.
-m *mechanism*	Utilize *mechanism* para especificar o mecanismo SASL que o cliente utiliza para se ligar ao servidor. O cliente utiliza a API ldap_sasl_bind_s(). Os mecanismos disponíveis incluem o CRAM-MD5 (codifica palavras-passe), EXTERNAL (utilizado com o SSL) e o GSSAPI (Kerberos). O comando ignora o parâmetro **-m** se estiver definido **-V 2**. Se **-m** não for especificado, será utilizada a autenticação simples.
-O*hopcount*	Especifique *hopcount* para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá utilizar durante a procura de sistemas de referência. A contagem de sistemas de passagem assumida é 10.
-h *ldaphost*	Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.
-p *ldapport*	Especifique uma porta alternativa para o Transmission Control Protocol (TCP) em que o servidor de LDAP esteja a aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado e a opção **-Z** tiver sido especificada, será utilizada a porta 636 de SSL de LDAP.
-f *file*	Leia as informações sobre a modificação de entradas de um ficheiro de LDIF, em vez do input standard. Se um ficheiro de LDIF não for especificado, tem de utilizar input standard para especificar os registos de actualização em formato LDIF.
-Z	Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. A opção **-Z** só é suportada por versões desta ferramenta activadas através do SSL.

-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, utilizará um conjunto de raízes de autoridade de certificados fidedignos assumidos de código incorporado. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (CAs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas. Este parâmetros activa efectivamente o parâmetro/comutador **-Z** .
-P *keyfilepw*	Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é necessária para aceder a informações codificadas no ficheiro da base de dados de chaves (incluindo a chave privada). Se um ficheiro para esconder a palavra-passe for associado ao ficheiro de base de dados de chaves, a palavra-passe é obtida a partir do ficheiro para esconder e este parâmetro deixa de ser necessário. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-N *certificatename*	Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Tenha em atenção que se o servidor de LDAP estiver configurado para efectuar 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 do Servidor, será necessário um certificado do cliente. O parâmetro *certificatename* não será necessário se um certificado/par de chaves privado assumido tiverem sido designados 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. Ele é ignorado se nem **-Z** nem **-K** forem especificados.

Formato de Input Alternativo:

O utilitário ldapmodify suporta um formato de input alternativo para manter a compatibilidade com as versões mais antigas do utilitário. Este formato é composto por uma ou mais entradas separadas por linhas em branco. Cada entrada tem o seguinte formato:

```
Nome Distinto (DN)
attr=value
[attr=value ...]
```

em que *attr* é o nome do atributo e *value* é o valor. Por valor assumido, são adicionados valores. Se utilizar o sinalizador **-r** de linhas de comandos, o valor assumido irá substituir os valores existentes pelo valor novo. Tenha em atenção que é possível que um determinado atributo seja apresentado mais do que uma vez (por exemplo, pode adicionar mais do que um valor a um atributo). Note também que pode utilizar uma barra final invertida (\) para continuar valores entre linhas e preservar novas linhas no valor em si. Para remover um valor, antes do valor *attr* escreva um traço (-). O sinal de igual (=) e o valor devem ser omitidos para remover um atributo na sua totalidade. Antes de *attr*, deverá ser incluído um sinal de mais (+) para que seja adicionado um valor na presença do sinalizador **-r**.

Exemplos: ldapmodify e ldapadd

Exemplo 1:

Se o ficheiro **/tmp/entrymods** existir e tiver o seguinte conteúdo:

```
dn: nc=Modificar Utilizador, e=Universidade de Estudos Superiores, p=PO
alterar tipo: modificar
substituir: correio electrónico
correio electrónico: modutil@estudante.de.arte.edu
-
adicionar: título
título: Grande Mestre
-
adicionar: jpegPhoto
```

```
jpegPhoto:< ficheiro:///tmp/modme.jpeg
-
eliminar: descrição
-
```

O comando `ldapmodify -b -r -f /tmp/entrymods` irá:

- Substituir o conteúdo do atributo de correio das entradas Modificar utilizador pelo valor`modutile@estudante.de.arte.edu`.
- Adicionar o título `Grande Mestre`.
- Adicionar o conteúdo do ficheiro **/tmp/modme.jpeg** como jpegPhoto.
- Remover completamente o atributo de `descrição`.

