Xerox
DocuShare®

DocuShare
Guide LDAP/Active Directory

Date de publication : Mars 2011

Le présent document se rapporte à DocuShare version 6.6.1.

Préparé par :

Xerox Corporation
DocuShare Business Unit
3400 Hillview Avenue
Palo Alto, Californie 94304
États-Unis

Table des matières

La structure LDAP 1

Aperçu de LDAP

Le présent guide fournit des informations de base nécessaires à la compréhension de notions élémentaires mais ne traite pas de la procédure de mise en oeuvre de LDAP ou Windows Active Directory proprement dite. Il présuppose que le serveur Active Directory est déjà en place et qu'il est géré par un administrateur Active Directory ou LDAP. Les exemples présentés dans l'annexe ont été créés à l'aide de Microsoft Windows 2000 Server et Microsoft Internet Explorer (IE) V.6.X.

LDAP (Lightweight Directory Access Protocol - protocole d'accès aux annuaires léger) est une solution de rechange légère au protocole X.500 DAP (Directory Access Protocol). LDAP fait appel à la suite de protocoles TCP/IP plutôt qu'à la pile de protocoles du modèle OSI exigée par la norme X.500. En tant que solution de rechange légère, LDAP simplifie certaines opérations, mais ne prend pas en charge certaines fonctions de X.500 DAP.

LDAP est le protocole utilisé entre un client d'annuaire et un serveur. LDAP définit le contenu des messages échangés entre un client et un serveur LDAP. Le client LDAP, ici le serveur DocuShare, communique avec le serveur LDAP. Le serveur LDAP, agissant comme une passerelle, accède à l'annuaire LDAP. L'annuaire LDAP peut être mis en oeuvre de manière autonome sur le serveur LDAP ou en tant qu'annuaire sur un serveur X.500.

DocuShare envoie au serveur LDAP des requêtes sur le contenu de l'annuaire. Le serveur LDAP accède à l'annuaire LDAP ou X.500 et renvoie les résultats à DocuShare. Le protocole LDAP permet au client de lire et de mettre à jour les données de l'annuaire.

Remarque : DocuShare ne met pas à jour les données d'annuaire LDAP. Il lit uniquement les résultats des requêtes qu'il envoie au serveur LDAP.

Structure LDAP

Les entrées d'un annuaire LDAP sont organisées selon une structure hiérarchique particulière.

Annuaires

Un annuaire est un type particulier de base de données. Les annuaires sont optimisés de manière à accepter un volume élevé de requêtes de **lecture** et un accès en **écriture** généralement réservé aux administrateurs système. Tout comme les pages blanches de l'annuaire téléphonique, l'annuaire LDAP est lu plus souvent qu'il n'est mis à jour.

De la même manière que l'annuaire téléphonique répertorie des individus, des entreprises et des organismes, un annuaire LDAP répertorie des objets comme des utilisateurs, des serveurs et des imprimantes. De la même façon que l'annuaire téléphonique contient des renseignements sur chaque entrée, comme le nom, le numéro de téléphone et l'adresse, les entrées de l'annuaire LDAP comportent également des informations pertinentes sur chaque objet. Ces informations sont qualifiées d'**attributs**.

Attributs

Chaque entrée d'objet dans un annuaire LDAP contient un ou plusieurs attributs. Chaque attribut est constitué d'un **type** et d'une **valeur**. Une entrée dans un annuaire téléphonique a aussi des attributs, comme le nom d'une personne et le numéro de téléphone correspondant. Les attributs LDAP apparaissent sous la forme **commonName=Jeanne Simard telephoneNumber=555-555-5555**. Le Tableau 1–1 présente certains attributs LDAP courants ainsi que l'alias associé à chacun.

Tableau 1–1 :

Attribut LDAP	Alias de l'attribut	Description de l'attribut	Exemple
commonName	cn	Nom courant d'une entrée	Jeanne Simard
Surname	sn	Nom de la personne	Simard
userID	uid	Nom d'utilisateur ou nom de connexion	jsimard
telephoneNumber	-	Numéro de téléphone	555-123-4567
originizationalUnitName	ou	Nom de l'unité organisationnelle	mon service
organization	o	Nom de l'entreprise	ma société
domainComponent	dc	Composant DNS	xyz.com

Nom distinctif relatif

Le nom distinctif relatif, ou **RDN** (Relative Distinguished Name), est représenté par la **paire de données d'un attribut** (type et valeur), telle que :

cn=Jeanne Simard

uid=jsimard

ou=marketing

dc=Xerox

Nom distinctif

Les entrées de l'annuaire sont organisées en fonction d'un nom distinctif (DN). Le nom distinctif est similaire au chemin d'accès absolu à un fichier dans le système de fichiers de Windows. Le DN d'un objet est constitué du nom et de l'emplacement de l'entrée dans l'annuaire.

Il est formé des paires de données des attributs RDN séparées par une virgule, comme dans les exemples ci-dessous :

cn=Jeanne Simard,ou=marketing,dc=Xerox,dc=com

cn=Jeanne Simard,ou=fabrication,dc=Xerox,dc=com

Les éléments du chemin d'un DN sont organisés du plus précis au plus général, soit un ordre d'assemblage inverse de celui utilisé dans le système de fichiers de Windows. De la même manière que le système de fichiers de Windows permet que plusieurs fichiers portent le même nom s'ils sont dans des répertoires différents, plusieurs utilisateurs peuvent avoir le même RDN dans la mesure où chaque DN est unique. Comme le montre l'exemple de DN précédent, une Jeanne Simard peut être répertoriée dans le service du marketing et une autre dans le service de fabrication.

