Xerox
DocuShare®

DocuShare
Guía de LDAP/Active Directory

Fecha de publicación: Marzo de 2011

Este documento cubre DocuShare versión 6.6.1.

Preparado por:

Xerox Corporation
DocuShare Business Unit
3400 Hillview Avenue
Palo Alto, California 94304
EE.UU.

Índice

Capítulo 1 Estructura de LDAP

Capítulo 2 Configuración de LDAP/DocuShare

Estructura de LDAP 1

Descripción general de LDAP

Aunque se proporciona información básica para comprender los conceptos básicos, en esta guía no se ofrecen instrucciones para implementar LDAP o Windows Active Directory. En la información de esta guía se supone que el servidor de Active Directory ya está en funcionamiento y que un administrador de Active Directory o de LDAP se encarga de su administración. En los ejemplos de este apéndice se utiliza Microsoft Windows 2000 Server con Microsoft Internet Explorer (IE) V.6.X.

LDAP, o Protocolo ligero de acceso a directorios, es una alternativa ligera al protocolo de acceso a directorios (DAP) de X.500. LDAP utiliza la pila de protocolos TCP/IP en lugar de la pila de protocolos OSI que necesita X.500. Como alternativa ligera, LDAP simplifica algunas operaciones, pero carece del soporte de algunas características de DAP de X.500.

LDAP es el protocolo que se utiliza entre un cliente de directorio y un servidor. LDAP define el contenido de los mensajes intercambiados entre un cliente y un servidor de LDAP. El cliente de LDAP, en este caso el servidor de DocuShare, se comunica con el servidor de LDAP. El servidor de LDAP, que actúa de puerta de enlace, accede al directorio de LDAP. El directorio de LDAP se puede implementar de forma independiente en el servidor de LDAP o como un directorio en un servidor de X.500.

DocuShare envía consultas de contenido de directorio al servidor de LDAP. El servidor de LDAP accede al directorio, ya sea LDAP o X.500, y devuelve los resultados a DocuShare. El protocolo LDAP permite la lectura y la actualización de operaciones de cliente en los datos de directorio.

Nota: DocuShare no actualiza los datos de directorio de LDAP. DocuShare sólo lee los resultados de las consultas que envía al servidor de LDAP.

Estructura de LDAP

Las entradas en un directorio de LDAP se organizan mediante una estructura jerárquica específica.

Directorios

Un directorio es un tipo especial de base de datos. Los directorios están optimizados para admitir un gran volumen de solicitudes de **lectura** junto con el acceso de **escritura** que, por lo general, está limitado a los administradores del sistema. Al igual que las páginas blancas de una guía telefónica, un directorio de LDAP se lee más veces de las que se actualiza.

Del mismo modo que una guía telefónica incluye personas, empresas y organizaciones, un directorio de LDAP incluye objetos como usuarios, servidores e impresoras. De la misma forma que una guía telefónica contiene información sobre cada elemento de la lista, como el nombre, el número y la dirección, las entradas del directorio de LDAP contienen la información correspondiente a cada objeto. Esta información de objeto se denomina **atributos**.

Atributos

Cada entrada de objeto de un directorio de LDAP contiene uno o varios atributos. Cada atributo consta de un **tipo** y un **valor**. Una entrada de la guía telefónica tiene atributos como el nombre de una persona y el correspondiente número de teléfono. Los atributos de LDAP aparecen con el formato **commonName=Juan García telephoneNumber=555-555-5555**. En la Tabla 1–1 se enumeran algunos atributos habituales de LDAP, así como el alias asociado a dicho atributo.

Tabla 1–1:

Atributo de LDAP	Alias de atributo	Descripción del atributo	Ejemplo
commonName	cn	Nombre común de una entrada	Juan Sierra
Surname	sn	Apellidos de la persona	Sierra
userID	uid	ID de usuario o nombre de inicio de sesión	jsierra
telephoneNumber	-	Número de teléfono	555-123-4567
originizationalUnitName	ou	Nombre de la unidad organizativa	mi departamento
organization	o	Nombre de la organización	mi empresa
domainComponent	dc	Componente de DNS	xyz.com

Nombre distinguido relativo

El nombre distinguido relativo, o **RDN**, se representa con el formato de una **pareja de datos de atributo** (tipo y valor), como:

cn=Juan Sierra

uid=garcía

ou=marketing

dc=Xerox

Nombre distinguido

Las entradas del directorio se organizan por nombre distinguido (DN). El nombre distinguido es similar a la ruta absoluta a un archivo en el sistema de archivos de Windows. El DN de un objeto se compone del nombre y de la ubicación de la entrada en el directorio.

Un DN consta de parejas de datos de atributo de RDN, separadas por comas, como:

cn=Pedro García,ou=marketing,dc=Xerox,dc=com

cn=Pedro García,ou=ingeniería,dc=Xerox,dc=com

La ruta de un DN va del orden inferior al superior. En el sistema de archivos de Windows se utiliza el orden inverso. Del mismo modo que el sistema de archivos de Windows permite que varios archivos tengan el mismo nombre si cada archivo se encuentra en un directorio distinto, varios usuarios pueden tener el mismo RDN siempre que cada DN sea único. Tal como muestra el ejemplo de DN anterior, puede aparecer un Pedro García en el departamento de marketing y otro Pedro García en el de ingeniería.

