R304
Gestion d'annuaires
Travaux pratiques

Sami Evangelista

IUT de Villetaneuse

Département Réseaux et Télécommunications

2025–2026

http://www.lipn.univ-paris13.fr/~evangelista/cours/R304

Table des matières

Sources des images utilisées dans ce document:

http://www-lipn.univ-paris13.fr/~evangelista/cours/credits.html

Remerciements Je remercie les collègues suivants, qui ont écrit des travaux pratiques ou supports de cours qui m'ont grandement aidé dans la rédaction de ce document.

— Christian Bulfone
`https://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASHS-DCISS/PDF/TP_LDAP.pdf`
— Guillaume Urvoy-Keller
`https://webusers.i3s.unice.fr/~urvoy/docs/R304/ldap.pdf`
— Micaela Mayero et Franck Butelle
`https://www-lipn.univ-paris13.fr/~butelle/`
— Xavier Monnin et Marisol Rodriguez
`https://lipn.fr/~monnin/Enseignement/ServicesAnnuaires/`

TP 1 — LDAP : introduction

Dans ce TP nous allons configurer un serveur LDAP avec une hiérarchie d'utilisateurs, ainsi qu'un poste client qui interrogera ce serveur. On utilisera le serveur LDAP *slapd* (Stand-alone LDAP Daemon).

Le TP est à réaliser avec marionnet.

Exercice 1 — Travail introductif

On travaillera sur un réseau de deux ordinateurs (ldap et client) connectés par un switch.

I 1.1 Créez le réseau et ajoutez les équipements.
I 1.2 Ouvrez une session root sur chaque hôte.
I 1.3 Attribuez aux hôtes des adresses dans le réseau 10.0.0.0/24 et activez leurs interfaces.
I 1.4 Vérifiez que les messages ping passent bien entre les hôtes.

Nous allons relancer la configuration initiale du paquet slapd pour initialiser notre annuaire. Les deux instructions suivantes doivent être suivies sur ldap.

I 1.5 Lancez la reconfiguration du paquet slapd :

```
$ dpkg-reconfigure slapd
```

Entrez les informations suivantes :
— *Omit OpenLDAP server configuration ?* → No
— *DNS domain name :* → `iutv.edu`
— *Organization name :* → `IUT de Villetaneuse`
— *Administrator password :* → `truc`
— *Database backend to use :* → HDB
— *Do you want the database to be removed when slapd is purged ?* → No
— *Move old database ?* → Yes
— *Allow LDAPv2 protocol ?* → Yes

I 1.6 Affichez le contenu de l'annuaire :

```
$ slapcat
```

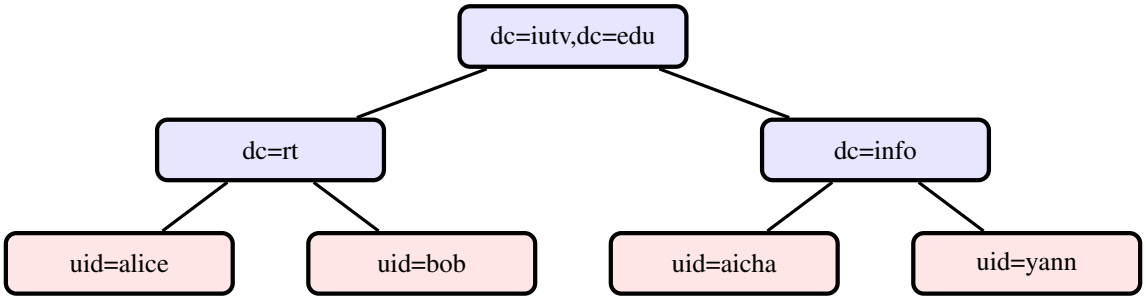
L'annuaire devrait contenir deux objets :
— la racine de votre annuaire, identifiée par le DN `dc=iutv,dc=edu` ;
— et un objet `cn=admin,dc=iutv,dc=edu` de la classe `simpleSecurityObject` qui représente un compte administrateur permettant de modifier le contenu de l'annuaire.

Vous verrez que le serveur a rajouté des attributs aux objets créés, comme leurs dates de création ou les classes structurelles auxquels ils appartiennent.

