

# Rappels LDAP

Benoit Métrot

*benoit.metrot@math.univ-poitiers.fr*

UMR 7348 - Laboratoire de Mathématiques et Applications (Poitiers)

ANF Développement logiciel pour l'administration  
système et réseau  
Angers, 23 mai 2012

Objectifs et  
caractéris-  
tiques d'un  
annuaire

Protocole  
LDAP

Outils LDAP

1 Objectifs et caractéristiques d'un annuaire

2 Protocole LDAP

3 Outils LDAP

# Progression

- 1 Objectifs et caractéristiques d'un annuaire
- 2 Protocole LDAP
- 3 Outils LDAP

# Organisation de l'information

Objectifs et caractéristiques d'un annuaire

Protocole LDAP

Outils LDAP

- Structure arborescente
  - Racine
  - Branches
  - Feuille ou entrée
- Types de données spécifiés par un schéma
- Structuration de l'information selon un modèle clé/valeur

# Comparaison avec une base de données

Objectifs et caractéristiques d'un annuaire

Protocole LDAP

Outils LDAP

- Opérations de lecture largement majoritaires
- Optimisé pour une lecture rapide
- Types de données extensibles
- Diffusion plus large
- Plus grande duplication de l'information

- Groupes de travail dépendant du CRU <sup>1</sup>
- Etude la construction d'annuaires pour les établissements de l'enseignement supérieur
- Rédaction de recommandations
  - SupAnn v1 (2003)
  - SupAnn 2008
  - SupAnn 2009
- Construction d'un schéma d'annuaire spécifique normalisé
- [http ://www.cru.fr/documentation/supann/index](http://www.cru.fr/documentation/supann/index)

---

1. CRU : Comité Réseau des Universités intégré à Renater depuis juin 2011

# Objectifs de SupAnn

Objectifs et  
caractéris-  
tiques d'un  
annuaire

Protocole  
LDAP

Outils LDAP

- Cohérence dans la mise en oeuvre des annuaires des établissements d'enseignement supérieur
- Favoriser la portabilité des logiciels
- Aboutir à une homogénéité des contenus entre les établissements

# Progression

- 1 Objectifs et caractéristiques d'un annuaire
- 2 Protocole LDAP**
- 3 Outils LDAP



# Historique

## Norme X500

- Conçu par les opérateurs téléphoniques pour échanger leurs annuaires
- Construit sur le modèle réseau OSI
- Annuaire à grande échelle et distribué
- Elle définit
  - Les règles de nommage des objets et des entités
  - Les protocoles pour fournir le service d'annuaire
  - Un mécanisme d'authentification
- Implémentations lourdes, difficiles et buggés

- Création à l'Université du Michigan en 1993
  - Simplification du protocole DAP (X500)
  - Adaptation à TCP/IP
- Repris par l'IETF pour aboutir à la définition de plusieurs RFC en 1995
  - *Lightweight Directory Access Protocol* (RFC 1777)
  - *The String Representation of Standard Attribute Syntaxes* (RFC 1778)
  - *A String Representation of Distinguished Names* (RFC 1779)
- Apparition de LDAPv3 en 2002 avec la RFC 3377  
*Lightweight Directory Access Protocol (v3) : Technical Specification*

# Modèle d'information

Fournit les structures et les types de données

- Directory Information Tree (DIT) → Arbre d'information LDAP
- L'entrée, élément de base de l'annuaire
  - Instance d'une ou plusieurs classes d'objet (*objectClass*)
  - Attributs facultatifs ou obligatoires
  - Une ou plusieurs valeurs par attribut
- Schéma d'annuaire
  - Type de données des attributs
  - Règles de codage
  - Règles de comparaison

# Modèle de nommage

RDN et DN

Objectifs et  
caractéris-  
tiques d'un  
annuaire

Protocole  
LDAP

Outils LDAP

→ Comment référencer de façon unique les entrées et les données du DIT

## RDN : Relative Distinguished Name

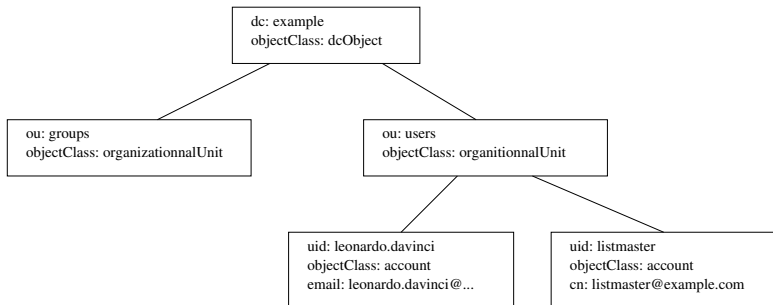
Attribut unique qui distingue une entrées des autres issues d'un même parent.

