Version : **2021.01**

Dernière mise-à-jour : 2021/02/03 14:29

SER701 - Présentation, Installation et Activation d'OpenLDAP

Contenu du Module

Présentation

Qu’est-ce que LDAP ?

LDAP est une abbréviation de **L**ightweight **D**irectory **A**ccess **P**rotocol. Comme son nom indique, LDAP est un service d'**annuaire**.

Un service d'annuaire est une base de données spécialisée optimisée pour la consultation. Certains services d'annuaire peuvent être locaux tandis que d'autres sont appellés **distribués**. Un bon exemple d'une service d'annuaire distribué est le **DNS**.

Plusieurs points sont à retenir :

- LDAP est un adaptation TCP/IP du protocole **DAP** (**D**irectory **A**ccess **P**rotocol),
- LDAP et DAP sont des protocoles d'interrogation des annuaires au format **X.500**,
- LDAP utilise TCP/IP au lieu de parcourir les sept couches du modèle OSI, d'où la notion de **Lighweight**,
- LDAP emploie une approche client/serveur en mode connecté sur le port **389/tcp**,
- LDAPS emploie une approche client/serveur sécurisée via SSL en mode connecté sur le port **636/tcp**. Il utilise aussi **TLS** et **SASL**,
- LDAP utilise le codage **B**asic **E**ncoding **R**ule au lieu d'ASCII. Cette approche consiste en un codage en hexadécimal d'un code en décimal correspondant à une action spécifique. Par exemple, l'opération **Search Request** correspond au code **63**,
- LDAP prévoit la **réplication** des données :
    - La réplication **Maître > Esclave** appelée **push-based** ou encore **SIR** (**S**erver **I**nitiated **R**eplication),
    - La réplication **Esclave > Maître** appelée **pull-based** ou encore **CIR** (**C**onsumer **I**nitiated **R**eplication),

Le Protocole X.500

X.500 est un ensemble de normes qui s'appuie sur le modèle **OSI** :

- **X.509** - mécanismes d'authentification par clefs publiques,
- **X.511** - services offerts par X.500 tels les recherches et les modifications,
- **X.519** - protocoles de communication, y compris le **DAP**, entre deux serveurs X.500 et entre un client et serveur X.500.

LDAP v3

LDAP est actuellement à la version **3**. Cette version est notamment définie par :

- **RFC 4510** - LDAP: Technical Specification Road Map qui remplace le **RFC3377**,
- **RFC 4511** - LDAP: Authentification Methods and Security Mechanisms qui remplace les RFC **RFC 2829** et **RFC 2830**,

Comment fonctionne LDAP ?

Le protocole LDAP définit neuf opérations divisées en trois catégories :

- **Accès à l'annuaire** - bind, unbind, abandon,
- **Interrogation** - search, compare,
- **Mise à jour** - add, delete, modify, modifyDN.