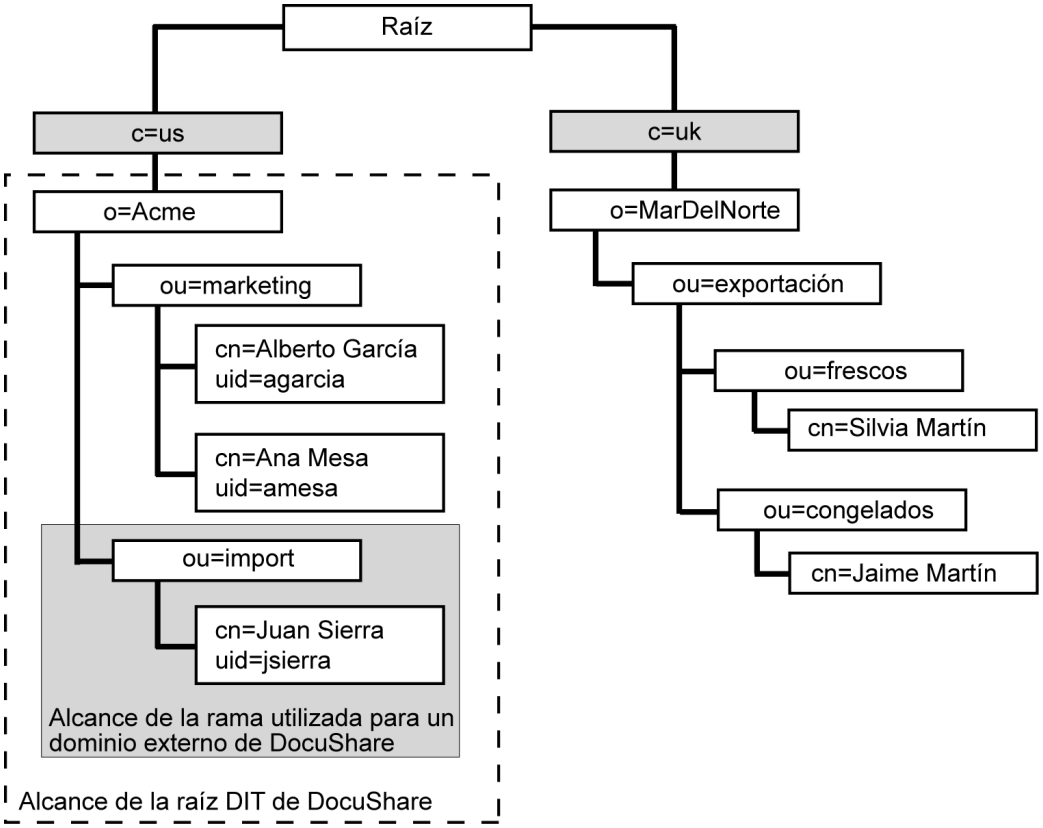
Árbol de información de directorio

El directorio organiza las entradas en una estructura de árbol jerárquica denominada árbol de información de directorio o **DIT**. Un DIT se basa en el nombre distinguido de las entradas y los nombres distinguidos están organizados en ramas que, por lo general, representan una estructura geográfica u organizativa. Microsoft Active Directory a menudo se organiza por dominios geográficos o por DNS.

Organización del DIT según dominios geográficos

En la ilustración siguiente se muestra el modo en que el administrador de una empresa de importación de marisco podría organizar la jerarquía de directorios de LDAP según la distribución geográfica. Con el fin de alojar un servidor de DocuShare para la empresa Acme en EE.UU., el administrador define la **raíz DIT** como **o=Acme, c=us**.

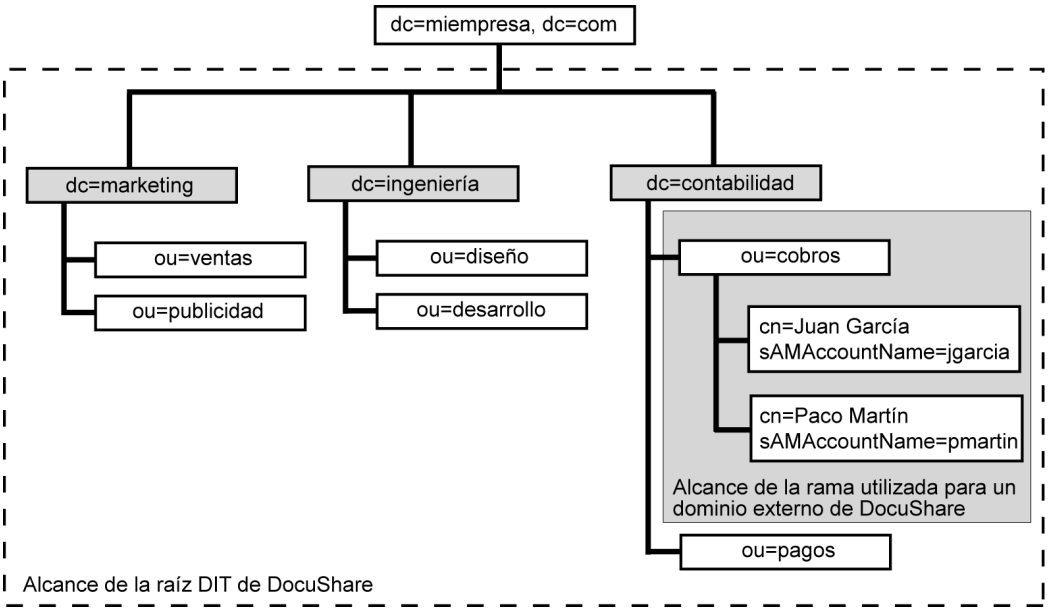
Para definir un **dominio externo** para el departamento de importación en Acme, el administrador define el localizador relativo de autenticación y de servicios de directorio como **ou=import**.



Organización del DIT según DNS

En la ilustración siguiente se muestra el modo en que el administrador de una empresa podría organizar la jerarquía de directorios de LDAP según el DNS. La empresa utiliza servidores de dominio de Windows para las divisiones de marketing, ingeniería y contabilidad. Al definir la raíz DIT como **dc=miempresa**, **dc=com**, el administrador puede crear un dominio externo de DocuShare para cada departamento de una división.

Para definir un **dominio externo** para el departamento de cobros de la división de contabilidad, el administrador define el localizador relativo de autenticación y de servicios de directorio como **ou=cobros**, **dc=contabilidad**.



Configuración de LDAP/ DocuShare 2

Configuración de DocuShare

Para configurar el sitio de DocuShare con el fin de que utilice LDAP/Active Directory, inicie la sesión como administrador en el sitio de DocuShare y, a continuación, realice los procedimientos A a F. Para configurar DocuShare correctamente, utilice la **Herramienta de administración de Active Directory** o el **comando LDIFDE de Active Directory** para recopilar la información necesaria. Ambos procesos de recopilación de información se describen en este capítulo.

A — Configuración de LDAP

Utilice la página **Configuración de LDAP** de administración de DocuShare para establecer una conexión entre el servidor de DocuShare y el servidor de LDAP, así como para definir el árbol de información de directorio que se utiliza para crear dominios externos de DocuShare.