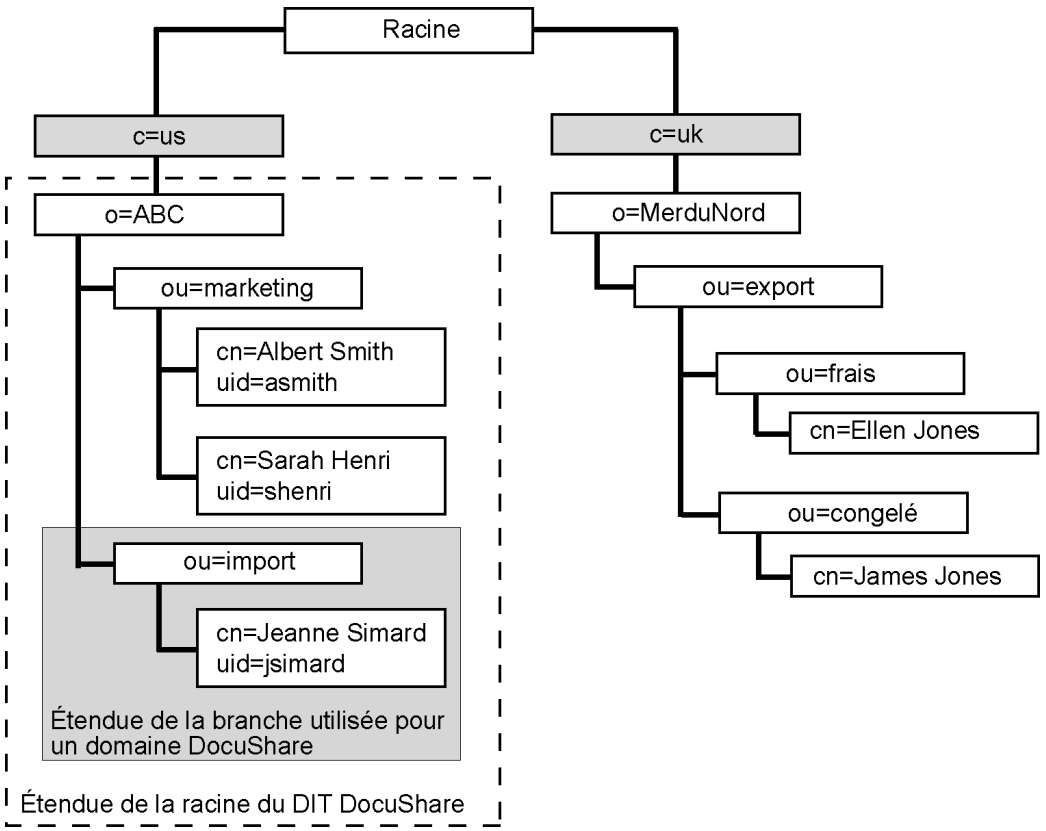
Arbre d'informations d'annuaire

L'annuaire organise les entrées dans une structure hiérarchique arborescente appelée **DIT** (Directory Information Tree) ou arbre d'informations d'annuaire. Le DIT repose sur les noms distinctifs des entrées, organisés en branches représentant généralement une structure géographique ou organisationnelle. Microsoft Active Directory est souvent organisé par domaine géographique ou par DNS.

DIT organisé par domaine géographique

La figure suivante montre comment l'administrateur d'une société d'importation de produits de la mer pourrait organiser l'annuaire LDAP en fonction des régions géographiques. Pour héberger un serveur DocuShare destiné à leur société Acme aux États-Unis, l'administrateur définirait la **racine du DIT** comme étant **o=Acme, c=us**.

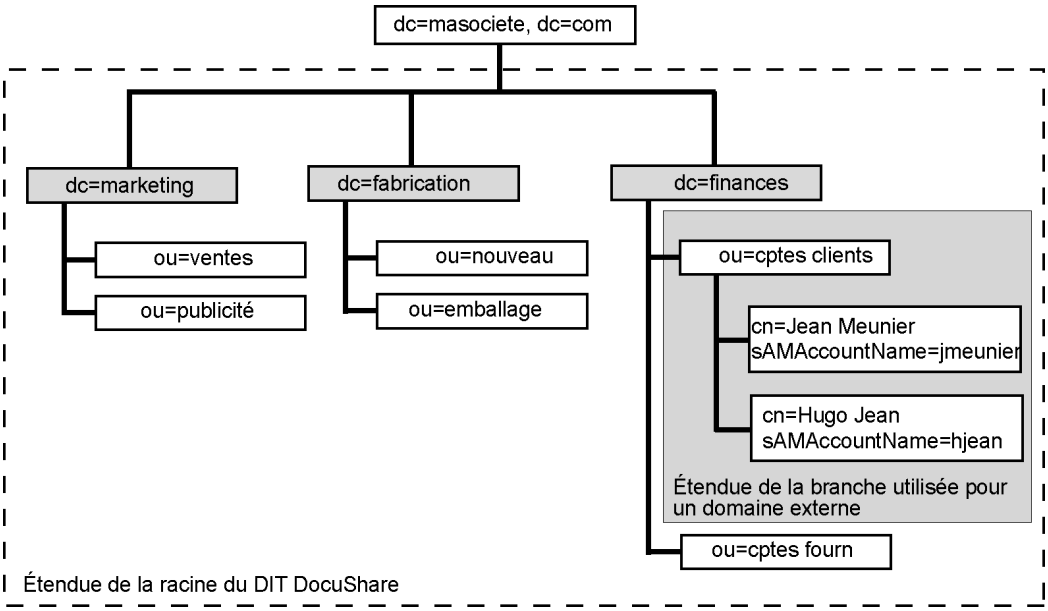
Pour définir un **domaine externe** correspondant au service des importations d'Acme, l'administrateur spécifierait l'authentification relative et le localisateur de service d'annuaire comme étant **ou=import**.