Q 1.1 Dans quel attribut trouve-t-on l'information `IUT de Villetaneuse` ?
Q 1.2 Même question pour `iutv`.

Exercice 2 — Création de l'annuaire

Le schéma de l'annuaire que l'on souhaite mettre en place est le suivant :



— Les nœuds dc=rt et dc=info représentent les domaines rt.iutv.edu et info.iutv.edu respectivement. Ils ont pour classes : top, dcObject et organization.
— Les nœuds uid=aicha, uid=alice, uid=bob et uid=yann représentent quatre utilisateurs répartis sur ces deux domaines. Ils ont pour classes : top, person, organizationalPerson et inetOrgPerson.

Toutes les instructions de cet exercice doivent être suivies sur ldap.

I 2.1 Éditez un fichier iutv.ldif contenant la description des 6 nouveaux objets de notre annuaire (i.e., tous ceux de la figure, sauf dc=iutv,dc=edu qui a été créé à l'exercice précédent). Vous devrez, pour chaque objet, définir ses attributs obligatoires (selon ses classes, voir pages 15–16 du cours). Vous définirez également les attributs optionnels permettant de représenter les informations suivantes :
— un numéro de téléphone pour Alice et Yann
— une adresse mail pour Alice et Aicha

Remarques :
— N'entrez aucun caractère accentué dans votre fichier.
— Vous ne devez pas avoir d'espaces en fin de ligne.

I 2.2 Ajoutez les objets à votre annuaire :

```
$ ldapadd -x -W -D "cn=admin,dc=iutv,dc=edu" -f iutv.ldif
```

Les options utilisées sont :
— -x ⟺ authentification simple
— -W ⟺ demande le mot de passe par la ligne de commande
— -D "..." ⟺ compte utilisé pour s'identifier au serveur

En cas d'erreur sur un objet inséré, p.ex., uid=bob,dc=rt,dc=iutv,dc=edu, le plus simple est de :
(a) supprimer l'objet :

```
$ ldapdelete -x -W -D "cn=admin,dc=iutv,dc=edu" "uid=bob,dc=rt,dc=iutv,dc=edu"
```

(b) puis de relancer votre commande ldapadd en ajoutant l'option -c qui permet de continuer la lecture du fichier même en cas d'erreur (p.ex., si un objet est déjà présent dans l'annuaire).

I 2.3 Vérifiez que votre annuaire contient bien les données attendues : slapcat.

Exercice 3 — Requêtes LDAP

Afin de nous familiariser avec les requêtes LDAP, nous ferons d'abord quelques requêtes de lecture. Nous utiliserons pour cela la commande ldapsearch avec la syntaxe suivante :

```
$ ldapsearch -x -H ldap://IP-DE-LDAP -b "DN-DE-RECHERCHE" "FILTRE"
```

où :
— DN-DE-RECHERCHE est le DN de la racine de recherche, (i.e., le sous-arbre à l'intérieur duquel on lance la recherche) ;
— et FILTRE (argument optionnel) est une condition de sélection (voir page 21 du cours).

Dans la configuration actuelle, l'annuaire est accessible en lecture par tous. Aucun mot de passe ne sera donc demandé pour une requête de sélection.

I 3.1 Donnez et testez, sur le client, les requêtes permettant de récupérer les objets suivants :
(a) Tous les objets.
(b) Tous les utilisateurs.
(c) Les utilisateurs dont l'identifiant commence par la lettre a.
(d) Les utilisateurs du département rt.
(e) Les utilisateurs ayant un numéro de téléphone.
(f) Les utilisateurs ayant un numéro de téléphone ou une adresse mail.
(g) Les utilisateurs n'ayant ni numéro de téléphone ni adresse mail.

Nous avons déjà vu les requêtes de sélection (ldapsearch), d'addition (ldapadd) et de suppression (ldapdelete). Il nous reste à voir les requêtes en modification (ldapmodify). Lorsqu'on souhaite modifier un objet, il faut décrire cette modification au format ldif. Nous allons voir deux cas.

Supposons d'abord que l'on souhaite supprimer l'attribut AAA de l'objet dont le DN est XXX. On écrira alors :

```
dn: XXX
changetype: modify
delete: AAA
```

Maintenant si l'on souhaite ajouter un attribut AAA: VVV à l'objet dont le DN est XXX, on écrira :

```
dn: XXX
changetype: modify
add: AAA
AAA: VVV
```

Sur le client :

I 3.2 Écrivez dans le fichier `del-tel.ldif` une modification permettant de supprimer le numéro de téléphone d'Alice.