Pode efectuar as modificações indicadas anteriormente com o formato de input ldapmodify antigo:

```
nc=Modificar Utilizador, e=Universidade de Estudos Superiores, p=PO
correio electrónico=modutil@estudante.de.arte.edu
+título=Grande Mestre
+jpegPhoto=/tmp/modme.jpeg
-descrição
```

O comando para utilizar o formato antigo seria:

```
ldapmodify -b -r -f /tmp/entrymods
```

Exemplo 2:

Parta do princípio de que o ficheiro **/tmp/newentry** existe e tem o seguinte conteúdo:

```
dn: nc=Joaquim Dias, e=Universidade de Estudos Superiores, p=PO
classe do objecto: pessoa
nc: Joaquim Dias
nc: Quim
ap: Dias
cargo: Gestor
correio electrónico: joaquimdias@estudante.de.arte.edu
UID: jdias
```

O comando `ldapadd -f /tmp/entrymods` irá adicionar uma nova entrada a Joaquim Dias, utilizando os valores do ficheiro /tmp/newentry.

Exemplo 3:

Se o ficheiro **/tmp/newentry** existir e tiver o conteúdo:

```
dn: nc=Joaquim Dias, e=Universidade de Estudos Superiores, p=PO
alterartipo: eliminar
```

O comando `ldapmodify -f /tmp/entrymods` removerá a entrada relativa a Joaquim Dias.

Utilitário ldapdelete

O utilitário ldapdelete permite-lhe eliminar uma ou mais entradas de um servidor de directórios de LDAP. É executado através da interface de comandos QSH no OS/400. Utiliza a interface de programação de aplicações (API) ldap_delete.

Formato:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C charset] [-d *debuglevel***] [-f** *file***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]** [*dn*]...

Nota: Se não fornecer argumentos de *dn*, o comando ldapdelete espera para ler uma lista de DNs do input standard. Para deixar de aguardar, prima a tecla SysReq e, em seguida, seleccione `2. Terminar pedido anterior.`

Diagnóstico:

Se não ocorrerem erros, o estado de saída será 0. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro standard.

Faça clique aqui para ver exemplos da utilização do utilitário ldapdelete.

Parâmetros:

-V	Especifica a versão de LDAP utilizada pelo utilitário para ligar ao servidor de LDAP. Por valor assumido, utiliza uma ligação V3 LDAP. Para seleccionar explicitamente LDAP V3, especifique V 3. Especifique -V 2 para executar como uma aplicação LDAP V2.
-M	Gerir objectos de referência como entradas normais.
-n	Mostre o procedimento que seria efectuado, mas não elimine realmente entradas. É útil para depurar em conjunto com a opção **-v**.
-v	Utilize o modo verbose, com muitos diagnósticos escritos no output standard.
-c	Modo de funcionamento contínuo. Os erros são comunicados, mas ldapdelete continuará com as eliminações. O valor assumido é sair depois de comunicar um erro.
-R	Especifica que as consultas não devem ser seguidas automaticamente.
-C *charset*	Especifica que os nomes distintos (DNs) fornecidos como input ao utilitário estão representados num conjunto de caracteres local (*charset*). Utilize **-C** *charset* para substituir o valor assumido, onde as cadeias têm de ser fornecidas em UTF-8. Utilize a opção **-C** charset se a página de códigos das cadeias de input for diferente do valor da página de códigos de trabalhos. Consulte a documentação para a API ldap_set_iconv_local_charset() para ver os valores *charset*.
-d *debuglevel*	Define o nível de depuração *debuglevel*.
-f *file*	Leia uma série de linhas de *file*, efectuando uma eliminação de LDAP para cada linha do ficheiro. Cada linha do ficheiro deve conter um único nome distinto (DN).
-D *binddn*	Utilize *binddn* para ligar ao directório de LDAP. A opção *binddn* deve ser um DN representado por uma cadeia.
-w *passwd*	Utilize *passwd* como a palavra-passe para autenticação.
-m *mechanism*	Utilize *mechanism* e especifique o mecanismo SASL para ser utilizado para estabelecer uma ligação com o servidor. Será utilizada a API ldap_sasl_bind_s(). Os mecanismos disponíveis incluem o CRAM-MD5 (codifica palavras-passe), EXTERNAL (utilizado com o SSL) e o GSSAPI (Kerberos). O parâmetro -m será ignorado se -V 2 for definido. Se **-m** não for especificado, é utilizada a autenticação simples.
-O *hopcount*	Especifique *hopcount* para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar durante a procura de sistemas de referência. A contagem de sistemas de passagem assumida é 10.
-h *ldaphost*	Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.
-p *ldapport*	Especifique uma porta alternativa para o Transmission Control Protocol (TCP) em que o servidor de LDAP esteja a aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado e a opção **-Z** tiver sido especificada, será utilizada a porta 636 de SSL de LDAP.
-Z	Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. A opção **-Z** só é suportada por versões desta ferramenta activadas através do SSL.