1. Abra la página **Configuración de LDAP** de la interfaz de usuario de administración.
2. En el campo **Host**, introduzca el nombre de host, la dirección IP o el nombre DNS del servidor de LDAP/Active Directory (es preferible el DN completo o la dirección IP si no hay DN completo). Utilice un espacio para separar varias entradas de dirección de servidor de LDAP.
3. En el campo **Puerto**, introduzca el número de puerto que utiliza el servidor de LDAP si es distinto del número de puerto prefijado 389.
4. **Opcional**: en el campo **SSL**, introduzca el número de puerto que se utiliza para Secure Socket Layer.
5. En el campo **Raíz DIT**, introduzca la información obtenida mediante la búsqueda de la herramienta de administración de Active Directory como referencia para namingContext. Por ejemplo, esta información podría tener el formato dc=adoc,dc=Xerox,dc=com.
6. En el campo **Clave de NDR de usuario**, introduzca el atributo **cn**. Se trata del alias del atributo commonName. El atributo puede ser distinto, según el tipo de servidor de LDAP utilizado (iPlanet, etc.).
7. Seleccione **Agente**, en el campo **Agente del sistema**.

   La mayoría de los servidores de Active Directory necesitan un inicio de sesión de cuenta de agente o de servicio.
8. En el campo **ND**, introduzca el nombre distinguido de la cuenta de agente.

   Por ejemplo, cn=pedro,cn=usuarios,dc=adoc,dc=xerox.

9. En el campo **Clave**, introduzca la clave de la cuenta de agente.
10. Acceda a la sección Probar conexión LDAP situada en la parte inferior de la página Configuración de LDAP.

    Utilice Probar conexión LDAP para comprobar si se establece una conexión válida y se realiza un inicio de sesión correcto en el servidor de LDAP.
11. Seleccione **Agente** en el campo ND de conexión.
12. En el campo **Nombre**, introduzca el nombre distinguido que introdujo en el campo ND del paso 8.
13. En el campo **Clave** introduzca la clave que introdujo en el campo Clave del paso 9.
14. Haga clic en **Aplicar y probar**.

    Aparecerá el mensaje "Correcto" si ha establecido correctamente una conexión con el servidor de LDAP.
15. Repita los pasos del 11 al 14 pero seleccione **Usuario** en el campo ND de conexión.

Nota: En esta prueba no se comprueba la validez de la raíz DIT ni el localizador relativo de autenticación de ningún dominio externo. Sólo se verifica si DocuShare ha recibido una respuesta positiva del servidor de LDAP.

B — Configuración avanzada

Utilice la configuración avanzada de LDAP para establecer cómo se definen determinadas clases de objeto en el servidor de LDAP.

1. Haga clic en **Avanzada**, en la parte inferior de la página Configuración de LDAP.

   Aparece la página Configuración avanzada de LDAP.
2. En la parte inferior de la página Configuración avanzada de LDAP, busque el título de sección **Clases de objeto**.
3. En el campo **Usuario**, reemplace la entrada prefijada **person** por la palabra **user** (todo en minúsculas).
4. En el campo **Grupo estático**, reemplace la entrada prefijada **groupOfUniqueNames** por la palabra **group** (todo en minúsculas).
5. Haga clic en **Aplicar**.

C — Activación de los proveedores de LDAP

Utilice las páginas **Servicios de seguridad** y **Servicios de directorio** de administración de DocuShare para activar los servicios de proveedor de seguridad y directorio para LDAP. De este modo, los usuarios pueden seleccionar los dominios externos de LDAP en la lista desplegable Dominios en las solicitudes de inicio de sesión.

1. Abra la página **Servicios de seguridad** de la interfaz de usuario de administración.
2. En la página Servicios de seguridad, active la casilla **LDAP** para activar LDAP como proveedor de autenticación para todos los dominios externos y, a continuación, haga clic en **Aplicar**.

3. Abra la página **Servicios de directorio** de la interfaz de usuario de administración.
4. En la página Servicios de directorio, active la casilla **LDAP** para activar LDAP como proveedor de servicio de directorio para todos los dominios externos y, a continuación, haga clic en **Aplicar**.

D — Enlace de usuario

Utilice la página **Enlazar usuario** de administración de DocuShare para establecer una asociación entre las propiedades de cuenta de DocuShare y los atributos de cuenta de LDAP.

1. Abra la página **Enlazar usuario** de la interfaz de usuario de administración.
2. En el campo **Nombre**, introduzca el atributo que LDAP utiliza para el nombre de un usuario. Por lo general es **givenName**.
3. En el campo **Apellido(s)**, introduzca el atributo que LDAP utiliza para los apellidos de un usuario. Por lo general es **surname** o **sn**. Este campo es necesario.
4. En el campo **Nombre de usuario**, introduzca el atributo que LDAP utiliza para el nombre de inicio de sesión de un usuario. Por lo general es **sAMAccountName**. Este campo es necesario.
5. Si el directorio de LDAP contiene atributos para agregar atributos, como dirección de e-mail, dirección postal, teléfono o página principal, introdúzcalos en los campos correspondientes de la página Enlazar usuario.
6. Haga clic en **Aplicar** para guardar esta información.

E — Enlace de grupo

Utilice la página **Enlazar grupo** de administración de DocuShare para establecer una asociación entre las propiedades de cuenta de DocuShare y los atributos de cuenta de LDAP.

1. Utilice la información obtenida mediante el comando LDIFDE e introduzca los atributos en los campos adecuados de la página Enlazar grupo.

   Para obtener más información, consulte la sección de este capítulo titulada **Comando LDIFDE de Active Directory/Análisis del contenido del archivo adexport.txt/E. Atributos de Enlazar grupo**.
2. Haga clic en **Aplicar** para guardar esta información.

F — Creación de dominios

Utilice la página **Dominios** de administración de DocuShare para crear dominios externos en el sitio de DocuShare local. Cada dominio externo de DocuShare representa una rama del árbol de directorios de LDAP. Y cada rama contiene una colección de cuentas de usuario y grupo de DocuShare.