## DN : Distinguished Name

Identifie de façon unique les entrées de l'arbre. S'obtient par agrégation des RDN suivant le chemin de l'entrée voulue jusqu'à la racine.

# Modèle de nommage

## Exemple



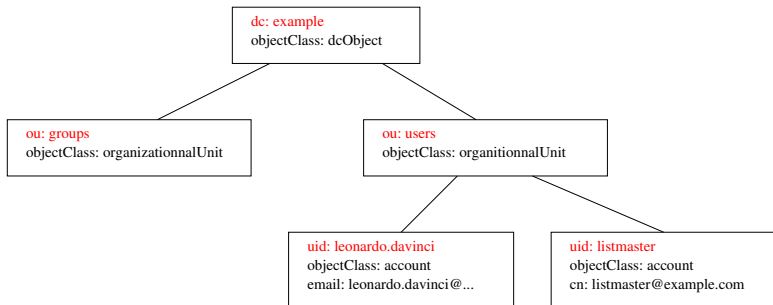
# Modèle de nommage

RDN

Objectifs et caractéristiques d'un annuaire

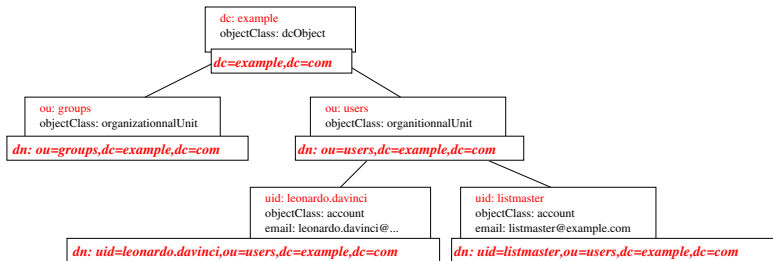
Protocole LDAP

Outils LDAP



# Modèle de nommage

DN



## Protocole d'accès à l'annuaire

- Mécanisme d'authentification
- Opérations sur les entrées
  - Recherche
  - Ajout
  - Suppression
  - Modification
  - ...



# Modèle de sécurité

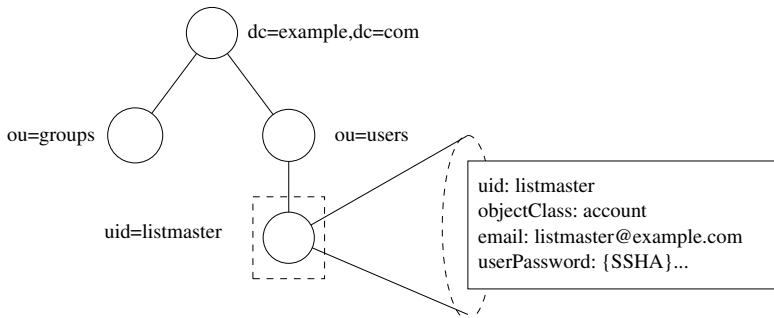
- Authentifier les clients (preuve d'identité)
- Contrôler l'accès aux données pour les clients authentifiés

# Objets LDAP

## Arbre

### *Directory Information Tree (DIT)*

- Classification hiérarchique des entrées
- Chaque noeud est une entrée de l'annuaire
- La racine de l'arbre caractérise l'annuaire (suffixe ou base LDAP)



# Objets LDAP

## Classe d'objet

- Détermine le type d'objet enregistré dans une entrée
- Définit les attributs de l'entrée
- Trois natures de classes :
  - Classe abstraite
  - Classe structurelle
  - Classe auxiliaire
- Une entrée peut instancier au plus une classe structurelle et plusieurs classes auxiliaires