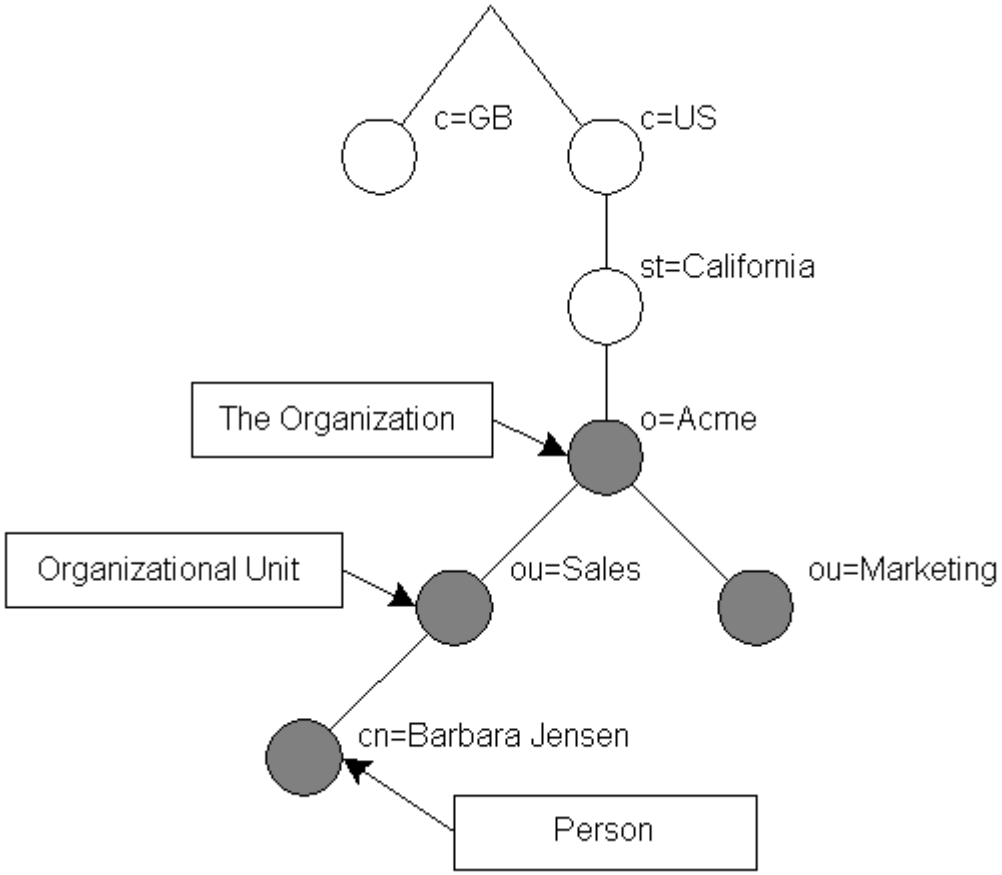
Le Modèle d'Information de LDAP

Le modèle d'information de LDAP est basé sur des **entrées** :

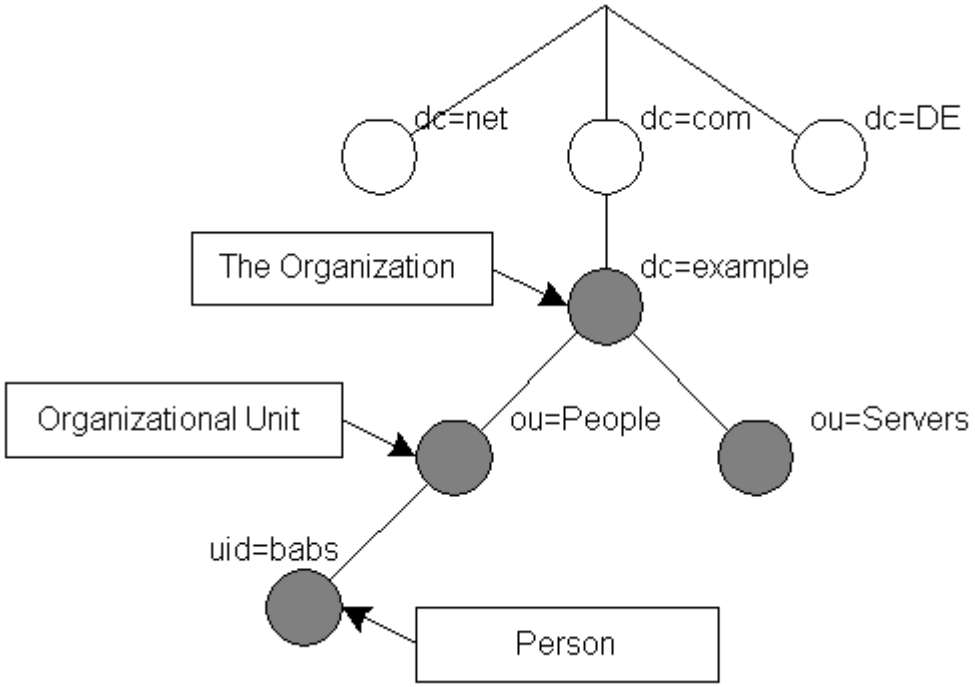
- L'ensemble des entrées est contenu dans un **DIT** (**D**irectory **I**nformation **T**ree),
- Chaque entrée représente une instance d'une **classe** d'objets contenant une collection d'**attributs** qui possède un nom unique appelé le **D**istinguished **N**ame et un nom relatif appelé le **R**elative **D**istinguished **N**ame.

Deux structures classiques des entrées sont :

- l'organisation géographique



- l'organisation Internet



Les DN et les RDN

Un DN est l'ensemble des RDN des noeuds supérieurs :

- cn=hugh norris,ou=formation,dc=i2tch,dc=com

Un RDN est un couple composé d'un attribut et un valeur, par exemple :

- mail=info@i2tch.com

Dans le cas de plusieurs couples, ceux-ci sont séparés par le caractère **+** :

- mail=info@i2tch.com+cn=info

Le format des valeurs de attributs ne doit **pas** contenir :

- Le caractère **#** ou un espace au début de la chaîne,
- Un espace à la fin de la chaîne.

En plus des ces restrictions, les caractères suivants doivent être protégés par le caractère **** :

- ,
- +
- “
- \
- <
- >
- ;

La Structure d’un annuaire LDAP

Les Attributs

Un attribut est défini par un ensemble d'informations :

- Un ou plusieurs noms,
- Des règles de comparaison telles EQUALITY, ORDERING, SUBSTR,
- Une syntaxe définie par un OID,
- Un indicateur de multivaluation tel SINGLE-VALUE,
- Un indicateur de modification par l'utilisateur tel NO-USER-MODIFICATION,
- Un indicateur d'usage USAGE qui indique le type de l'attribut soit utilisateur ou opérationnel.

Les Attributs Utilisateur

Ce sont des attributs pouvant être modifiés par des utilisateurs ayant le droit d'écriture.

Les Attributs Opérationnels

Ce sont de attributs stockant les information sur le statut de l'annuaire.