DIT organisé par DNS

La figure suivante montre comment l'administrateur d'une société d'importation de produits de la mer pourrait organiser l'annuaire LDAP en fonction du DNS. L'entreprise utilise des serveurs de domaine Windows pour les divisions du marketing, de la fabrication et des finances. En définissant la racine du DIT comme étant **dc=masociete**, **dc=com**, l'administrateur peut créer un domaine externe DocuShare pour chaque service au sein d'une division.

Pour définir un **domaine externe** pour le service des comptes clients dans la division Finances, l'administrateur spécifierait l'authentification relative et le localisateur de service d'annuaire comme étant **ou=cptes clients**, **dc=finances**.



Configuration LDAP/DocuShare 2

Configuration DocuShare

Pour configurer votre site DocuShare de manière à utiliser LDAP/Active Directory, connectez-vous au site en tant qu'admin, puis effectuez les procédures A à F. Pour configurer DocuShare correctement, utilisez l'**outil d'administration Active Directory** ou la **commande Active Directory LDIFDE** afin d'obtenir les informations nécessaires. Ces deux processus de collecte d'information sont décrits dans le présent chapitre.

A — Configuration LDAP

Utilisez la page **Configuration LDAP** de l'outil d'administration DocuShare pour établir une connexion entre votre serveur DocuShare et votre serveur LDAP et définir l'arbre d'informations d'annuaire servant à créer des domaines externes DocuShare.

1. Ouvrez la page **Configuration LDAP** de l'outil d'administration.
2. Dans le champ **Hôte(s)**, entrez le nom d'hôte, l'adresse IP ou le nom DNS du serveur LDAP/Active Directory (de préférence le nom distinctif complet [FQDN] ou, sinon, l'adresse IP). Séparez plusieurs adresses de serveur LDAP par un espace.
3. Dans le champ **Port**, entrez le numéro de port de votre serveur LDAP s'il est différent du numéro de port 389 par défaut.
4. **Facultatif** : dans le champ **SSL**, entrez le numéro du port utilisé pour Secure Socket Layer.
5. Dans le champ **Racine du DIT**, entrez les informations obtenues lors de la recherche d'une référence namingContext à l'aide de l'outil d'administration Active Directory. Cette information se présenterait sous la forme dc=adoc,dc=Xerox,dc=com, par exemple.
6. Dans le champ **Clé RDN utilisateur**, entrez l'attribut **cn**. Il s'agit de l'alias de l'attribut commonName. Cet attribut varie selon le type de serveur LDAP utilisé (iPlanet, etc.).
7. Sélectionnez **Agent** dans le champ **Agent système**.

   La majorité des serveurs Active Directory exigent que la connexion soit établie au moyen d'un compte d'agent ou de service.
8. Dans le champ **DN**, entrez le nom distinctif du compte d'agent.

   Exemple : cn=jean,cn=users,dc=adoc,dc=xerox.
9. Dans le champ **Mot de passe**, entrez le mot de passe du compte d'agent.

10. Allez à la section Vérifier la connexion LDAP au bas de la page Configuration LDAP.

    Utilisez Test pour vérifier que la connexion est valide et qu'une session s'ouvre sur le serveur LDAP.

11. Sélectionnez **Agent** dans le champ DN de connexion.
12. Dans le champ **Nom**, entrez le nom distinctif que vous avez saisi dans le champ DN à l'étape 8.
13. Dans le champ **Mot de passe**, entrez le même mot de passe que celui que vous avez saisi à l'étape 9.
14. Cliquez sur **Appliquer et vérifier**.

    Le message « Réussite » apparaît si vous avez correctement établi une connexion au serveur LDAP.

15. Répétez les étapes 11 à 14, mais sélectionnez **Utilisateur** dans le champ DN de connexion.

Remarque : Ce test ne vérifie pas la validité de la racine du DIT ni le localisateur relatif d'authentification des domaines externes ; il vérifie seulement si DocuShare a reçu une réponse positive du serveur LDAP.

B — Configuration avancée

Utilisez la page Configuration LDAP avancée pour spécifier comment certaines classes d'objets sont définies sur votre serveur LDAP.

1. Cliquez sur **Avancé** au bas de la page Configuration LDAP.

   La page Configuration LDAP avancée apparaît.

2. Au bas de la page Configuration LDAP avancée, repérez la section **Classes d'objets**.
3. Dans le champ **Utilisateur**, remplacez l'entrée par défaut (**person**) par le mot **user** (en lettres minuscules).
4. Dans le champ **Groupe statique**, remplacez l'entrée **groupOfUniqueNames** par défaut par le mot **group** (en lettres minuscules).
5. Cliquez sur **Appliquer**.

C — Activation des services de fournisseur LDAP

Utilisez les pages **Services de sécurité** et **Service d'annuaire** de l'outil d'administration DocuShare afin d'activer les services de sécurité et de fournisseur d'annuaire pour LDAP. Cela permet aux utilisateurs de sélectionner les domaines externes LDAP à partir de la liste déroulante Domaines dans les invites de connexion.

1. Ouvrez la page **Services de sécurité** de l'outil d'administration.
2. Dans la page Services de sécurité, cochez la case **LDAP** pour activer LDAP en tant que fournisseur d'authentification pour tous les domaines externes, puis cliquez sur **Appliquer**.
3. Ouvrez la page **Service d'annuaire** de l'outil d'administration.

