Annuaires LDAP

Manche Open School

Paul Lecuq

18 juillet 2016

LDAP : Sommaire

- Concepts
- Historique
- Fonctionnement
- Modèle
- Fichiers et exploitation

LDAP : Concepts

- Lightweight Directory Access Protocol
- Définition d'un annuaire
  - Stockage d'informations de type base de données
  - Dédié à la consultation plus qu'à la modification
  - Recherche des données par critères

LDAP : Concepts

- Protocole d'accès et couche réseau applicative
- Modèle de distribution et de duplication
- Contenu évolutif

LDAP : Historique

- Basé sur X.500 de l'UIT
- Ce standard était conçu historiquement l'interconnexion d'annuaires téléphonique d'opérateurs
- X.500 était peu performant et très complexe

LDAP : Historique

- LDAP a été conçu pour être compatible avec Internet
- Utilisation de TCP/IP
- Normalisé par l'IETF (RFC 2251)
- Implémentations libres et propriétaires

LDAP : Historique

Implémentations libres

- OpenLDAP
- 389 Directory Server (Red Hat)
- OpenBSD ldapd
- Apache Directory

LDAP : Historique

Implémentations propriétaires

- Novell Directory Server
- Microsoft Active Directory
- Apple OpenDirectory (basé en partie sur OpenLDAP)
- Red Hat Directory Server

LDAP : Fonctionnement

- Le protocole décrit comment se déroulent les connexions clients-serveur (binding)
- Les connexions serveur-serveur (réplication des données et délégations)
- Description du transport des données
- Chiffrement et accès aux données (authentification)
- Opérations sur l'arbre (add, search, delete)

LDAP : Modèle

- Une entrée
  - Un annuaire LDAP comporte plusieurs entrées (élément de base d'un annuaire LDAP)
  - Ces entrées sont sujettes à une convention décrites par les classes d'objets
  - Attributs obligatoires ou optionnels (exemple avec posixAccount)

LDAP : Modèle

- Schéma LDAP : exemple avec nis.schema

```
attributetype ( 1.3.6.1.1.1.1.0 NAME 'uidNumber'
    DESC 'An integer uniquely identifying a user in an administrative
domain'
    EQUALITY integerMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
...
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
        DESC 'Abstraction of an account with POSIX attributes'
        SUP top AUXILIARY
        MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
        MAY ( userPassword $ loginShell $ gecos $ description ) )
```

LDAP : Modèle

attributetype

NAME : Nom de l'attribut

DESC : Description

EQUALITY : Type de donnée

SYNTAX : OID définie identifiant l'attribut (OID privée pour utilisation spécifiques et non-standards)

objectclass

SUP : définit la classe d'objet parente de la classe d'objet

MUST : attributs obligatoires

MAY : attributs facultatifs

LDAP : Modèle

- Un schéma
  - Ensemble de définitions de données
  - Décrit la syntaxe, le type des attributs d'une classe d'objets
  - Vérification de la conformité de la donnée insérée
  - Nativement, le protocole LDAP par ses schémas va vérifier la cohérence et l'intégrité des données qui y sont ajoutées (différent de SQL)

LDAP : Modèle

- Attributs

type	valeur
cn	FactorFX
uid	factorfx
telephoneNumber	0800 623 120
mail	informatique@factorfx.com

LDAP : Modèle

- La classe d'objet
  - Identifie quels attributs sont obligatoires ou optionnels
  - Structurelle : description des objets
  - Auxiliaire : permet l'ajout d'informations
  - Abstraite : objet basique du protocole LDAP

LDAP : Modèle

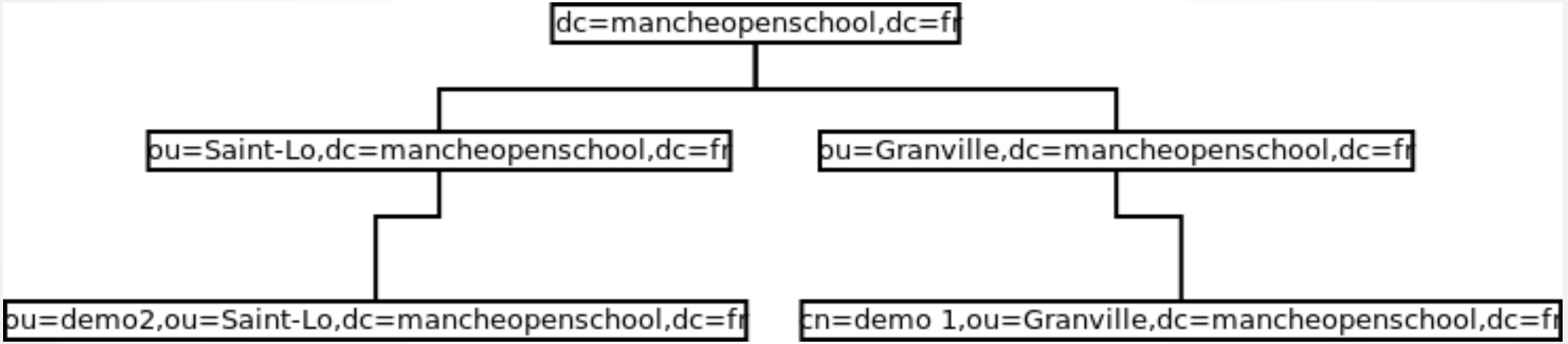
- Classe d'objet
  - Dans une optique d’interopérabilité, certaines classes ont été standardisées par l'IETF
  - Exemples avec les organisations et les unités organisationnelles
  - o : Organization
  - ou : Organizational Unit

LDAP : Modèle

- DIT (Directory Information Tree)
  - Les entrées ont toutes un nom et chaque entrée doit être unique
  - Organisation sous forme d'arbre
- Nommage hiérarchique
  - Nom complet depuis la racine de l'arbre (DN)
  - Nom relatif (RDN)

LDAP : Modèle

- Arborescence LDAP



LDAP : Modèle

- Accès aux données
  - Opérations d'interrogation (ldapsearch)
  - Opérations de comparaison (ldapsearch)
  - Opérations de mise à jour (ldapmodify)
  - Opérations d'authentification et de contrôle (SASL ou Kerberos)

LDAP : Modèle

- Interrogation
  - Pour connaître les attributs d'un objet, il est impératif d'effectuer une requête
  - Sur un scope (partie de l'arbre telle que base, subtree, one)
  - Sur un filtre testant la valeur d'un attribut

LDAP : Modèle

- Interrogation
  - (uid=*)
  - Retourne tous les utilisateurs de l'arbre
  - (uidNumber>500)
  - Retourne les utilisateurs dont l'identifiant utilisateur est supérieur à 500

LDAP : Modèle

- Scope
  - base : interrogation uniquement sur le DN indiqué
  - subtree : interrogation récursive sur le DN indiqué
  - one : interrogation sur le premier niveau enfant du DN

LDAP : Fichiers

- Présentation d'un fichier LDIF (Lightweight Directory Interchange Format)
- Présentation d'un fichier de schéma
- Présentation d'OpenLDAP

LDAP : Exploitation

- Présentation des commandes ldap
- Présentation d'outils d'exploitation (JXPlorer, console Active Directory)
- Références utiles

LDAP : Démos

- Présentation d'OpenLDAP
- Présentation de domaine Active Directory avec Samba 4
- Administration d'un domaine Active Directory
- Présentation d'application dont l'authentification ou la base d'utilisateur fonctionne avec LDAP

LDAP

Questions