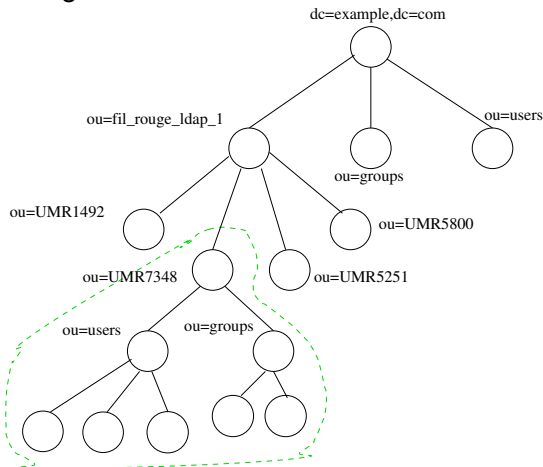
# Objets LDAP

## Une entrée, des attributs

- Modélise un objet stocké dans l'annuaire
- Les classes d'objet associées à l'entrée définissent ses attributs
- Attributs obligatoires ou facultatifs
- Attributs mono-valués (une seule valeur) ou multi-valués (plusieurs valeurs)

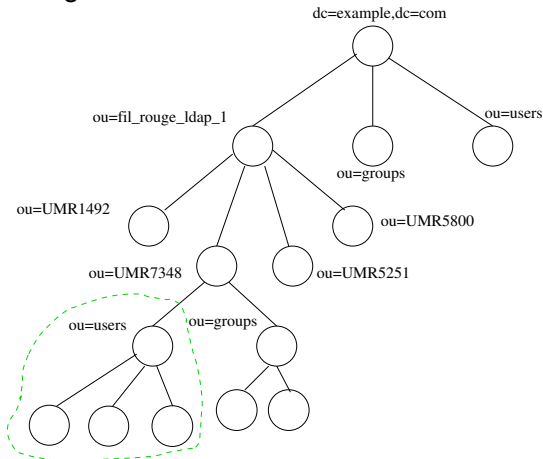
- 1 Etablissement de la connexion TCP (négociation SSL ou TLS)
- 2 Authentification (bind) avec un DN ou anonyme
- 3 Envoi de la requete par le client (opération de recherche, mise à jour...)
- 4 Envoi des résultats des la requête par le serveur au client (ensemble d'entrées)
- 5 Fermeture de la connexion