-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 e 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 (CAs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas. Este parâmetro activa efectivamente o parâmetro/comutador **-Z**.
-P *keyfilepw*	Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é necessária para aceder a informações codificadas no ficheiro da base de dados de chaves (incluindo a chave privada). Se um ficheiro para esconder a palavra-passe for associado ao ficheiro de base de dados de chaves, a palavra-passe é obtida a partir do ficheiro para esconder e este parâmetro deixa de ser necessário. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-N *certificatename*	Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Tenha em atenção que se o servidor de LDAP estiver configurado para efectuar 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 do Servidor, será necessário um certificado do cliente. O parâmetro *certificatename* não será necessário se tiver sido designado um par assumido de certificado/chave privada como 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. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
dn	Especifica um ou mais argumentos de *dn*. Cada *dn* deve ser um DN representado por uma cadeia.

Exemplo: ldapdelete

O comando que se segue tentará eliminar a entrada designada com o nomecomum ″Eliminar Utilizador″ directamente abaixo da entrada da empresa Universidade de Arte:

```
ldapdelete nc=Eliminar Utilizador, e=Universidade de Arte, p=PO
```

Pode ser necessário aplicar *binddn* e uma *palavra-passe* (consulte as opções **-D** e **-w**).

Utilitário ldapsearch

O utilitário ldapsearch permite-lhe procurar uma entrada no servidor de directórios de LDAP a partir da interface de comandos QSH no OS/400. Utiliza a interface de programação de aplicações (API) ldap_search.

A procura utiliza um filtro que está em conformidade com a representação de cadeias de filtros de LDAP. Para obter mais informações sobre filtros de procura de LDAP, consulte as informações sobre a API ldap_search no tópico OS/400 Directory Services em Programming, no iSeries Information Center.

Se o utilitário ldapsearch localizar uma ou mais entradas, obterá os atributos especificados por *attrs* e imprime as entradas e os valores em output standard. Se não listar quaisquer atributos, o utilitário devolverá todos os atributos.

Formato:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *charset***] [-d** *debuglevel***] [-F** *sep***] [-f** *file***] [-D** *binddn***] [-w** *bindpasswd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-b** *searchbase***] [-s** *scope* **] [-a** *deref***] [-l** *time limit***] [-z** *size limit***]** *filter* **[***attrs...***]**

Diagnóstico:

Se não ocorrerem erros, o estado de saída será 0. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro standard.

Formato de Output:

Se o ldapsearch localizar uma ou mais entradas, escreverá todas as entradas no output standard no formato:

```
Nome Distinto (DN)
nome do atributo=valor
nome do atributo=valor
nome do atributo=valor
...
```

Múltiplas entradas são separadas por uma linha em branco simples. Se utilizar a opção **-F** para especificar um carácter separador, o output apresenta esse carácter em vez do carácter de igual (=). Se utilizar a opção **-t**, o nome de um ficheiro temporário substituirá o valor real. Se especificar a opção **-A**, só será escrita a parte relativa ao `nome do atributo`.

Faça clique aqui para ver exemplos da utilização do utilitário ldapsearch.

Parâmetros:

-V	Especifica a versão de LDAP utilizada pelo utilitário para ligar ao servidor de LDAP. Por valor assumido, utiliza uma ligação V3 LDAP. Para seleccionar explicitamente o LDAP V3, especifique -V 3. Especifique -V 2 para o executar como uma aplicação de LDAP V2.
-n	Mostre o procedimento que seria efectuado mas, na realidade, não execute a procura. É útil para depurar em conjunto com a opção **-v**.
-v	Utilize o modo verboso, com muitos diagnósticos escritos no output standard.
-t	Escreva valores obtidos num conjunto de ficheiros temporários. Isto é útil para processar valores binários como, por exemplo, jpegPhoto ou áudio.
-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	Não anule a apresentação de valores binários. Isto é útil para processar valores que aparecem em conjuntos de caracteres alternativos como, por exemplo, o ISO-8859.1. Esta opção é ocasionada pela opção **-L**
-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	Gerir objectos de referência como entradas normais.
-R	Especifica que as consultas não devem ser seguidas automaticamente.
-C *charset*	Especifica que as cadeias fornecidas como input ao utilitário ldapsearch estão representadas num conjunto de caracteres local (*charset*). O input de cadeias inclui o filtro, o DN associado e o DN de base. De modo semelhante, quando está a apresentar os dados, o ldapsearch converterá os dados recebidos do servidor de LDAP para os caracteres especificados. Utilize a opção **-C** de conjunto de caracteres se a página de códigos das cadeias de input for diferente do valor da página de códigos do trabalho. Consulte a documentação para a API ldap_set_iconv_local_charset() para ver os valores *charset*. Além disso, se as opções -C e -L estiverem especificadas, é presumido que o input está no conjunto de caracteres especificado, mas o output de ldapsearch está sempre preservado na respectiva representação em UTF-8 ou numa representação de código base64 dos dados, quando são detectados caracteres não imprimíveis. É este o caso, desde que que os ficheiros de LDIF standard apenas contêm representações em UTF-8 (UTF-8 de código base64) dos dados de cadeias.