4. Dans la page Service d'annuaire, cochez la case **LDAP** pour activer LDAP en tant que fournisseur de services d'annuaire pour tous les domaines externes, puis cliquez sur **Appliquer**.

D — Liaison d'un utilisateur

Utilisez la page **Lier un utilisateur** de l'outil d'administration DocuShare pour associer les propriétés de compte DocuShare aux attributs de compte LDAP.

1. Ouvrez la page **Lier un utilisateur** de l'outil d'administration.
2. Dans le champ **Prénom**, entrez l'attribut que LDAP utilise pour le prénom d'un utilisateur. Il s'agit généralement de **givenName**.
3. Dans le champ **Nom**, entrez l'attribut que LDAP utilise pour le nom de famille d'un utilisateur. Il s'agit généralement de **surname** ou **sn**. Ce champ est obligatoire.
4. Dans le champ **Nom d'utilisateur**, entrez l'attribut que LDAP utilise pour le nom de connexion d'un utilisateur. Il s'agit généralement de **sAMAccountName**. Ce champ est obligatoire.
5. Si l'annuaire LDAP contient des attributs supplémentaires tels que l'adresse électronique, l'adresse postale, le numéro de téléphone ou une page d'accueil, entrez ces attributs dans les champs appropriés de la page Lier un utilisateur.
6. Cliquez sur **Appliquer** pour enregistrer ces informations.

E — Liaison d'un groupe

Utilisez la page **Lier un groupe** de l'outil d'administration DocuShare pour associer les propriétés de compte DocuShare aux attributs de compte LDAP.

1. Servez-vous des informations obtenues à l'aide de la commande LDIFDE et entrez ces attributs dans les champs pertinents de la page Lier un groupe.

   Pour plus d'informations, reportez-vous, dans ce chapitre, à la section **Commande Active Directory LDIFDE/Analyse du contenu du fichier adexport.text/E. Propriétés Lier un groupe**.
2. Cliquez sur **Appliquer** pour enregistrer ces informations.

F — Création d'un domaine

Utilisez la page **Domaines** de l'outil d'administration DocuShare pour créer des domaines externes sur votre site DocuShare local. Chaque domaine externe DocuShare forme une branche dans l'arborescence de l'annuaire LDAP. Chaque branche contient une collection de comptes d'utilisateur et de groupe DocuShare.

1. Ouvrez la page **Domaines** de l'outil d'administration.
2. Dans le champ **Ajouter**, entrez le nom du domaine externe que vous désirez ajouter à votre site local.

   Il peut s'agir d'un nom descriptif comme Fabrication.
3. Sélectionnez **LDAP** dans les pages Fournisseurs l Services de sécurité et Fournisseurs l Service d'annuaire de l'outil d'administration.

4. Dans le champ **Localisateur relatif d'authentification**, entrez une ou plusieurs paires d'attributs afin de définir le chemin d'accès au répertoire qui contient les comptes d'utilisateur et de groupe.

   Utilisez les composants d'attribut du DN à gauche de la racine du DIT et à droite du RDN de l'utilisateur.

   Par exemple, le DN d'un compte d'utilisateur dans un domaine est cn=nom d'utilisateur,ou=fabrication,ou=docushare,dc=adoc,dc=xerox,dc=com.
   Le domaine Fabrication est dans la branche ou=fabrication, ou=docushare.
   La racine du DIT est dc=adoc, dc=xerox, dc=com.

5. Dans le champ **Localisateur relatif de service d'annuaire**, entrez une ou plusieurs paires d'attributs.

   Utilisez les mêmes paires d'attributs que celles que vous avez entrées dans le champ Localisateur relatif d'authentification.

   Étant donné que DocuShare 6.5 prend en charge LDAP uniquement pour les services d'authentification et d'annuaire, les valeurs du Localisateur relatif d'authentification et du Localisateur relatif de service d'annuaire sont identiques.

6. Cliquez sur **Ajouter** pour ajouter ce domaine externe à votre menu de connexion local.

G — Ajout de comptes

Après avoir rempli les pages Configuration LDAP, Fournisseurs, Lier un utilisateur et Domaines, vous pouvez ajouter des comptes d'utilisateur et de groupe dans le domaine externe de votre site DocuShare. Si vous demandiez maintenant la liste des utilisateurs ou des groupes dans le nouveau domaine externe, elle apparaîtrait vide. Vous devez donc ouvrir le domaine sur le serveur LDAP et sélectionner les comptes d'utilisateur et de groupe que vous désirez ajouter dans votre domaine externe local.

1. Ouvrez la page **Ajouter** de l'outil d'administration.

   Il s'agit d'une page différente de la page **Ajouter un utilisateur**.

2. Sélectionnez un **type de compte** et un **domaine** externe.

3. Indiquez comment la liste des comptes du domaine externe doit être filtrée et incluez un filtre simple tel qu'un nom ou un nom partiel, ou une propriété d'objet spécifique.

4. Cliquez sur **Aller à** pour afficher la liste des types de comptes que vous avez sélectionnés.

5. Sélectionnez les comptes que vous souhaitez afficher localement sur votre site, puis cliquez sur la flèche **Ajouter** pour les déplacer vers le champ **Sélectionné**. En n'incluant pas un compte dans le champ Sélectionné, vous empêchez l'utilisateur ou le groupe correspondant d'accéder à votre site.

6. Lorsque vous avez terminé, cliquez sur **Ajouter des comptes**. DocuShare ajoute les comptes d'utilisateur ou de groupe à la liste locale du domaine externe.

7. Accédez à la page **Aller à Répertorier/Rechercher/Ajouter des utilisateurs** pour afficher les utilisateurs affectés au nouveau domaine externe.