1. Abra la página **Dominios** de la interfaz de usuario de administración.
2. En el campo **Agregar**, introduzca el nombre del dominio externo que desea agregar al sitio local.

   Puede tratarse simplemente de un nombre descriptivo, como Ingeniería.

3. Seleccione **LDAP** en las páginas Proveedores/Servicios de seguridad y Proveedores/Servicios de directorio de la interfaz de usuario de administración.
4. En el campo **Localizador relativo de autenticación**, introduzca una o varias parejas de atributos para definir la ruta al directorio que contiene las cuentas de usuario y grupo.

   Utilice los componentes de atributo del ND que están a la izquierda de la raíz DIT y a la derecha del NDR de usuario.

   Por ejemplo, el ND de una cuenta de usuario de un dominio es cn=nombre de usuario,ou=ingeniería,ou=docushare,dc=adoc,dc=xerox,dc=com. El dominio Ingeniería está en la rama ou=ingeniería, ou=docushare. La raíz DIT es dc=adoc, dc=xerox, dc=com.
5. En el campo **Localizador relativo de servicios de directorio**, introduzca una o varias parejas de atributos.

   Utilice las mismas parejas de atributos que ha introducido en el campo Localizador relativo de autenticación.

   DocuShare 6.5 sólo admite LDAP para los servicios de autenticación y directorio, por lo que los valores de Localizador relativo de autenticación y Localizador relativo de servicios de directorio son idénticos.
6. Haga clic en **Agregar** para agregar este dominio externo al menú de inicio de sesión local.

G — Adición

Después de completar las páginas Configuración de LDAP, Proveedores, Enlazar usuario y Dominios, ya está listo para agregar cuentas de usuario y grupo al dominio externo del sitio de DocuShare. Si utilizara las opciones Lista de usuarios o Lista de grupos en el nuevo dominio externo, el dominio estaría vacío. Tiene que abrir el dominio en el servidor de LDAP y seleccionar las cuentas de usuario y grupo que desea como miembros del dominio externo local.

1. Abra la página **Agregar** de la interfaz de usuario de administración.

   No es la misma página que **Agregar usuario**.
2. Seleccione un **Tipo de cuenta** y un **Dominio** externo.
3. Seleccione cómo desea filtrar la lista de cuentas de dominio externo e incluir un filtro simple, como un nombre, parte de un nombre o una propiedad de objeto específica.
4. Haga clic en **Ir** para mostrar una lista de los tipos de cuenta que ha seleccionado.
5. Seleccione las cuentas que desea que aparezcan localmente en el sitio y haga clic en la flecha de **Agregar** para moverlas al campo **Seleccionado**. Si no se incluye una cuenta en el campo Seleccionado, se impide que dicho usuario o grupo acceda al sitio.
6. Cuando finalice, haga clic en **Agregar cuentas**. DocuShare agrega las cuentas de usuario o grupo de dominio externo a la lista local de dominios externos.
7. Vaya a la página **Ir a Listar/Buscar/Agregar usuario** para ver los usuarios asignados al nuevo dominio externo.

H — Vista del inicio de sesión

1. Vuelva a la página principal de DocuShare.
2. En la sección Iniciar sesión de la página principal, el nuevo dominio externo debe aparecer en el menú de **dominio de Inicio de sesión**.
3. Un usuario de un dominio externo debe seleccionar el dominio correcto para iniciar la sesión o DocuShare muestra un mensaje de error de inicio de sesión y una solicitud para que se vuelva a intentar.

LDAP y SSL

Secure Socket Layer, o SSL, es un protocolo desarrollado por Netscape para transmitir documentos privados a través de Internet. SSL funciona mediante el uso de una clave pública para cifrar los datos que se transfieren a través de una conexión SSL. Netscape Navigator e Internet Explorer admiten SSL. Muchos sitios web utilizan SSL para obtener información de usuario confidencial, como números de tarjeta de crédito y claves de cuenta. Una sesión SSL se inicia mediante el uso de una URL que empieza por **https** en vez de **http**.

Certificados

Cuando se utiliza SSL, los servidores y los clientes emplean certificados como pruebas de identidad antes de establecer una conexión segura. Un certificado también contiene claves públicas y privadas que se utilizan para establecer una sesión. Servidores y clientes utilizan **claves de sesión** para cifrar y descifrar datos.

Los certificados pueden estar firmados automáticamente o emitidos por una entidad emisora de certificados (CA) como Entrust, Equifax, Valicert o Verisign. Los certificados emitidos por una CA se considera que proceden de una **entidad independiente de confianza**. Básicamente, la entidad independiente garantiza la identidad de un usuario. La mayoría de los exploradores cliente están configurados para reconocer y confiar en los certificados emitidos por las CA.

Cuando los certificados son de firma automática, el usuario actúa como una entidad emisora de certificados. Un certificado de firma automática se debe instalar en el almacén de entidades del explorador y no se reconoce como una entidad independiente de confianza.

Los certificados se emiten como certificados de cliente o de servidor. DocuShare no admite los certificados de cliente. DocuShare utiliza una copia del certificado del servidor de LDAP para establecer la sesión SSL con el servidor de LDAP.

Importar el certificado en DocuShare

Según la CA que ha emitido el certificado, puede que el administrador tenga que importarlo desde el servidor de LDAP en el almacén de certificados del explorador de web del servidor de DocuShare. Si el certificado es de firma automática, el administrador **debe** importarlo en el almacén de certificados del explorador de web del servidor de DocuShare.

Para importar el certificado desde un servidor de LDAP específico:

1. Abra un explorador de web en el servidor de DocuShare.
2. Conéctese al servidor de LDAP mediante la dirección https://<su.servidor.ldap>:636.

   El puerto 636 es el estándar para SSL.
3. Si el certificado no se ha instalado en el explorador del servidor de DocuShare, aparecerá una ventana de alerta de seguridad solicitando que lo instale.
4. Para instalar el certificado, haga clic en **Ver certificado** en la parte inferior de la ventana de alerta de seguridad.

   Aparece la ventana Certificado.
5. Haga clic en la ficha **Detalles** y, a continuación, en el botón **Copiar al archivo**.

Exportar el certificado y guardarlo como archivo CER

Después de haber importado el certificado desde el servidor de LDAP, tiene que exportarlo al directorio de DocuShare y guardarlo como archivo de certificado.