-d *debuglevel*	Define o nível de depuração *debuglevel*.
-F *sep*	Utilize *sep*como o separador de campos entre os nomes do atributo e os valores. O separador assumido é `=, a menos que tenha sido especificado o sinalizador **-L**, caso em que esta opção é ignorada.
-f *file*	Leia um conjunto de linhas do ficheiro, efectuando uma procura de LDAP em cada linha do ficheiro. Cada linha do ficheiro deve conter um único nome distinto (DN).
-D *binddn*	Utilize *binddn* para ligar ao directório de LDAP. A opção *binddn* deve ser um DN representado por uma cadeia.
-w *passwd*	Utilize *passwd* como a palavra-passe de autenticação.
-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(). Os mecanismos disponíveis incluem o CRAM-MD5 (codifica palavras-passe), EXTERNAL (utilizado com o SSL) e o GSSAPI (Kerberos). O parâmetro **-m** será ignorado se **-V** 2 for definido. Se **-m** não for especificado, é utilizada a autenticação simples.
-O *hopcount*	Especifique *hopcount* para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar durante a procura de sistemas de referência. A contagem de sistemas de passagem assumida é 10.
-h *ldaphost*	Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.
-p *ldapport*	Especifique uma porta alternativa para o Transmission Control Protocol (TCP) em que o servidor de LDAP esteja a aguardar uma resposta. A porta de LDAP assumida é a 389. Se não for especificado e a opção **-Z** tiver sido especificada, será utilizada a porta 636 do Secure Sockets Layer (SSL) de LDAP.
-Z	Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. A opção **-Z** só é suportada por versões desta ferramenta activadas através do SSL.
-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, utilizará um conjunto de raízes de autoridade de certificados fidedignos assumidos de código incorporado. O ficheiro da base de dados de chaves contém normalmente um ou mais certificados de autoridades de certificação (CAs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas. Este parâmetros activa efectivamente o parâmetro/comutador **-Z** .
-P *keyfilepw*	Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é necessária para aceder a informações codificadas no ficheiro da base de dados de chaves (incluindo a chave privada). Se um ficheiro para esconder a palavra-passe for associado ao ficheiro de base de dados de chaves, a palavra-passe é obtida a partir do ficheiro para esconder e este parâmetro deixa de ser necessário. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-N *certificatename*	Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Tenha em atenção que se o servidor de LDAP estiver configurado para efectuar 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 do Servidor, será necessário um certificado do 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. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-b *searchbase*	Utilize a opção *searchbase* como ponto de partida para a procura em vez de utilizar o valor assumido. Se **-b** não for especificado, este utilitário irá examinar a variável do ambiente LDAP_BASEDN para uma definição de *searchbase* .

-s *scope*	Especifique o âmbito da procura. A opção *scope* deve ser `base`, `um` ou `sub` para especificar um procura num objecto base, num nível ou na sub-árvore. O valor assumido é `sub`.
-a *deref*	Especifique o modo como será feita a anulação de referências de nomes alternativos. A opção *deref* deve ser nunca, sempre, procurar ou localizar para especificar que a referência a nomes alternativos nunca seja anulada, seja sempre anulada, seja anulada quando procurar ou só seja anulada quando localizar o objecto base da procura. O valor assumido é nunca anular a referência a nomes alternativos.
-l *timelimit*	Aguardar no máximo *timelimit* segundos a conclusão de uma procura.
-z *sizelimit*	Limitar os resultados da procura a no máximo entradas com *sizelimit.* Isto possibilita a colocação de um limite superior ao número de entradas que são devolvidas para uma operação de procura.
filter	Especifica o nome do filtro utilizado pela procura.
attrs...	Especifica os atributos que o utilitário recupera se a procura encontrar uma ou mais entradas. Se não listar quaisquer valores de *attrs*, o utilitário devolverá todos os atributos.