H — Affichage du domaine de connexion

1. Retournez à la page d'accueil de DocuShare.
2. Le nouveau domaine externe devrait apparaître dans le menu **Domaine** de la section Connexion de la page d'accueil.
3. Pour se connecter, un utilisateur d'un domaine externe doit sélectionner le domaine correct ; sinon DocuShare affiche un message d'erreur lui demandant d'essayer de nouveau.

LDAP et SSL

SSL (Secure Socket Layer) est un protocole mis au point par Netscape pour la transmission de documents privés par Internet. Il utilise une clé publique pour chiffrer les données transférées via une connexion SSL. Netscape Navigator et Internet Explorer prennent tous deux en charge SSL. De nombreux sites Web utilisent SSL pour recueillir des renseignements confidentiels auprès des utilisateurs, comme des numéros de carte de crédit ou des mots de passe d'accès à des comptes. On ouvre une session SSL en utilisant une URL qui commence par **https** au lieu de **http**.

Certificats

Avec SSL, les serveurs et les clients utilisent des certificats pour fournir une preuve d'identité avant d'établir une connexion sécurisée. Un certificat contient aussi les clés publiques et privées qui servent à établir une connexion. Les serveurs et les clients utilisent des **clés de session** pour chiffrer et déchiffrer les données.

Les certificats sont autosignés ou émis par une autorité de certification (CA) comme Entrust, Equifax, Valicert ou Verisign. Les CA sont considérées comme des **tiers de confiance**. Essentiellement, ces tiers répondent de l'identité des utilisateurs. La majorité des navigateurs clients sont configurés de manière à reconnaître et à faire confiance aux certificats émis par les CA.

Dans le cas des certificats autosignés, l'utilisateur agit à titre d'autorité de certification. Un certificat autosigné doit être installé dans le magasin des autorités du navigateur et il n'est pas considéré comme provenant d'un tiers de confiance.

Les certificats sont émis en tant que certificat de client ou de serveur. DocuShare n'accepte pas les certificats de client. DocuShare utilise une copie du certificat du serveur LDAP pour établir la session SSL avec le serveur LDAP.

Importation du certificat dans DocuShare

Selon la CA qui a émis le certificat, l'administrateur peut devoir importer ce dernier du serveur LDAP vers le magasin de certificats du navigateur Web du serveur DocuShare. Dans le cas d'un certificat autosigné, l'administrateur **doit** importer le certificat dans le magasin de certificats du navigateur Web du serveur DocuShare.

Pour importer le certificat d'un serveur LDAP particulier, procédez comme suit :

1. Ouvrez un navigateur Web sur le serveur DocuShare.
2. Ouvrez une session sur le serveur LDAP avec l'adresse - https://<votre.serveur.ldap>:636.

   Le port 636 est le port standard pour SSL.
3. Si le certificat n'a pas été installé dans le navigateur du serveur DocuShare, une fenêtre d'alerte de sécurité apparaît pour vous inviter à le faire.
4. Pour installer le certificat, cliquez sur **Afficher le certificat** au bas de la fenêtre d'alerte de sécurité.

   Une fenêtre Certificat apparaît.
5. Cliquez sur l'onglet **Détails**, puis cliquez sur le bouton **Copier dans un fichier**.

Exportation du certificat et enregistrement en tant que fichier CER

Après avoir importé le certificat du serveur LDAP, vous devez ensuite l'exporter dans un répertoire DocuShare et l'enregistrer en tant que fichier de certificat.

Pour exporter le certificat et l'enregistrer en tant que fichier de certificat, procédez comme suit :

1. Cliquez sur **Suivant** au bas de la fenêtre de l'Assistant.

   Si le certificat contient une clé privée, la fenêtre Exportation de la clé privée apparaît.

2. Dans la fenêtre Exportation de la clé privée, sélectionnez **Non, ne pas exporter la clé privée**.

   DocuShare n'aura pas besoin de clé privée pour établir une session SSL avec le serveur LDAP.

3. Cliquez sur **Suivant**.

   La fenêtre Format de fichier d'exportation apparaît.

4. Sélectionnez **Codé à base 64 X.509 (.cer)** dans la fenêtre Format de fichier d'exportation.

5. Cliquez sur **Suivant**.

   La fenêtre d'invite Fichier à exporter apparaît.

6. Dans le champ **Nom du fichier**, entrez le chemin d'accès à l'emplacement où vous désirez exporter le certificat sur votre lecteur, par exemple, **D:**.

7. À la suite du chemin d'accès dans le champ Nom du fichier, entrez un nom de fichier avec extension **.cer** pour le certificat, par exemple, **D:\SSL_Cert4LDAP.cer**.

8. Cliquez sur **Suivant** pour terminer l'exportation du certificat.

   La fenêtre Fin de l'Assistant Exportation de certificat apparaît.

9. Cliquez sur **Terminer** pour fermer l'Assistant.

   Le certificat LDAP est enregistré en tant que fichier .cer sur votre site DocuShare.

10. Suivez les instructions de la page suivante, **Mise en place du certificat dans DSTrustStore**.

Mise en place du certificat dans DSTrustStore

Après avoir enregistré le certificat en tant que fichier de certificat, vous devez le placer dans le fichier **DSTrustStore**.

Pour placer le fichier .cer du certificat dans le fichier DSTrustStore, procédez comme suit :

1. Repérez le fichier .cer que vous avez exporté à l'aide de l'Assistant Exportation de certificat.
2. Copiez le fichier .cer dans le répertoire DocuShare contenant le fichier DSTrustStore, **jdk1.5.0\jre\lib\security**.
3. Ouvrez une fenêtre de commande et allez au répertoire contenant **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 fichier(s)        15 184 octets
          2 Rép(s)    1 486 024 704 octets libres

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

4. À l'invite, entrez la commande **set PATH** afin de définir la variable d'environnement PATH. Utilisez **set PATH=%PATH%;**<votre répertoire 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. Après avoir défini la variable PATH, entrez **keytool** sans arguments à l'invite.

