

# TP: Authentification LDAP sous GNU/Linux

Benoit Métrot

Rencontres Mathrice - Mars 2008

# Plan

- 1 Environnement expérimental
- 2 Le protocole LDAP

# Logiciels installés

- Distribution Ubuntu 7.10
- VirtualBox 1.5.0
  - Trois machines virtuelles sous Debian Etch
  - Réseau privé virtuel en 192.168.1.0/24
  - Isolé du réseau physique de la salle
  - Configuration par SSH/SCP ou via la console VirtualBox
- Identifiants : `tpldap / mathrice`

# Machines virtuelles

## Master :

- IP : 192.168.1.2
- Role : Serveur LDAP principal

# Machines virtuelles

## Master :

- IP : 192.168.1.2
- Role : Serveur LDAP principal

## Replica :

- IP : 192.168.1.3
- Role : Replica du serveur LDAP principal

# Machines virtuelles

## Master :

- IP : 192.168.1.2
- Role : Serveur LDAP principal

## Replica :

- IP : 192.168.1.3
- Role : Replica du serveur LDAP principal

## Client :

- IP : 192.168.1.4
- Role : Tester l'authentification LDAP

# VirtualBox OSE

The screenshot shows the VirtualBox OSE application window. The title bar reads "VirtualBox OSE". The menu bar includes "Fichier", "Machine", and "Aide". The toolbar contains icons for "Nouveau", "Préférences", "Supprimer", "Lancer", and "Rejeter".

On the left, a list of machines is shown:

- Client** (LINUX) - Eteint
- Master** (LINUX) - Eteint (highlighted)
- Replica** (LINUX) - Eteint

The right pane shows the "Général" settings for the selected machine:

Propriété	Valeur
<b>Nom</b>	Master
<b>Système</b>	Linux 2.6
<b>Mémoire de base</b>	256 Mo
<b>Mémoire vive vidéo</b>	8 Mo
<b>Ordre d'amorçage</b>	Disque dur, CD/DVD-ROM
<b>ACPI</b>	Activé
<b>IO APIC</b>	Désactivé
<b>Disque dur</b>	
Primaire Maître	Master.vdi [Normal, 8,00 GB]
<b>CD/DVD-ROM</b>	
Image	debian-40r3-i386-CD-1.iso
<b>Disquette</b>	
Non installée	
<b>Audio</b>	
Désactivé	
<b>Réseau</b>	
Adaptateur 0	tap0
<b>Serial Ports</b>	
Désactivé	
<b>Répertoires partagés</b>	
Rien	

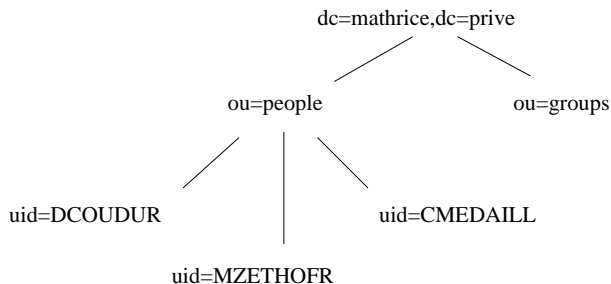
# Plan

- 1 Environnement expérimental
- 2 Le protocole LDAP

# Un service d'annuaire

- Alternative légère à la norme X.500
- Conçu à l'université du Michigan en 1993
- Repris ensuite par l'IETF
- Défini par un ensemble de RFC dont :
  - RFC-3377 *Lightweight Directory Access Protocol(v3) : Technical specification*
  - RFC-2829 *Authentication methods for LDAP*
  - RFC-2830 *Lightweight Directory Access Protocol(v3) : Extension for Transport Security Layer*

# Représentation de l'annuaire



Chaque nœud de l'arbre correspond à une entrée de l'annuaire

# Definitions (1)

## Entrée

Une entrée est un élément de l'annuaire. Elle représente une personne, un ordinateur, un groupe, un nom de machine.

## Attributs

Une entrée est composée d'attribut. Un attribut est un champ d'information. Il représente un numéro de téléphone, un nom, un mot de passe, un numéro d'utilisateur.

## Classe d'objet

Chaque entrée possède une classe d'objet (objectClass). Cela définit ce que va représenter l'entrée.

## Définitions (2)

### Schema

Le schéma définit les relations entre les classes d'objet et les attributs. Il précise les attributs obligatoires ou facultatifs pour chaque classe.

### DIT

C'est l'arbre d'information d'annuaire LDAP ou la représentation des entrées et des relations entre elles.

### LDIF

C'est un format de fichier texte, défini dans la RFC 2849, pour le stockage d'informations contenus dans un annuaire LDAP.

## Exemple d'entrée

```
dn: uid=HDUPANNI,ou=people ,dc=mathrice ,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Hans.Dupannier
sn: Dupannier
uid: HDUPANNI
uidNumber: 1012
gidNumber: 300
homeDirectory: /home/hdupanni
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Hans.Dupannier@domain.tld
mail: HDUPANNI
```

# DN et RDN

DN :

- Nom distinctif
- Identifie une entrée de l'annuaire de manière absolue
- Concaténation des RDN de toutes les entrées entre l'élément considéré et la racine de l'arbre
- Exemple :  
*uid=HDUPANNI,ou=people,dc=mathrice,dc=prive*

RDN :

- Nom distinctif relatif
- Identifie l'entrée par rapport au sein d'une partie de l'arbre
- Exemple : *uid=HDUPANI*

# Un protocole d'échange d'informations

- Modèle client/serveur en mode connecté
- Repose sur des messages
- Identification avec un DN
- Authentification
  - Anonyme → DN et mot de passe vide
  - Simple → mot de passe stocké dans l'annuaire
  - SASL → S/Key, GSSAPI, Kerberos
- Chiffrement des échanges avec TLS/SSL

# OpenLDAP

Implémentation GPL de LDAP incluant :

- Le serveur (slapd)
- Mécanismes de réplication (slurpd, syncrepl)
- Backends de stockage de l'information
- Overlay
- Clients LDAP : `ldapsearch`, `ldapadd`, `ldapdelete`...