Exemplos: ldapsearch

Exemplo 1:

O comando `ldapsearch nc=joaquim dias cn Númerotelefone` executa uma procura de sub-árvore (utilizando a base de procura assumida) relativamente a entradas com um nome Comum `joaquim dias`. A procura obtém os valores de nome Comum e os valores de número de telefone e imprime-os no output standard. Se a procura localizar duas entradas, o output assemelhar-se-á a:

```
nc=Joaquim E Dias, uo=Universidade de Literatura, Ciências e Artes,
uo=Estudantes, uo=Pessoas, e=Universidade de Estudos Superiores, p=PO
nc=Joaquim Dias
nc=Joaquim Eduardo Dias
nc=Joaquim E Dias 1
nc=Joaquim E Dias
número de Telefone=+1 313 555-5432

nc=Joaquim B Dias, uo=Departamento de Tecnologia de Informações,
uo=Sector e Pessoal,
uo=Pessoas, e=Universidade de Estudos Superiores, p=PO
nc=Joaquim Dias
nc=Joaquim B Dias 1
nc=Joaquim B Dias
número de telefone=+1 313 555-1111
```

Exemplo 2:

O comando `ldapsearch -t uid=jed jpegPhoto audio` executa uma procura de sub-árvore utilizando a base de procura assumida relativamente a entradas com o ID de utilizador jed. A procura obtém os valores de jpegPhoto e de audio e escreve-os em ficheiros temporários. Se a procura localizar uma entrada com um valor para cada um dos atributos pedidos, o output assemelhar-se-á a:

```
nc=Joaquim E Dias,
uo=Departamento de Tecnologia de Informações,
uo=Sector e Pessoal,
uo=Pessoas, e=Universidade de Estudos Superiores, p=PO
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Exemplo 3:

O comando `ldapsearch -L -s one -b p=PO e=university* o description` executa uma procura de um nível no nível `p=PO`. Esta procura pesquisa todas as empresas cujo nome de Organização comece por `universidade`. A procura apresenta os seus resultados no formato de LDIF. Obtém o valor do atributo nome de Organização e os valores do atributo de descrição e imprime-os no output standard que se assemelha a:

```
dn:
e=Universidade de Viseu, p=PO
e: Universidade de Viseu
descrição: Preparar Viseu para os desafios do amanhã
descrição: apenas nó de folhas

dn: e=Universidade de Lisboa em Faro, p=PO
e: Universidade de Lisboa em Faro
descrição: Não existem informações sobre o pessoal
descrição: Instituição de educação e pesquisa

dn: e=Universidade de Lisboa em Faro, p=PO
e: Universidade de Lisboa em Faro
e: ULF
e: UL/Faro
e: CU-Faro
descrição: Instituto de Estudos Superiores e Pesquisa

dn: e=Universidade de Évora, p=PO
e: Universidade de Évora
o: UEl
descrição: Orientador de mentes jovens
...
```

Exemplo 4:

Como foi explicado no “Consultas do directório de LDAP” na página 39, os directórios de LDAP do Serviços de Directório podem conter objectos de consulta, desde que só contenham o seguinte:

- Um nome distinto (`dn`).
- Uma classe de objectos (`objectClass`).
- Um atributo de consulta (`ref`).

Este exemplo apresenta procuras em que está envolvido um objecto de consulta.

Assuma que o Sistema_A contém a entrada de consulta:

```
dn: nc=Bárbara Jorge, uo=Porto, e=Empresa Principal, p=PO
ref: ldap://Sistema_B:389/nc=Bárbara Jorge,
  uo=Porto, e=Empresa Principal, p=PO classe de objectos: consulta
```

Todos os atributos associados à entrada deverão residir no Sistema_B.

O Sistema_B contém uma entrada:

```
dn: nc=Bárbara Jorge, uo=Porto, e=Empresa Principal, p=PO
nc: Bárbara Jorge
classe de objectos: organizationalPerson
ap: Jorge
número de telefone: (800) 555 1212
```

Quando um cliente emite um pedido ao Sistema_A e não envia o controlomanageDsaIT, o servidor devolve uma consulta. Por exemplo, utilizando-M em ldapsearch, o servidor de LDAP no Sistema_A responde ao cliente com o seguinte URL:

```
ldap://Sistema_B:389/nc=Bárbara Jorge,
  uo=Porto, e=Empresa Principal, p=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 ignora estes atributos.

Quando um cliente receber uma resposta de consulta de um servidor, enviará o pedido de novo, desta vez para o servidor ao qual se refere o URL devolvido. Se a procura tiver sido executada com um âmbito de um nível, o pedido de consulta utilizará o âmbito base. Os resultados desta procura variam dependendo do valor que especificar para o âmbito da procura (**-b**).

Se especificar `-s sub`, como neste exemplo:

```
ldapsearch -h Sistema_A -b uo=Rochester, e=Empresa Principal, p=PO
     -s sub sn=Jorge
```

a procura devolverá todos os atributos relativos a todas as entradas com sn=Jorge que residam em ou abaixo de `uo=Rochester, e=Empresa Principal, p=PO` tanto no Sistema_A como no Sistema_B. O cliente recebe uma consulta do Sistema_A e pesquisa o Sistema_B, devolvendo `nc=Barb Jorge,uo=Rochester,e=Empresa Principal,p=PO`.