   L'aide de l'utilitaire Keytool apparaît. L'utilitaire Keytool place le certificat SSL dans le magasin de certificats DSTrustStore.

6. À l'invite, entrez la commande d'utilitaire **keytool -import -alias <nom_alias> -file <fichier_cert> -keystore dstruststore**

   Remplacez **<nom_alias>** par un nom unique pour le fichier de certificat.

   Remplacez **<fichier_cert>** par le nom du fichier de certificat (.cer) que vous avez exporté et copié dans le répertoire contenant le fichier dstruststore.

7. Appuyez sur **Entrée** pour exécuter la commande.

   Une invite de mot de passe apparaît.

8. Entrez le **mot de passe** et appuyez sur **Entrée**.

```
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. Examinez les informations affichées pour vous assurer que l'utilitaire Keytool a bien ajouté le certificat dans le magasin de certificats. Si Keytool a effectué l'opération avec succès, votre serveur DocuShare est maintenant prêt à utiliser le certificat pour établir une session SSL avec votre serveur LDAP.
10. Après avoir importé le certificat, redémarrez le serveur DocuShare.

Outil d'administration Active Directory

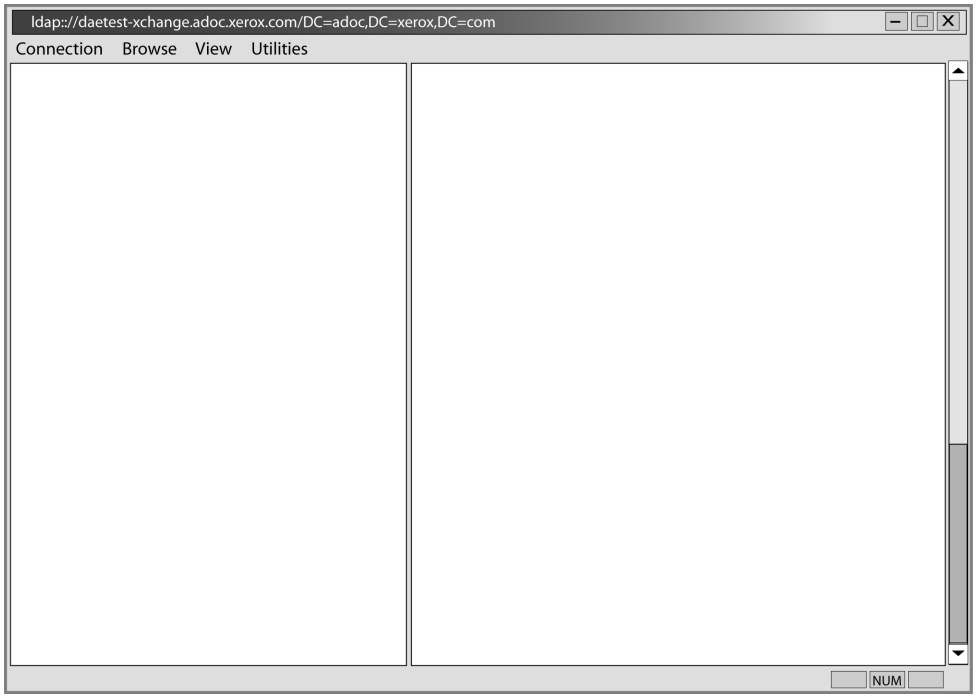
Vous pouvez utiliser l'outil d'administration Active Directory (ldp.exe) pour effectuer diverses opérations sur un annuaire Active Directory et pour interroger un serveur d'annuaire LDAP.

Si vous établissez une connexion à un serveur LDAP SSL à l'aide de ldp.exe, vous devez dans un premier temps activer le certificat SSL sur votre serveur DocuShare. Pour importer et charger un certificat SSL, suivez les instructions fournies à la section **LDAP et SSL** au *Chapitre 2* de ce guide.

Pour installer et utiliser l'outil d'administration Active Directory afin de vous aider à configurer votre site DocuShare, procédez de la façon suivante :

1. Ouvrez le support de Windows 2000 Server, puis repérez et lisez le fichier **sreadme.doc**.
2. Repérez le fichier **setup.exe** dans le répertoire Support\Tools.
3. Cliquez sur le fichier **setup.exe** pour lancer l'installation du fichier ldp.exe.
4. Suivez les instructions à l'écran pour installer **ldp.exe**.
5. Une fois l'installation terminée, ouvrez le menu Démarrer de Windows et cliquez sur **Active Directory Administration Tool**.

   Cette opération lance ldp.exe et l'outil d'administration Active Directory apparaît. L'outil comporte une barre de navigation avec des commandes, ainsi qu'un volet gauche et un volet droit pour afficher les informations.



Utilisation de l'outil d'administration Active Directory

Vous pouvez utiliser l'outil d'administration Active Directory pour recueillir les informations nécessaires relatives à votre serveur LDAP afin de configurer votre site DocuShare de manière qu'il utilise le serveur pour les domaines externes. Effectuez les procédures A à F.

Remarque : Cette procédure permet de recueillir des informations sur une configuration classique de serveur LDAP. Des variantes peuvent exister selon la façon dont le serveur a été configuré.

A — Connexion

1. Sélectionnez **Connection** dans la barre de navigation de l'outil d'administration Active Directory, puis sélectionnez **Connect** dans le menu Connection.

   La boîte de dialogue Connect apparaît.

2. Dans le champ **Server**, entrez l'adresse IP ou le nom DNS du serveur LDAP Active Directory.

3. Dans le champ **Port**, entrez le numéro du port utilisé, s'il est différent de celui affiché par défaut.

4. Cliquez sur **OK**.

   Vous avez défini l'adresse et le numéro de port du serveur LDAP.

B — Liaison

Après avoir défini la connexion au serveur LDAP, vous devez associer le serveur à un compte d'administrateur ayant les droits d'accès nécessaires pour effectuer des recherches dans l'annuaire.

1. Sélectionnez **Connection** dans la barre de navigation de l'outil d'administration Active Directory, puis sélectionnez **Bind** dans le menu Connection.

   La boîte de dialogue Bind apparaît.

2. Entrez le nom du compte d'utilisateur dans le champ **User**, le mot de passe dans le champ **Password** et le domaine dans le champ **Domain**.

3. Cliquez sur **OK**.

   Si vous avez bien établi la connexion et créé une liaison au serveur LDAP, celui-ci affiche une **réponse textuelle dans le volet droit** de l'outil d'administration Active Directory.

C — Repérage du nom distinctif de base

Le DN de base sera le point de départ de notre examen de l'arborescence de l'annuaire.