### Désigne le sous-arbre de l'annuaire à considérer



dn: ou=UMR7348,ou=fil\_rouge\_ldap\_1,dc=example,dc=com

### Désigne le sous-arbre de l'annuaire à considérer

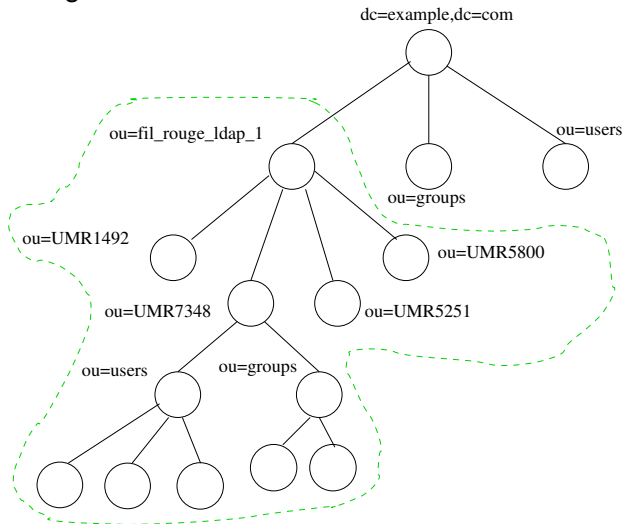


dn: ou=users,ou=UMR7348,ou=fil\_rouge\_ldap\_1,dc=example,dc=com

# Recherche

## Base de recherche

Désigne le sous-arbre de l'annuaire à considérer



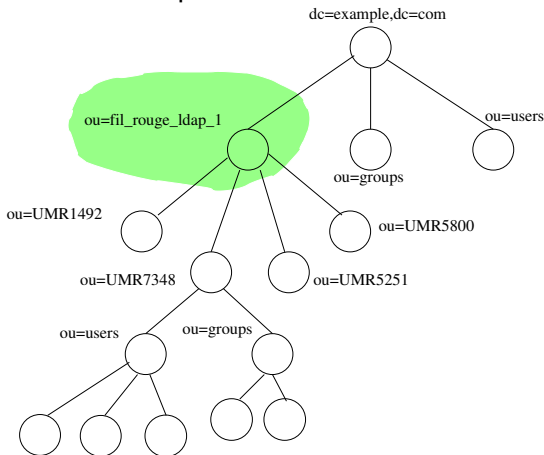
`dn: ou=fil_rouge_ldap_1,dc=example,dc=com`



# Portée de recherche

*base*

Détermine la profondeur de recherche dans le sous-arbre

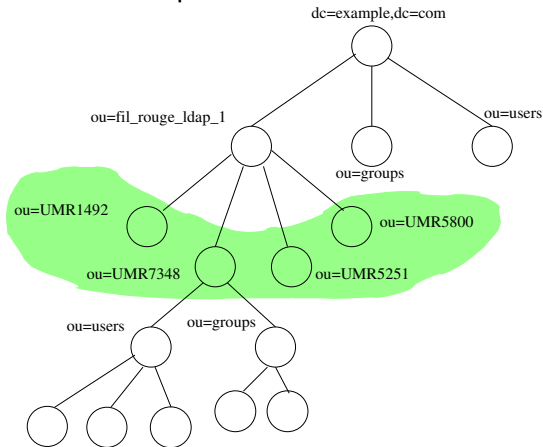


Base de recherche : ou=fil\_rouge\_ldap\_1,dc=example,dc=com

# Portée de recherche

*one*

Détermine la profondeur de recherche dans le sous-arbre

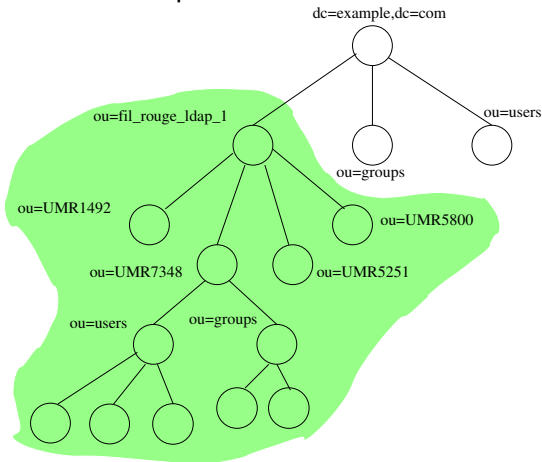


Base de recherche : ou=fil\_rouge\_ldap\_1,dc=example,dc=com

# Portée de recherche

*sub*

Détermine la profondeur de recherche dans le sous-arbre

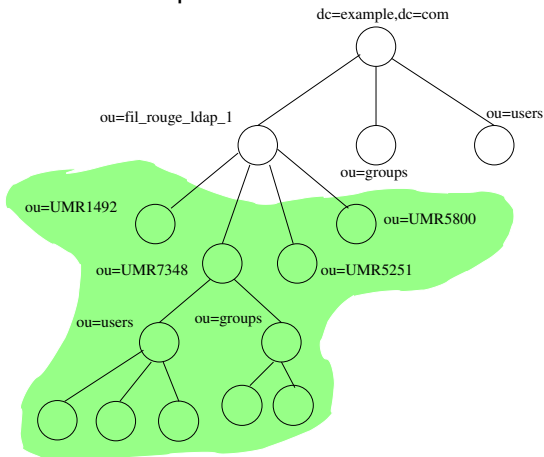


Base de recherche : ou=fil\_rouge\_ldap\_1,dc=example,dc=com

# Portée de recherche

*children*

Détermine la profondeur de recherche dans le sous-arbre



Base de recherche : `ou=fil_rouge_ldap_1,dc=example,dc=com`

## Filtre de recherche

- Chaque critère est de la forme (*attribut*<cmp>*valeur*)
- Les critères (<op><critère1><critère2>) s'assemblent avec des opérateurs logiques