Se especificar `-s one`, como neste exemplo:

```
ldapsearch -h Sistema_A -b uo=Rochester, e=Empresa Principal, p=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/nc=Bárbara Jorge,
  uo=Rochester, e=Empresa Principal, p=PO??base
```

Por sua vez, o cliente submete um pedido:

```
 ldapsearch -h Sistema_B -b nc=Barb Jorge, uo=Rochester, e=Empresa Principal, p=PO
     -s base sn=Jorge
```

Este devolve a entrada `nc=Barb Jorge,uo=Rochester,e=Empresa Principal,p=PO`.

Utilitário ldapmodrdn

O utilitário ldapmodrdn permite-lhe alterar o Nome Distinto Relativo (RDN) de entradas do servidor de directórios de LDAP. Utilize-o a partir da interface de comandos QSH no OS/400. Utiliza a interface de programação de aplicações (API) ldap_modrdn.

Formato:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-f** *file* **] [***dn rdn***]**

Notas:

1. Se utilizar os argumentos de comando-linha *dn* e *rdn*, o *rdn* substituirá o RDN da entrada que é especificada pelo DN, *dn*. Caso contrário, o conteúdo do ficheiro (ou do input standard se não utilizar o sinalizador **-f**) deve ser composto por uma ou mais entradas.

   ```
   Nome Distinto (DN)

   Nome Distinto Relativo (RDN)
   ```

   Uma ou mais linhas em branco separam os pares DN/RDN.
2. Se não fornecer informações de entrada de *file* utilizando a opção **-f** (ou do par comando-linha *dn* e *rdn*), o comando ldapmodrdn aguardará para ler as entradas do input standard. Para deixar de aguardar, prima a tecla SysReq e, em seguida, seleccione `2. Terminar pedido anterior`.

Diagnóstico:

Se não ocorrerem erros, o estado de saída será 0. Os erros resultam num estado de saída diferente de zero e no envio de uma mensagem de diagnóstico para o erro standard.

Faça clique aqui para ver um exemplo da utilização do utilitário ldapmodrdn.

Parâmetros:

-V	Especifica a versão de LDAP utilizada pelo utilitário para ligar ao servidor de LDAP. Por valor assumido, utiliza uma ligação LDAP V3. Para seleccionar explicitamente o LDAP V3, especifique -V 3. Especifique -V 2 para o executar como uma aplicação de LDAP V2.
-r	Remove da entrada valores antigos do nome distinto relativo (RDN). O valor assumido é manter os valores antigos.
-M	Gerir objectos de referência como entradas normais.
-n	Mostre o procedimento que seria efectuado mas, na realidade, não altere as entradas. É útil para depurar em conjunto com a opção **-v**.
-v	Utilize o modo verboso, com muitos diagnósticos escritos no output standard.
-c	Modo de funcionamento contínuo. Os erros são comunicados, mas ldapmodrdn continuará as modificações. O valor assumido é sair depois de comunicar um erro.
-R	Especifica que as consultas não devem ser seguidas automaticamente.
-C *charset*	Especifica que as cadeias fornecidas como input ao utilitário estão representadas num conjunto de caracteres local (*charset*) e têm de ser convertidas para UTF-8. Utilize a opção **-C** charset se a página de códigos das cadeias de input for diferente do valor da página de códigos de trabalhos. Consulte a documentação para a API ldap_set_iconv_local_charset() para ver os valores *charset* .
-d *debuglevel*	Define o nível de depuração *debuglevel*.
-D *binddn*	Utilize *binddn* para ligar ao directório de LDAP. A opção *binddn* deve ser um DN representado por uma cadeia.
-w *passwd*	Utilize *passwd* como a palavra-passe para autenticação.
-m *mechanism*	Utilize *mechanism* e especifique o mecanismo SASL para ser utilizado para estabelecer uma associação com o servidor. Será utilizada a API ldap_sasl_bind_s(). Os mecanismos disponíveis incluem o CRAM-MD5 (codifica palavras-passe), EXTERNAL (utilizado com o SSL) e o GSSAPI (Kerberos). O parâmetro -m será ignorado se -V 2 for definido. Se **-m** não for especificado, é utilizada a autenticação simples.
-O *hopcount*	Especifique *hopcount* para definir o número máximo de sistemas de passagem que a biblioteca do cliente irá passar durante a procura de sistemas de referência. A contagem de sistemas de passagem assumida é 10.
-h *ldaphost*	Especifique um sistema central alternativo no qual o servidor de LDAP esteja a ser utilizado.
-p *ldapport*	Especifique uma porta alternativa para o Transmission Control Protocol (TCP) em que o servidor de LDAP esteja a aguardar uma resposta. A porta de LDAP assumida é a 389. Se não estiver especificado e a opção **-Z** tiver sido especificada, será utilizada a porta 636 de SSL de LDAP.
-Z	Utilize uma ligação de SSL protegida para comunicar com o servidor de LDAP. A opção **-Z** só é suportada por versões desta ferramenta activadas através do SSL.