1. Repérez le texte **namingContext** dans la réponse affichée dans le volet droit de l'outil d'administration Active Directory.

   Le format de namingContext dépend du serveur LDAP utilisé.

2. Le texte en évidence est le nom distinctif de base pour le DIT.

Le DN de base en évidence pourrait être **dc=adoc,dc=Xerox,dc=com**, par exemple. Votre DN de base réel dépend de la structure unique de votre arborescence d'annuaire LDAP. Prenez note de ces informations, vous en aurez besoin plus loin.

D — Affichage de l'arbre d'informations d'annuaire

1. Sélectionnez **View** dans la barre de navigation de l'outil d'administration Active Directory, puis sélectionnez **Tree** dans le menu View.

   La boîte de dialogue Tree View apparaît.

2. Dans le champ **BaseDN**,entrez le **nom distinctif de base** que vous avez trouvé lors de la recherche de namingContext ci-dessus.

3. Cliquez sur **OK**.

   Le DIT de votre serveur LDAP est affiché dans le volet gauche de la fenêtre de l'outil d'administration Active Directory.

4. Examinez l'arbre afin de déterminer où situer la racine du DIT pour les domaines externes DocuShare que vous désirez créer.

   La racine doit être suffisamment élevée dans la hiérarchie pour inclure toutes les branches (telles que organizationUnit et domainComponents) qui accéderont au serveur DocuShare.

   Pour notre exemple, nous utiliserons dc=adoc, dc=xerox,dc=com comme racine du DIT car nous voulons inclure uniquement les utilisateurs du domaine ADOC et non tous les utilisateurs à Xerox.com.

E — Repérage du compte d'agent

Dans la majorité des cas, Active Directory n'accepte pas les interrogations anonymes dans l'annuaire. Il faut donc utiliser un compte d'agent ou de service pour interroger le serveur. Utilisez la commande Search pour trouver le DN du compte d'agent.

1. Sélectionnez **Browse** dans la barre de navigation de l'outil d'administration Active Directory, puis sélectionnez **Search** dans le menu Browse.

   La boîte de dialogue Search apparaît.

2. Dans le champ **Base DN**, entrez un DN de base.

   Selon la valeur utilisée comme DN de base et l'emplacement du compte d'agent dans la hiérarchie, il vous faudra peut-être sélectionner **Subtree** pour étendre la portée de la recherche.

3. Remplissez le champ **Filter**.

   Nous avons utilisé l'attribut sAMAccoutName comme filtre car nous connaissions le nom de connexion du compte d'agent. Cet attribut est unique à Active Directory et provient de Windows NT. Si nous connaissions le commonName (cn) du compte, nous pourrions utiliser commonName=Peter Pan, par exemple. Un serveur iPlanet peut utiliser l'attribut uid ou commonName (cn).

4. Sélectionnez l'étendue (**Scope**) de la recherche.

   La valeur **One Level** pour **Subtree** n'est pas suffisante.

5. Cliquez sur **Run**.

Les résultats de la recherche apparaissent sous forme de texte dans le volet droit de la fenêtre de l'outil d'administration Active Directory. Par exemple, une recherche pourrait montrer que le **nom distinctif** du compte d'agent est cn=TestUser1,cn=users,dc=adoc,dc=xerox,dc=com.

F — Étape suivante

Après avoir effectué les procédures A à E, vous devriez être en mesure d'utiliser l'outil d'administration Active Directory pour recueillir les informations nécessaires afin de configurer votre site DocuShare de manière à ce qu'il utilise LDAP pour authentifier les comptes d'utilisateur.

- L'adresse IP ou le nom DNS du serveur LDAP
- La racine du DIT
- Le compte d'agent pour DocuShare

Commande Active Directory LDIFDE

Si vous exécutez votre serveur LDAP sous Windows 2000 ou Windows 2003, vous pouvez utiliser la commande **LDIFDE** pour écrire dans un fichier texte le contenu de l'annuaire LDAP complet ou d'un domaine particulier de l'annuaire. Ce fichier texte contient la majeure partie des informations dont vous avez besoin pour configurer DocuShare afin de l'utiliser avec LDAP.

Le fichier généré par LDIFDE est le principal fichier utilisé par le service d'assistance DocuShare pour résoudre les problèmes de configuration LDAP.

Ressources : Pour plus d'informations sur l'utilisation de la commande LDIFDE, visitez le site **http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q237/6/77.ASP&NoWebContent=1**

Syntaxe et utilisation de la commande LDIFDE

Pour utiliser la commande LDIFDE, ouvrez une fenêtre d'invite de commande sur le serveur LDAP, tapez **C:\Windows\system32>ldifde -?** et appuyez sur **Entrée**. LDIFDE affiche ce qui suit :