Comparaison <cmp>	
=	Egalité
≈	Approximation
<=	Inférieur ou égal
>=	Supérieur ou égal

Op. logique <op>	
&	Et
	Ou
!	Négation

*Exemple : toutes les entrées  
(objectClass=\*)*

## Filtre de recherche

- Chaque critère est de la forme (*attribut*<cmp>*valeur*)
- Les critères (<op><critère1><critère2>) s'assemblent avec des opérateurs logiques

Comparaison <cmp>	
=	Egalité
≈	Approximation
<=	Inférieur ou égal
>=	Supérieur ou égal

Op. logique <op>	
&	Et
	Ou
!	Négation

*Exemple : les entrées de comptes POSIX avec une adresse mail*

*( & ( objectClass=posixAccount ) ( mail=\* ) )*

## Filtre de recherche

- Chaque critère est de la forme (*attribut*<cmp>*valeur*)
- Les critères (<op><critère1><critère2>) s'assemblent avec des opérateurs logiques

Comparaison <cmp>	
=	Egalité
≈	Approximation
<=	Inférieur ou égal
>=	Supérieur ou égal

Op. logique <op>	
&	Et
	Ou
!	Négation

*Exemple : les entrées dont le nom complet (cn) commence par M ou T*  
( | (cn=M\*) (cn=T\*) )

## Filtre de recherche

- Chaque critère est de la forme (*attribut*<cmp>*valeur*)
- Les critères (<op><critère1><critère2>) s'assemblent avec des opérateurs logiques

Comparaison <cmp>	
=	Egalité
≈	Approximation
<=	Inférieur ou égal
>=	Supérieur ou égal

Op. logique <op>	
&	Et
	Ou
!	Négation

*Exemple : les entrées dont le prénom ne contient pas ben*  
( ! ( givenName=\*ben\* ) )



# LDIF

- Fichier texte (utf-8) pour l'échange d'entrées LDAP
- Ligne de commentaire commence par #
- Les entrées sont séparées par une ligne vide
- Chaque ligne représente un attribut avec sa valeur
- Un attribut peut s'écrire sur plusieurs lignes à condition qu'elles commencent par un et un seul espace

```
dn: ou=people , dc=example , dc=com  
ou: people  
objectClass: organizationalUnit
```

```
dn: ou=groups , dc=example , dc=com  
ou: groups  
objectClass: organizationalUnit
```

# Opérations sur les entrées

Ajout

```
dn: cn=user.no_1,ou=users,ou=UMR7348,  
    ou=fil_rouge_ldap_1,dc=example,dc=com  
changetype: add  
objectClass: organizationalPerson  
objectClass: person  
objectClass: inetOrgPerson  
cn: user.no_1  
sn: user.no_1  
mail: user.no_1@example.com  
uid: user.no_1  
userPassword: {SSHA}LeHashDuPassword
```

# Opérations sur les entrées

## Suppression

```
dn: cn=user.no_1,ou=users,ou=UMR7348,  
ou=fil_rouge_ldap_1,dc=example,dc=com  
changetype: delete
```

# Opérations sur les attributs

Ajout

Objectifs et  
caractéris-  
tiques d'un  
annuaire

Protocole  
LDAP

Outils LDAP

```
dn: cn=user.no_1,ou=users,ou=UMR7348,  
ou=fil_rouge_ldap_1,dc=example,dc=com  
changetype: modify  
add: telephoneNumber  
telephoneNumber: +33 5 49 49 49 49
```

# Opérations sur les attributs

Modification

Objectifs et  
caractéris-  
tiques d'un  
annuaire

Protocole  
LDAP

Outils LDAP

```
dn: cn=user.no_1,ou=users,ou=UMR7348,  
ou=fil_rouge_ldap_1,dc=example,dc=com  
changetype: modify  
replace: telephoneNumber  
telephoneNumber: +33 5 94 94 94 94
```

# Opérations sur les attributs

## Suppression

```
dn: cn=user.no_1,ou=users,ou=UMR7348,  
ou=fil_rouge_ldap_1,dc=example,dc=com  
changetype: modify  
delete: telephoneNumber
```