-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 (CAs) nos quais o cliente confia. Estes tipos de certificados X.509 também são conhecidos como raízes fidedignas. Este parâmetros activa efectivamente o parâmetro/comutador **-Z** .
-P *keyfilepw*	Especifique a palavra-passe da base de dados de chaves. Esta palavra-passe é necessária para aceder a informações codificadas no ficheiro da base de dados de chaves (incluindo a chave privada). Se um ficheiro para esconder a palavra-passe for associado ao ficheiro de base de dados de chaves, a palavra-passe é obtida a partir do ficheiro para esconder e este parâmetro deixa de ser necessário. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-N *certificatename*	Especifique a etiqueta associada ao certificado do cliente no ficheiro de base de dados de chaves. Tenha em atenção que se o servidor de LDAP estiver configurado para efectuar 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 do Servidor, será necessário um certificado do 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. Ele é ignorado se nem **-Z** nem **-K** forem especificados.
-f *file*	Leia as informações de modificação de entradas de um ficheiro de LDIF em vez de as ler de input standard ou do argumento comando-linha (especificando *dn* e o novo *rdn*). O input standard também pode ser fornecido a partir de um ficheiro (ficheiro <).
dn rdn	Especifique o nome distinto de uma entrada à qual pretende mudar o nome e o novo nome distinto relativo da entrada.

Exemplo: ldapmodrdn

Parta do princípio que já criou o ficheiro de texto **/tmp/entrymods** e que este tem o seguinte conteúdo:

```
nc=Modificar
Utilizador, e=Universidade de Arte, p=PO
nc=O Novo Utilizador
```

O comando seguinte:

```
ldapmodrdn -r -f /tmp/entrymods
```

alterará o RDN da entrada `Modificar Utilizador` de `Modificar Utilizador` para `O Novo Utilizador`. O cn antigo, `Modificar Utilizador` será removido.

Notas sobre a utilização de SSL com os utilitários de 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 Fornecedor de Acesso Criptográfico (5722-ACx).

O “Utilizar Secure Sockets Layer (SSL) e Translation Layer Security com o servidor de directórios de LDAP” na página 41 explica a utilização de SSL com o servidor de LDAP dos Serviços de Directório. 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 (CAs). 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 servidor de directórios. 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 CA 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 CAs 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 servidor de directórios.
- Crie um par de chaves e peça um certificado de cliente a partir de uma CA. Depois de receber o certificado assinado de uma CA, receba o certificado no ficheiro do conjunto de chaves mistas do cliente.

Capítulo 7. Resolução de problemas dos Serviços de Directório

Infelizmente, mesmo os servidores fiáveis como, por exemplo, o servidor de LDAP dos Serviços de Directório por vezes têm problemas. Quando o servidor de directórios de LDAP tiver problemas, as informações que se seguem poderão ajudá-lo a descobrir o erro e a corrigir o problema.

- "Procedimento básico de resolução de problemas dos Serviços de Directório"
- "Erros comuns do cliente de LDAP" na página 68

Para obter informações sobre os problemas comuns dos Serviços de Directório, visite a home page Serviços de Directório no seguinte URL:

`http://www.iseries.ibm.com/ldap`

Procedimento básico de resolução de problemas dos Serviços de Directório

Pode procurar códigos de retorno para erros de LDAP no ficheiro ldap.h, que está localizado no sistema em QSYSINC/H.LDAP.

Quando obtém um erro no servidor de directórios de LDAP e pretende obter mais detalhes, outra acção a efectuar é ver o registo de trabalhos QDIRSRV. Para obter erros reproduzíveis, pode utilizar o comando Rastrear Aplicação de TCP/IP (TRCTCPAPP APP(*DIRSRV)) para executar um rastreio dos erros. Consulte a secção "Utilizar TRCTCPAPP para ajudar a localizar problemas" na página 66 para obter mais informações.

Os Serviços de Directório utilizam vários servidores da Structured Query Language (SQL). 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, poderá ajudá-lo saber quais os servidores de SQL que devem ser iniciados e para que os Serviços de Directório os utilizam.