Para exportar el certificado y guardarlo como archivo de certificado:

1. Haga clic en **Siguiente** en la ventana del asistente.

   Si el certificado contiene una clave privada, aparecerá la ventana Exportar la clave privada.

2. En la ventana Exportar la clave privada, seleccione **No exportar la clave privada**.

   DocuShare no necesita una clave privada para establecer una sesión SSL con el servidor de LDAP.

3. Haga clic en **Siguiente**.

   Aparecerá la ventana Formato de archivo de exportación.

4. Seleccione **X.509 codificado base 64 (.CER)** en la ventana Formato de archivo de exportación.

5. Haga clic en **Siguiente**.

   Aparecerá la ventana Archivo para exportar.

6. En el campo **Nombre de archivo** introduzca la ruta de directorio a una ubicación de la unidad donde desee exportar el certificado. Por ejemplo, **D:**.

7. En el campo Nombre de archivo, después de la ruta de directorio, introduzca el nombre del certificado con la extensión **.cer**. Por ejemplo, **D:\SSL_Cert4LDAP.cer**.

8. Haga clic en **Siguiente** para terminar la exportación del certificado.

   Aparecerá la ventana Finalización del Asistente para exportación de certificados.

9. Haga clic en **Finalizar** para cerrar el asistente.

   El certificado de LDAP se guarda como archivo .cer en el sitio de DocuShare.

10. Siga las instrucciones de la siguiente página, **Colocar el certificado en DSTrustStore**.

Colocar el certificado en DSTrustStore

Una vez guardado el certificado como archivo de certificado, debe colocarlo en el archivo **DSTrustStore**.

Para colocar el archivo .cer de certificado en el archivo DSTrustStore:

1. Busque el archivo .cer que ha exportado mediante el Asistente para exportación de certificados.
2. Copie el archivo .cer en el directorio de DocuShare que contiene el archivo DSTrustStore **jdk1.5.0\jre\lib\security**.
3. Abra una ventana del símbolo del sistema y desplácese al directorio que contiene **dstruststore**.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>cd\xerox\docushare\jdk1.5.0\jre\lib\security
C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security\dir
 Volume in drive C is Local Disk
 Volume in Serial Number is 508B-0D2F
 Directory of C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security
18-11-02   15:55         <DIR>          -
18-11-02   15:55         <DIR>          --
02-10-02   12:25                 7,365 cacerts
02-10-02   12:26                   589 dstruststore
02-10-02   12:26                 2,271 java.policy
02-10-02   12:26                 4,115 java.security
10-11-02   15:43                   844 SLL_Cert4LDAP.cer
          5 Files(s)         15,184 bytes
          2 Dir(s)    1,486,024,704 bytes free

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

4. En el símbolo del sistema, introduzca el comando **set PATH** para definir la variable de entorno PATH. Utilice **set PATH=%PATH%;**<su directorio de DocuShare>**\jdk1.5.0\jre\bin**.

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

5. Después de definir la variable PATH, en el símbolo del sistema, introduzca **keytool**, sin argumentos.

   Aparece la ayuda de la utilidad Keytool. La utilidad Keytool coloca el certificado SSL en DSTrustStore.

6. En el símbolo del sistema, introduzca el comando de la utilidad keytool **keytool -import -alias <alias_name> -file <cert_file> -keystore dstruststore**

   Reemplace **<alias_name>** por un nombre exclusivo para el archivo de certificado.

   Reemplace **<cert_file>** por el nombre del archivo de certificado (.cer) que ha exportado y copiado en el directorio que contiene el archivo dstruststore.

7. Pulse **Intro** para iniciar el comando.

   Aparecerá una solicitud de una clave.

8. Introduzca **password** y pulse **Intro**.

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

Enter keystore password: password
Owner: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
Issuer: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
Serial number: 5ee8abd44c2cd2b14ffbee159f03d354
Valid from: Tue Feb 19 10:57:21 PST 2002 until: Thu Jan 26 10:57:21 PST 2102
Certificate fingerprints:
        MD5: 78:C7:A3:04:32:69:EB:97:76:FE:F4:8A:11:A2:65:26
        SHA1: 02:DD:9A:BE:BE:DE:3C:AA:22:AE:14:9A:F2:F2:5B:11:61:6D:5A:5F
Trust this certificate? [no]: yes
Certificate was added to keystore

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

9. Examine los resultados de la pantalla para asegurarse de que Keytool ha agregado correctamente el certificado al almacén de claves. Si Keytool ha terminado la operación, el servidor de DocuShare ahora está listo para utilizar el certificado con el fin de establecer una sesión SSL con el servidor de LDAP.
10. Una vez terminada la importación del certificado, reinicie el servidor de DocuShare.

Herramienta de administración de Active Directory

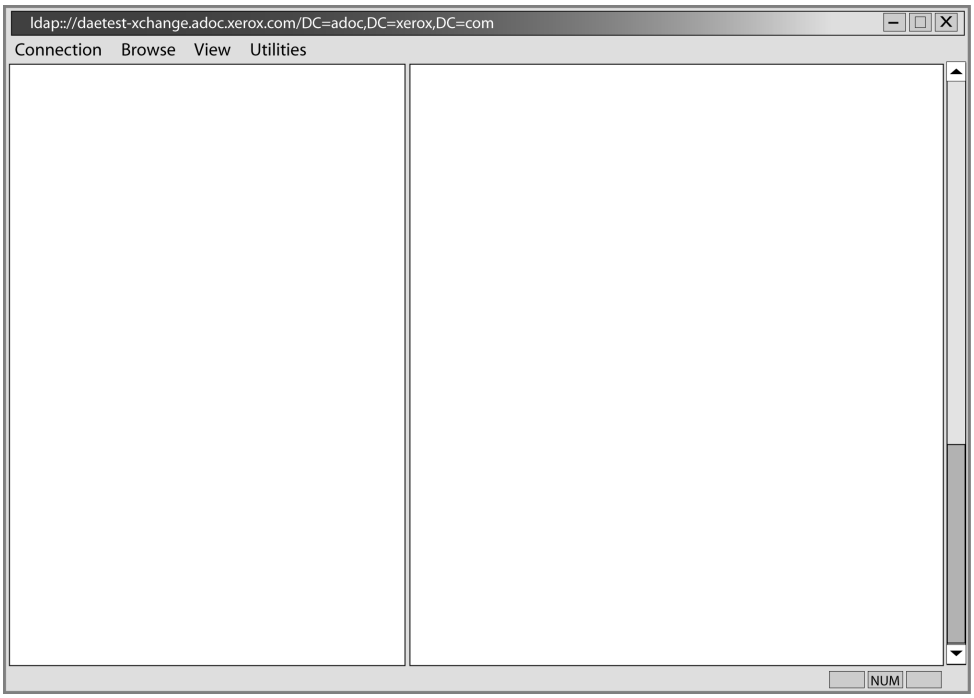
Se puede utilizar la herramienta de administración de Active Directory (ldp.exe) para realizar varias operaciones en un directorio enlazado a Active Directory y consultar a un servidor de directorio de LDAP.