Les Classes d'Objets

Une classe d'objets est définie par :

- Un OID,
- Un nom,
- Une hiérarchie de classes supérieurs,
- Un type, soit Abstract, Structural ou Auxiliary,
- Une liste d'attributs obligatoires,
- Une liste d'attributs facultatifs.

Les Types de Classe d'Objets

Le type de classe d'objets peut être :

- **Abstract** - une classe abstraite dont d'autres classes vont pouvoir hériter,
- **Structural** - un objet **réel**. Chaque entrée de l'annuaire n'a qu'une seule classe d'objets structurelle,
- **Auxiliary** - une classe d'objets auxiliaire qui sert à compléter un objet structurel :
  - **extensibleObject** - ne contenant aucun attribut obligatoire, elle contient en tant qu'attributs facultatifs tous les attributs définis dans le schéma de l'annuaire,
  - **subschema** - ne contenant aucun attribut obligatoire, elle contient l'ensemble des classes d'objets de l'annuaire, les règles de comparaison, les attributs et les syntaxes.

Les OID

Chaque attribut et chaque classe d'objets est décrit par un OID (**O**ject **ID**entifier) :

- Les OID sont attibués par IANA (**I**nternet **A**ssigned **N**umbers **A**uthority),
- LDAP contient les OID suivants :
    - 2.5.4 - attributs utilisateurs,
    - 2.5.18 - attributs opérationnels,
    - 1.3.6.1.4.1.1466.115.121.1 - syntaxe des attributs,
    - 2.5.6 - classes d'objets.

Les Schémas de l'Annuaire

Un **schéma** regroupe les informations suivantes :

- Les classes d'objets,
- Les attributs,
- La syntaxe des attributs,
- Les règles de comparaison.

Un schéma **doit** contenir au moins une classe d'objets.

Les schémas les plus utilisés sont :

Schéma	**Description**
core.schema	**Obligatoire**. Permet de stocker dans l'annuaire les Common Attribute Object Classes. C'est le noyau OpenLDAP.
cosine.schema	**Utile** - Permet le support des annuaires **cosine** et X.500.
inetorgperson.schema	**Utile** - Permet de stocker dans l'annuaire les informations concernant les personnes.
bind.schema	Permet de stocker dans l'annuaire des objets DNS.
dhcp.schema	Permet de stocker dans l'annuaire des objets DHCP.
nis.scema	Permet de stocker dans l'annuaire les utilisateurs UNIX et les paramètres associés.
samba3.schema	Permet l'intégration de samba et LDAP.
cobra.schema	Permet de stocker dans l'annuaire des objets **COBRA** (**C**ommon **O**bject **B**roker **R**equest **A**rchitecture).
openldap.schema	**Expérimental**. Concerne le projet OpenLDAP Project.
dyngroup.schema	**Expérimental**. Dynamic Group - utilisé avec le Netscape Enterprise Server.
collective.schema	**Expérimental**. Permet de stocker dans l'annuaire des objets collectifs.

Schéma	Description
java.schema	**Expérimental**. Permet de stocker dans l'annuaire des objets java.
misc.schema	**Expérimental**. Permet le routage des messages électroniques (emails).
ppolicy.schema	**Expérimental**. Schéma de stratégie de mots de passe.

LAB #1 - Installation et Activation du serveur OpenLDAP sous CentOS 7

Avant d'installer OpenLDAP, passez SELinux en mode permissive :

```
[root@centos7 ~]# setenforce permissive
[root@centos7 ~]# vi /etc/sysconfig/selinux
[root@centos7 ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Ensuite désactivez le pare feu firewalld :

```
[root@centos7 ~]# systemctl stop firewalld
[root@centos7 ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service.
[root@centos7 ~]# systemctl status firewalld
```

```
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)

Jan 10 08:25:43 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 10 08:25:44 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Jan 10 12:15:48 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Jan 10 12:15:48 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Pour installer le serveur OpenLDAP sous GNU/Linux ou Unix vous pouvez soit utiliser la version binaire fournie par les dépôts de paquets de votre distribution GNU/Linux ou Unix soit télécharger la dernière version à compiler du site d'OpenLDAP.

Dans notre cas, nous allons installer OpenLDAP à partir des dépôts sur un système RHEL / CentOS. Commencez par mettre à jour le système :

```
[trainee@centos7 ~]$ su -
Mot de passe : fenestros
[root@centos7 ~]# yum update
...
[root@centos7 ~]# reboot
```

Puis installez OpenLDAP :

```
[root@centos7 ~]# yum install openldap-servers openldap-clients openldap
```

Sous RHEL / CentOS le service OpenLDAP s'appelle **slapd**. Une vérification de son état démontre qi'il n'est pas activé :

```
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
```

```
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
```

Il convient donc d'activer le service **sans** le démarrer :

```
[root@centos7 ~]# systemctl enable slapd
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to
/usr/lib/systemd/system/slapd.service.
[root@centos7 ~]# systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
```

<html>

</html>