Quando o servidor de directórios de LDAP é iniciado normalmente, gera mensagens semelhantes às seguintes:

Nota: As mensagens e o número de trabalhos do servidor de SQL iniciados podem diferir em qualquer um dos casos que se seguem:
- Está a iniciar o servidor pela primeira vez.
- É necessário efectuar a migração.
- O servidor está a utilizar o registo de alterações.
- O servidor está definido de modo a permitir um maior número de ligações de bases de dados.

```
                                                    Sistema:   WARMERS
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.
    Servidor dos Serviços de Directório foi iniciado com êxito.
```

Os Serviços de Directório utilizam o primeiro servidor de SQL, 057448/QUSER/QSQSRVR, durante o arranque do servidor de LDAP. Se for necessário, os Serviços de Directório podem iniciar servidores de SQL adicionais durante o arranque do servidor de LDAP se iniciar o servidor pela primeira vez, se for necessário efectuar a migração ou se o servidor estiver a utilizar o registo de alterações. Após o arranque, estes servidores de SQL são abandonados.

Neste exemplo, não foram utilizados servidores de SQL adicionais para migração ou arranque do servidor e o registo de alterações não está configurado. Os Serviços de Directório utilizam o servidor de SQL seguinte (057340/QUSER/QSQSRVR) para replicação.

A última ligação neste exemplo (057288/QUSER/QSQSRVR) é utilizada para operações adicionar, modificar, modrdn e eliminar. As outras ligações são utilizadas para as operações procurar, ligar e comparar.

Na página Propriedades de **Base de Dados/Sufixos** do iSeries Navigator, deve especificar o número total de servidores de SQL que os Serviços de Directório utilizam para operações de directório após o arranque do servidor. Para além disso, é sempre configurado um servidor de SQL para replicação.

Supervisionar erros e o acesso com o registo de trabalhos dos Serviços de Directório

A visualização do registo de erros do servidor de LDAP pode alertá-lo para erros e ajudá-lo a supervisionar o acesso ao servidor.

Se o servidor estiver iniciado, efectue os seguintes procedimentos 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: Os Serviços de Directório utilizam 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, os Serviços de Directório podem não conseguir determinar onde poderá 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 Aplicação de TCP/IP (TRCTCPAPP) com a opção *DIRSRV pode ser utilizado no servidor de directórios de LDAP para ajudar a localizar problemas com clientes ou aplicações.

Para obter informações mais detalhadas sobre as utilizações do comando TRCTCPAPP com LDAP, bem como as restrições das autoridades necessárias, consulte a Descrição do Comando TRCTCPAPP (Rastrear Aplicação de TCP/IP).

Para obter informações gerais sobre a utilização do rastreio de comunicações, consulte Rastreio de comunicações.

Utilizar a opção LDAP_OPT_DEBUG para rastrear erros

A partir da V5R2, pode utilizar a opção LDAP_OPT_DEBUG da API **ldap_set_option()** para rastrear problemas com clientes que estejam a utilizar as APIS 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 QPOZnnnnnn
```

em que `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(QAPOZDMP LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   em que *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 do cliente de LDAP, consulte o tópico OS/400 Directory Services em Programming, 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 parte do princípio de que o cliente está a comunicar com um servidor de LDAP no OS/400. 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 69
- "[Falha na operação de LDAP]: Não é possível contactar o servidor de LDAP" na página 69
- "[Falha na operação de LDAP]: A ligação ao servidor de SSL falhou" na página 69

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 procura do servidor de directórios de LDAP. Consulte "Ajustar o rendimento do servidor de directórios de LDAP" na página 33 para obter mais informações sobre a execução deste procedimento.
- 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 relativamente a uma ocorrência em particular, consulte os registos de trabalhos do servidor QDIRSRV e Structured Query Language (SQL) tal como está descrito na secção "Procedimento básico de resolução de problemas dos Serviços de Directório" na página 65.

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 nc=Administrador.

Para obter detalhes sobre o erro, consulte o registo de trabalhos QDIRSRV como se encontra descrito na secção "Procedimento básico de resolução de problemas dos Serviços de Directório" na página 65.

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 OS/400, com um atributo UID 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 OS/400, 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 “Procedimento básico de resolução de problemas dos Serviços de Directório” na página 65.

[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 da QDIRSRV tal como se encontra descrito em “Procedimento básico de resolução de problemas dos Serviços de Directório” na página 65.

[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 “Procedimento básico de resolução de problemas dos Serviços de Directório” na página 65. Se o servidor dos Serviços de Directório tiver sido iniciado com êxito, aparecerá a mensagem ″O servidor dos Serviços de Directório foi iniciado com êxito″ no registo de trabalhos QDIRSRV.

[Falha na operação de LDAP]: A ligação ao servidor de SSL falhou

Este erro ocorre quando o servidor de LDAP rejeita a ligação do cliente porque não é possível estabelecer uma ligação protegida ao socket. 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 Gestor de Certificados Digitais para se assegurar de que os seus certificados estão definidos correctamente 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 em C do OS/400, estão disponíveis informações de erro de SSL. Consulte a documentação sobre as APIs individuais dos Serviços de Directório para obter mais detalhes.