Si se utiliza ldp.exe para conectar con un servidor de LDAP que admite SSL, primero se deberá activar el certificado SSL en el servidor de DocuShare. Para importar y cargar un certificado SSL, siga las instrucciones para **LDAP y SSL** que aparecen en el *capítulo 2* de esta guía.

Para instalar y utilizar la herramienta de administración de Active Directory con el fin de configurar el sitio de DocuShare:

1. Abra el soporte de software del servidor Windows 2000 y busque y consulte el archivo **sreadme.doc**.
2. Localice el archivo **setup.exe** en el directorio Support\Tools.
3. Haga clic en el archivo **setup.exe** para comenzar la instalación del archivo ldp.exe.
4. Siga las instrucciones que aparecen en la pantalla para instalar **ldp.exe**.
5. Una vez terminada la instalación, abra el menú Inicio de Windows y haga clic en la **herramienta de administración de Active Directory**.

   De este modo se inicia ldp.exe y aparece la herramienta de administración de Active Directory. La herramienta dispone de una barra de desplazamiento con comandos y un marco a la izquierda y otro a la derecha donde muestra la información.



Uso de la herramienta de administración de Active Directory

Puede utilizar la herramienta de administración de Active Directory para obtener información del servidor de LDAP que necesita para configurar el sitio de DocuShare con el fin de que utilice el servidor para los dominios externos. Realice los procedimientos A a F.

Nota: Este procedimiento se basa en el uso de la herramienta para obtener información de una configuración de servidor de LDAP típica. Puede haber variaciones según el modo en que se haya configurado el servidor.

A — Conexión

1. Seleccione **Conexión** en la barra de desplazamiento de la herramienta de administración de Active Directory y, a continuación, seleccione **Conectar** en el menú Conexión.

   Aparecerá el cuadro de diálogo Conectar.

2. Introduzca en el campo **Servidor** la dirección IP o el nombre DNS del servidor de LDAP/Active Directory.
3. Introduzca en el campo **Puerto** el número de puerto utilizado si es distinto del que se muestra.
4. Haga clic en **Aceptar**.

   Ya ha definido la dirección y el número de puerto del servidor de LDAP.

B — Enlace

Después de configurar la conexión al servidor de LDAP, debe enlazar el servidor a una cuenta de administrador que tenga permiso de acceso para buscar en el directorio.

1. Seleccione **Conexión** en la barra de desplazamiento de la herramienta de administración de Active Directory y, a continuación, seleccione **Enlazar** en el menú Conexión.

   Aparecerá el cuadro de diálogo Enlazar.

2. Introduzca el nombre de cuenta de usuario en el campo **Usuario**, la clave en el campo **Clave** y el dominio en el campo **Dominio**.
3. Haga clic en **Aceptar**.

   Si se ha conectado y ha creado correctamente un enlace al servidor de LDAP, el servidor muestra un **texto de respuesta en el marco derecho** de la herramienta de administración de Active Directory.

C — Búsqueda del nombre distinguido base

El ND base será el punto de partida del examen del árbol de directorios.

1. Busque en el texto de respuesta del marco derecho de la herramienta de administración de Active Directory una referencia a **namingContext**.

   El formato de namingContext varía según el servidor de LDAP que utilice.

2. El texto resaltado es el nombre distinguido base del DIT.

   Por ejemplo, el ND base resaltado puede ser **dc=adoc,dc=Xerox,dc=com**. Su ND base real puede ser distinto según la estructura única de su árbol de directorios de LDAP. Anote esta información para utilizarla más adelante.

D — Vista del árbol de información de directorio

1. Seleccione **Ver** en la barra de desplazamiento de la herramienta de administración de Active Directory y, a continuación, seleccione **Árbol** en el menú Ver.

   Aparecerá el cuadro de diálogo Vista de árbol.

2. En el campo **ND base** introduzca el **nombre distinguido base** que ha encontrado en la búsqueda de namingContext anterior.

3. Haga clic en **Aceptar**.

   El DIT del servidor de LDAP se muestra en el marco izquierdo de la herramienta de administración de Active Directory.

4. Examine el árbol para determinar dónde estará la raíz DIT para cualquier dominio externo de DocuShare que desee crear.

   La raíz debe tener una posición suficientemente alta en la jerarquía para que incluya todas las ramas (como organizationUnit y domainComponents) que tendrán acceso al servidor de DocuShare.

   En el ejemplo se utilizará dc=adoc, dc=xerox,dc=com como raíz DIT ya que sólo se desea incluir a los usuarios del dominio ADOC y no a todos los de Xerox.com.

E — Búsqueda de la cuenta de agente

En la mayoría de los casos, el servidor de Active Directory no acepta consultas anónimas al directorio. Esto requiere el uso de una cuenta de agente o de servicio para consultar el servidor. Utilice el comando Buscar para buscar el ND de la cuenta de agente.

1. Seleccione **Examinar** en la barra de desplazamiento de la herramienta de administración de Active Directory y, a continuación, seleccione **Buscar** en el menú Examinar.

   Aparecerá el cuadro de diálogo Buscar.

2. Introduzca un ND base en el campo **ND base**.

   Según el valor de ND base utilizado y la ubicación en la jerarquía de la cuenta de agente, puede que tenga que seleccionar **Subárbol** para ampliar el alcance de la búsqueda.