# Progression

- 1 Objectifs et caractéristiques d'un annuaire
- 2 Protocole LDAP
- 3 Outils LDAP**

# Coté serveur

- OpenLDAP (slapd)
- Apache Directory Server



## Coté client

- Comandes OpenLDAP pour interagir avec l'annuaire
  - *ldapadd*
  - *ldapmodify*
  - *ldapsearch*
  - ...
- Bibliothèque dynamique cliente configurable via */etc/ldap/ldap.conf*
- LdapVI
- GQ
- Apache Directory Studio

# Méthode d'authentification

- Anonyme
- Simple → Identifiant + Mot de passe
- SASL / GSSAPI → Kerberos

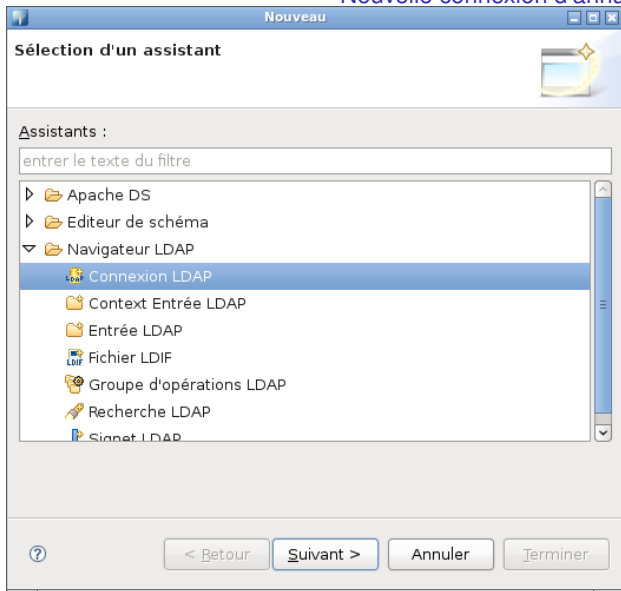
# Apache Directory Studio

## Nouvelle connexion d'annuaire

Objectifs et caractéristiques d'un annuaire

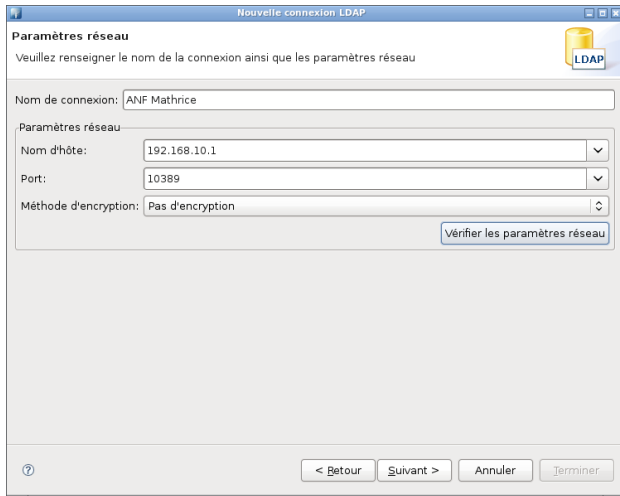
Protocole LDAP

Outils LDAP



# Apache Directory Studio

## Nouvelle connexion d'annuaire



Nouvelle connexion LDAP

**Paramètres réseau**

Veillez renseigner le nom de la connexion ainsi que les paramètres réseau

Nom de connexion: ANF Mathrice

Paramètres réseau

Nom d'hôte: 192.168.10.1

Port: 10389

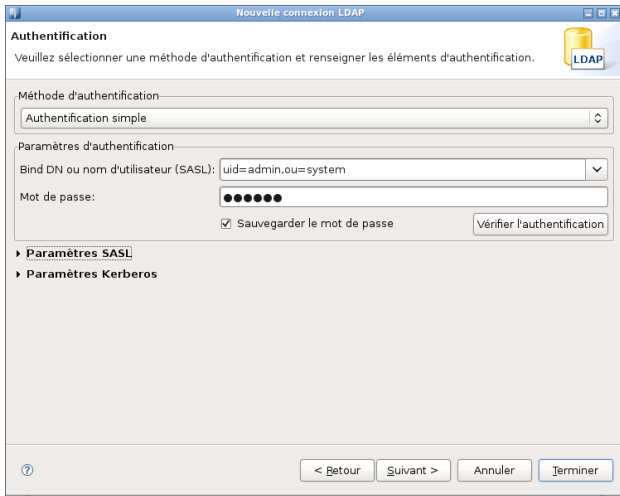
Méthode d'encryption: Pas d'encryption

Vérifier les paramètres réseau

< Retour Suivant > Annuler Terminer

# Apache Directory Studio

## Nouvelle connexion d'annuaire



Nouvelle connexion LDAP

### Authentification

Veuillez sélectionner une méthode d'authentification et renseigner les éléments d'authentification.

Méthode d'authentification: Authentification simple

Paramètres d'authentification

Bind DN ou nom d'utilisateur (SASL): uid=admin,ou=system

Mot de passe: ●●●●●●

Sauvegarder le mot de passe

Vérifier l'authentification

► Paramètres SASL

► Paramètres Kerberos

< Retour Suivant > Annuler Terminer

# Apache Directory Studio

## Nouvelle connexion d'annuaire

Nouvelle connexion LDAP

**Options du navigateur**

Vous pouvez spécifier des paramètres de connexion additionnels

DN de base

Obtenir les DN de base depuis la Root DSE. Récupérer les DN de base

DN de base:

Limites

Limite quantitative:

Limite temporelle (s):

Déréférencement d'alias

En trouvant le DN de base

Recherche

Gestion des références

Suivre les références manuellement

Suivre les références automatiquement

Ignorer les références

Controls

Utiliser le control ManageDsaIT durant la navigation