```
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
-?                  Aide

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

Importer
======
-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)"
```

Exemple d'utilisation de la commande LDIFDE

Dans l'exemple suivant, la commande LDIFDE écrit le contenu de l'annuaire Active Directory sur un serveur nommé Corvette dans un fichier texte intitulé **adexport.txt**.

Exécution de la commande LDIFDE

Entrez la commande **C:\Windows\system32\LDIFDE.exe -f adexport.txt -s corvette** et appuyez sur **Entrée**.

La commande est exécutée et son déroulement est affiché progressivement :

```
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
```

Fichier adexport.txt généré

L'encadré ci-dessous présente le contenu du fichier adexport.txt produit par la commande FDIFDE de l'exemple précédent. L'encadré ne montre qu'une partie du contenu du fichier. Portez une attention particulière aux éléments **en gras** ; ce sont ceux que vous devez configurer sur DocuShare pour utiliser ce serveur LDAP particulier.

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
●
●
●

Suite du fichier texte...

[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

Analyse du contenu du fichier adexport.txt

Dans notre exemple, le fichier adexport.txt utilise le nom distinctif (DN) de Duncan Donkey, un membre de l'équipe Digital Actors du service InfoDev de la division DSBU chez Xerox Corporation.

Le DN de Duncan Donkey est défini ainsi : **CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com**

En examinant le nom distinctif des utilisateurs, vous pouvez trouver les informations nécessaires pour identifier les éléments suivants :

a. Racine de l'arbre d'informations d'annuaire (DIT)
b. Clé RDN utilisateur
c. Localisateurs relatifs d'authentification et de service d'annuaire
d. Attributs de liaison utilisateur
e. Attributs de liaison groupe

A — Racine de l'arbre d'informations d'annuaire (DIT)

Définissez la racine du DIT au niveau approprié de l'arbre d'annuaire, de manière à englober toutes les branches contenant les utilisateurs qui ont besoin d'accéder au serveur DocuShare. Dans notre exemple, seuls les membres de l'organisation DSBU de Xerox auront accès au serveur DocuShare.

L'organisation DSBU regroupe plusieurs services, chacun étant constitué de plusieurs équipes. Ces services et ces équipes sont organisés dans l'annuaire LDAP par composants de domaine (DC) et unités organisationnelles (OU). Pour notre exemple, nous allons créer un domaine externe dans DocuShare pour authentifier les utilisateurs qui sont membres de l'équipe Digital Actors du service InfoDev de DSBU chez Xerox Corporation.

La racine DIT du DN de Duncan Donkey est présentée en gras dans l'exemple : CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, **DC=dsbu, DC=xerox, DC=com**.

En définissant la racine du DIT à ce niveau dans la hiérarchie, on peut créer un domaine externe pour chaque service ou équipe de DSBU.

B — Clé RDN utilisateur

La clé RDN utilisateur est l'alias d'attribut utilisé pour identifier l'utilisateur.

La clé RDN utilisateur du DN de Duncan Donkey est présentée en gras dans l'exemple : **CN=Duncan Donkey**, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com.

C — Localisateurs relatifs d'authentification et de service d'annuaire

Les localisateurs relatifs d'authentification et de service d'annuaire sont des pointeurs vers la branche d'annuaire du domaine externe qui contient un utilisateur, des utilisateurs ou un groupe spécifiques.

Ils sont présentés en gras dans l'exemple : CN=Duncan Donkey, **OU=Digital, OU=Actors, DC=infodev**, DC=dsbu, DC=xerox, DC=com.

D — Attributs de liaison utilisateur

Le fichier texte généré par la commande FDIFDE contient les alias des attributs servant à préciser le nom de famille, le nom d'utilisateur et l'adresse de courrier électronique de chaque utilisateur répertorié. Vous utiliserez ces alias d'attribut pour configurer les propriétés Lier un utilisateur DocuShare LDAP. Dans le fichier texte produit par la commande FDIFDE, les utilisateurs figurant dans l'annuaire LDAP sont identifiés par l'entrée **objectClass: user**.

Dans l'exemple, vous trouverez les **alias d'attribut LDAP** pour les propriétés suivantes :

Nom de famille = **sn**

Nom d'utilisateur = **sAMAccountName**

Adresse électronique = **mail**

Dans l'exemple, les valeurs données à ces alias d'attribut LDAP sont les suivantes :

sn: Donkey

sAMAccountName: duncan

mail: ddonkey@infodev.xerox.com

E — Attributs de liaison groupe

Le fichier texte généré par la commande FDIFDE contient les alias des attributs servant à préciser le titre, la description et le sommaire de chaque groupe répertorié. Vous utiliserez ces alias d'attribut pour configurer les propriétés Lier un groupe DocuShare LDAP.

Dans le fichier texte produit par la commande FDIFDE, les groupes figurant dans l'annuaire LDAP sont identifiés par l'entrée **objectClass: group**.

Dans l'exemple, vous trouverez les **alias d'attribut LDAP** pour les propriétés suivantes :

Titre = **cn**

Description = **description**

Sommaire = **info**

Dans l'exemple, les valeurs données à ces alias d'attribut LDAP sont les suivantes :

cn: labusers

description: InfoDev Lab Users

info: Authorized Login User to the InfoDev Lab