3. Introduzca un filtro en el campo **Filtro**.

   Se ha utilizado el atributo sAMAccoutName para el filtro puesto que se conoce el nombre de inicio de sesión de la cuenta de agente. Este atributo es exclusivo de Active Directory y procede de Windows NT. Si conociéramos el atributo commonName (cn) de la cuenta, se podría haber utilizado, por ejemplo, commonName=Peter Pan. Un servidor de iPlanet puede utilizar el atributo uid o commonName (cn).

4. Seleccione el **Alcance** de la búsqueda.

   Seleccione **Subárbol** si **Un nivel** no ofrece suficiente alcance.

5. Haga clic en **Ejecutar**.

   El resultado de la búsqueda aparecerá como texto en el marco derecho de la ventana de la herramienta de administración de Active Directory. Por ejemplo, la búsqueda podría mostrar que el atributo **distinguishedName** de la cuenta de agente es cn=TestUser1,cn=users,dc=adoc,dc=xerox,dc=com.

F — Siguiente paso

Después de realizar los procedimientos A a E, debe poder utilizar la herramienta de administración de Active Directory con el fin de recopilar la información necesaria para configurar el sitio de DocuShare y utilizar LDAP para la autenticación de cuentas de usuario.

- Dirección IP o nombre DNS del servidor de LDAP
- Raíz DIT
- Cuenta de agente para DocuShare

Comando LDIFDE de Active Directory

Si ejecuta el servidor de LDAP en Windows 2000 o Windows 2003, puede utilizar el comando **LDIFDE** para escribir en un archivo de texto el contenido de todo el directorio de LDAP o de un dominio específico del directorio de LDAP. Este archivo de texto contiene la mayor parte de la información que necesita para configurar DocuShare y utilizarlo con LDAP.

El archivo de texto generado por LDIFDE es el archivo principal que utiliza el servicio de asistencia técnica de DocuShare para solucionar los problemas relacionados con la configuración de LDAP.

Recursos: Para obtener más información acerca del comando LDIFDE, vaya a **http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q237/6/77.ASP&NoWebContent=1**

Sintaxis y uso del comando LDIFDE

Para utilizar el comando LDIFDE, abra una ventana de símbolo del sistema en el servidor de LDAP, introduzca **C:\Windows\system32>idifde -?** y pulse **Intro**. LDIFDE devuelve lo siguiente:

```
LDIF Directory Exchange

General Parameters
==================
-i                  Turn on Import Mode (The default is Export)
-f filename         Input or Output filename
-s servername       The server to bind to (Default to DC of logged in Domain)
-c FromDN ToDN      Replace occurences of FromDN to ToDN
-v                  Turn on Verbose Mode
-j                  Log File Location
-t                  Port Number (default = 389)
-u                  Use Unicode format
-?                  Help

Export Specific
===============
-d RootDN           The root of the LDAP search (Default to Naming Context)
-r Filter           LDAP search filter (Default to "(objectClass=*)")
-p SearchScope      Search Scope (Base/OneLevel/Subtree)
-l list             List of attributes (comma separated) to look for in an LDAP search
-o list             List of attributes (comma separated) to omit from input.
-g                  Disable Paged Search.
-m                  Enable the SAM logic on export.
-n                  Do not export binary values

Import
======
-k                  The import will go on ignoring 'Constraint Violation' and 'Object
                    Already Exists' errors
-y                  The import will use lazy commit for better performance

Credentials Establishment
=========================
Note that if no credentials is specified, LDIFDE will bind as the currently
logged on user, using SSPI.

-a UserDN [Password | *]          Simple authentication
-b UserName Domain [Password | *]   SSPI bind method
Example: Simple import of current domain
    ldifde -i -f INPUT.LDF

Example: Simple export of current domain
    ldifde -f OUTPUT.LDF

Example: Export of specific domain with credentials
    ldifde -m -f OUTPUT.LDF
          -b USERNAME DOMAINNAME *
          -s SERVERNAME
          -d "cn=users,DC=DOMAINNAME,DC=Microsoft,DC=Com"
          -r "(objectClass=user)"
```

Ejemplo de comando LDIFDE

A continuación se presenta el ejemplo de un comando LDIFDE que escribe el contenido de Active Directory en un servidor denominado Corvette en un archivo de texto denominado **adexport.txt**.

Ejecutar el comando LDIFDE:

Introduzca el comando **C:\Windows\system32\LDIFDE.exe -f adexport.txt -s corvette** y pulse **Intro**.

El comando se ejecuta y muestra su progreso:

```
Connecting to "corvette"
Logging in as current user using SSPI
Exporting directory to file adexport.txt
Searching for entries...
Writing out entries.....................................................
.....................................................
132 entries exported

The command has completed successfully

C:\Documents and Settings\Administrator>LDIFDE -f adexport.txt -s corvette
Connecting to "corvette"
Logging in as current user using SSPI
Exporting directory to file adexport.txt
Searching for entries...
Writing out entries.....................................................
.....................................................
132 entries exported

The command has completed successfully
```

El archivo adexport.txt generado

A continuación se muestra el contenido del archivo adexport.txt generado por el comando FDIFDE de nuestro ejemplo. Este ejemplo muestra únicamente un fragmento del contenido completo del archivo. Fíjese ante todo en los elementos **en negrita**; se trata de elementos que necesita para configurar DocuShare para utilizar este servidor de LDAP en concreto.