Récupérer les sous-entrées au cours de la navigation (nécessite une requête de recherche supplémentaire)

Recherche paginée Taille de page:   Mode de défilement

Fonctionnalités

Récupérer les attributs opérationnels au cours de la navigation

? < Retour Suivant > Annuler Terminer

# Apache Directory Studio

## Nouvelle connexion d'annuaire

Objectifs et caractéristiques d'un annuaire

Protocole LDAP

Outils LDAP

Nouvelle connexion LDAP

**Options d'édition**

Vous pouvez spécifier des paramètres pour l'édition des entrées.

Modification d'entrée

Mode de modification:	Opérations de modification optimisées
Mode de modification (sans règle de comparaison d'égalité):	Opérations de modification optimisées
Ordre de modification:	DELETE en premier

< Retour   Suivant >   Annuler   Terminer

# Apache Directory Studio

## Fenêtre principale

The screenshot displays the Apache Directory Studio interface with the following components:

- Titre de la fenêtre:** LDAP - uid=leonardo.davinci,ou=users,dc=example,dc=com - ANF Mathrice - Apache Directory Studio
- Menu:** Fichier, Edition, Navigation, LDAP, Fenêtre, Aide
- Navigateur LDAP (Gauche):**
  - Root DSE (4)
    - dc=example,dc=com (4)
      - ou=fil\_rouge\_ldap\_1
      - ou=fil\_rouge\_ldap\_2
      - ou=groups
      - ou=users (3)
        - uid=david.delavennat
        - uid=leonardo.davinci (sélectionné)
        - uid=listmaster
      - ou=schema
      - ou=system
    - Recherches
    - Signets

- Zone principale (Centre):**
- DN: uid=leonardo.davinci,ou=users,dc=example,dc=com
- Description d'attribut | Valeur
- objectClass | account (structural)
- objectClass | extensibleObject (auxiliary)
- objectClass | top (abstract)
- uid | leonardo.davinci
- email | leonardo.davinci@example.com
- userPassword | SSHA mot de passe haché
- Structure (Droite):**
- uid=leonardo.davinci
  - uid (1)
  - email (1)
  - userPassword (1)
  - objectClass (3)
- Connexions (Bas Gauche):**
- ANF Mathrice (sélectionné)
- LMA - Admin (LDAPS)
- LMA - Anonyme (LDAPS)
- Logs de modifications / Logs de recherches (Bas Centre):**

```
#! CONNECTION ldap://192.168.10.1:10389
#! DATE 2012-05-22T17:02:13.581
#! numEntries : 3
```
- Progress (Bas Droite):** Aucune opération à afficher