dn: DC=infodev,DC=dsbu,DC=xerox,DC=com
changetype: add
masteredBy:CN=NTDS Settings, CN=CORVETTE, CN=Servers, CN=infodev-dsbu-site, CN=Sites,CN=Configuration, DC=infodev, DC=dsbu, DC=xerox, DC=com
auditingPolicy:: AAE=
creationTime: 127199619543431088
dc: infodev
forceLogoff: -9223372036854775808
fSMORoleOwner:CN=NTDS Settings, CN=CORVETTE, CN=Servers,CN=infodev-dsbu-site, CN=Sites, CN=Configuration, DC=infodev, DC=dsbu, DC=xerox, DC=com
●
●
●
[Sample Directory Record for a single User]
dn: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com
changetype: add
accountExpires: 9223372036854775807
badPasswordTime: 0
badPwdCount: 0
codePage: 0
cn: Duncan Donkey
countryCode: 0
displayName: Duncan Donkey
mail: ddonkey@infodev.xerox.com
givenName: Duncan
instanceType: 4
lastLogoff: 0
lastLogon: 0
logonCount: 0
distinguishedName: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com
objectCategory:CN=Person, CN=Schema, CN=Configuration, DC=infodev, DC=dsbu, DC=xerox,DC=com
objectClass: user
objectGUID:: xmi02W78lEmpYca7AtiupQ==
objectSid:: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0bgQAAA==
primaryGroupID: 513
pwdLastSet: 127293917905389760
name: Duncan Donkey
sAMAccountName: duncan
sAMAccountType: 805306368
sn: Donkey
userAccountControl: 512
userPrincipalName: duncan@infodev.dsbu.xerox.com
uSNChanged: 7353
uSNCreated: 7349
whenChanged: 20040518220950.0Z
whenCreated: 20040518220933.0Z
●
●
●

Continuación del archivo de texto...

[Sample Directory Record for a Group]
dn: CN=labusers,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
changetype: add
member: CN=Greg Wong,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Janet Gilmore,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Jennings\, Ferris,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Cua\, Kiam T,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
info: Authorized Login User to the InforDev Lab
cn: labusers
description: InfoDev Lab Users
groupType: -2147483644
instanceType: 4
distinguishedName:CN=labusers, CN=Users, DC=infodev, DC=dsbu, DC=xerox, DC=com
objectCategory: CN=Group, CN=Schema, CN=Configuration, DC=infodev, DC=dsbu, DC=xerox, DC=com
objectClass: group
objectGUID:: Cm9phZkOn0ig4iEWMRPWsg==
objectSid:: AQUAAAAAAAUVAAAAqDfWZRUlr0f4n7R0VgQAAA==
name: labusers
sAMAccountName: labusers
sAMAccountType: 536870912
uSNChanged: 3975
uSNCreated: 2540
whenChanged: 20040302161513.0Z
whenCreated: 20040130190128.0Z

Análisis del contenido del archivo adexport.txt

Nuestro archivo de ejemplo adexport.txt utiliza el nombre distinguido (ND) de Duncan Donkey, miembro del equipo de actores digitales en el departamento InfoDev de DSBU de Xerox Corporation.

En nuestro ejemplo, el ND de Duncan Donkey se define como: **CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com**

Al examinar el nombre distinguido de un usuario, puede encontrar la información necesaria para identificar:

a. La raíz del árbol de información de directorio (DIT)
b. La clave de NDR de usuario
c. Los localizadores relativos de autenticación y de servicios de directorio
d. Atributos de Enlazar usuario
e. Atributos de Enlazar grupo

A — Raíz del árbol de información de directorio (DIT)

Establezca la raíz DIT en el nivel del árbol de directorio que incluya todas las ramas del directorio que contienen usuarios con necesidad de acceso al servidor de DocuShare. En nuestro ejemplo, sólo los miembros de la organización DSBU de Xerox tendrán acceso al servidor de DocuShare de ejemplo.

La organización DSBU incluye varios departamentos y equipos dentro de cada departamento. Estos departamentos y equipos están organizados en el directorio de LDAP por componentes de dominio (DC) y unidades organizativas (OU). Para nuestro ejemplo, configuraremos un dominio externo en DocuShare para autenticar a los usuarios que sean miembros del equipo de actores digitales en el departamento InfoDev de DSBU de Xerox Corporation.

En el ejemplo, la raíz DIT del ND de Duncan Donkey se muestra aquí en negrita: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, **DC=dsbu, DC=xerox, DC=com**

Al definir la raíz DIT en este nivel de la jerarquía, se pueden crear dominios externos para cada departamento/equipo en DSBU.

B — Clave de NDR de usuario

La clave de NDR de usuario es el alias de atributo que se utiliza para identificar al usuario.

En el ejemplo, la clave de NDR de usuario del ND de Duncan Donkey se muestra aquí en negrita: **CN=Duncan Donkey**, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com

C — Localizadores relativos de autenticación y de servicios de directorio

Los localizadores relativos de autenticación y de servicios de directorio son los punteros a la rama del directorio del dominio externo que contiene un usuario, varios usuarios o un grupo específico.

En el ejemplo, el localizador relativo de autenticación y de servicios de directorio se muestra aquí en negrita: CN=Duncan Donkey, **OU=Digital, OU=Actors, DC=infodev**, DC=dsbu, DC=xerox, DC=com.

D — Atributos de Enlazar usuario

El archivo de texto generado por el comando FDIFDE contiene los alias de atributo utilizados para identificar el apellido, el nombre de usuario y la dirección de correo electrónico de cada usuario de la lista. Estos alias de atributo se utilizan para configurar las propiedades de Enlazar usuario de DocuShare LDAP. En el archivo de texto del comando FDIFDE, los usuarios del directorio de LDAP se identifican con la entrada **objectClass: user**.

En nuestro ejemplo, encontrará los **alias de atributo de LDAP** para las siguientes propiedades:

Apellido = **sn**

Nombre de usuario = **sAMAccountName**

Dirección de correo electrónico = **mail**

En el ejemplo, los valores que se otorgan a estos alias de atributo de LDAP son:

sn: Donkey

sAMAccountName: duncan

mail: ddonkey@infodev.xerox.com

E — Atributos de Enlazar grupo

El archivo de texto generado por el comando FDIFDE contiene los alias de atributo utilizados para identificar el título, la descripción y la información de resumen de cada grupo de la lista. Estos alias de atributo se utilizan para configurar las propiedades de Enlazar grupo de DocuShare LDAP.

En el archivo de texto del comando FDIFDE, los grupos del directorio de LDAP se identifican con la entrada **objectClass: group**.

En nuestro ejemplo, encontrará los **alias de atributo de LDAP** para las siguientes propiedades:

Título = **cn**

Descripción = **description**

Resumen = **info**

En el ejemplo, los valores que se otorgan a estos alias de atributo de LDAP son:

cn: labusers

description: InfoDev Lab Users

info: Authorized Login User to the InfoDev Lab