I 3.3 Envoyez la requête de modification au serveur :

```
$ ldapmodify -x -H ldap://IP-DE-LDAP -W -D "cn=admin,dc=iutv,dc=edu" -f del-tel.ldif
```

I 3.4 Réitérez les deux instructions précédentes pour ajouter une adresse postale à Yann.

Exercice 4 — Droits d'accès à l'annuaire

Nous avons vu que l'annuaire est accessible en écriture par `cn=admin,dc=iutv,dc=edu` en lecture par tous. Nous allons affiner un peu ces droits d'accès en définissant un compte `cn=admin,dc=rt,dc=iutv,dc=edu` qui ne pourra modifier que le sous-arbre `dc=rt,dc=iutv,dc=edu`. Sa définition est la suivante :

```
dn: cn=admin,dc=rt,dc=iutv,dc=edu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: administrateur LDAP de rt.iutv.edu
userPassword: XXX
```

Le fichier est disponible ici :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/tp1/admin-rt.ldif`

Sur ldap :

I 4.1 Chiffrez un mot de passe de votre choix avec la commande `slappasswd`. La commande devrait afficher le mot de passe chiffré dans le terminal.

I 4.2 Récupérez le fichier `admin-rt.ldif` à l'adresse indiquée et remplacez dans ce fichier les caractères `XXX` à la dernière ligne par le mot de passe chiffré obtenu à l'instruction précédente (ajoutez *toute la ligne* affichée, y compris les caractères `{SSHA}`).

I 4.3 Ajoutez cet objet à l'annuaire.

Nous allons maintenant modifier les droits d'accès à notre annuaire. Pour cela il faut modifier la configuration de notre annuaire. Cette configuration est aussi représentée comme objet de l'annuaire, fils de l'objet `cn=config`. Le fichier permettant de redéfinir nos droits est le suivant :

```
# on supprime d'abord tous les droits d'acces existants
# (olcDatabase={1}hdb,cn=config est le DN designant la configuration
# de notre annuaire)
dn: olcDatabase={1}hdb,cn=config
changetype: modify
delete: olcAccess

# on ajoute ensuite des droits d'acces
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcAccess
# l'arbre dc=rt,dc=iutv,dc=edu est accessible par
# cn=admin,dc=rt,dc=iutv,dc=edu en ecriture et par les autres en
# lecture
olcAccess: to dn.subtree="dc=rt,dc=iutv,dc=edu"
  by dn="cn=admin,dc=rt,dc=iutv,dc=edu" write
  by * read
# tout le reste est accessible par cn=admin,dc=iutv,dc=edu en ecriture
# et par les autres en lecture
olcAccess: to *
  by dn="cn=admin,dc=iutv,dc=edu" write
  by * read
```

Le fichier est disponible ici :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/tp1/admin-rt-rights.ldif`

I 4.4 Sur ldap : récupérez le fichier `admin-rt-rights.ldif` à l'adresse indiquée.

I 4.5 Sur ldap : lancez les modifications décrites dans ce fichier :

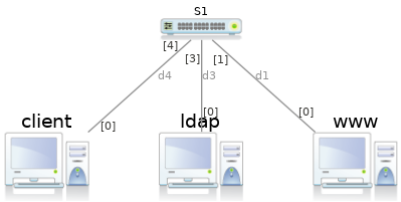
```
$ ldapmodify -Y EXTERNAL -H ldapi:// -f admin-rt-rights.ldif
```

(Ici `-Y EXTERNAL -H ldapi://` permet de se connecter "en root" à l'annuaire. C'est nécessaire car le compte que nous utilisions jusqu'à maintenant (`cn=admin,dc=iutv,dc=edu`) ne permet pas de modifier la configuration de l'annuaire.)

I 4.6 Sur le client : vérifiez par deux requêtes LDAP de votre choix que le compte `cn=admin,dc=rt,dc=iutv,dc=edu` peut écrire dans la branche `dc=rt,dc=iutv,dc=edu`, mais pas dans la branche `dc=info,dc=iutv,dc=edu`.

TP 2 — LDAP : authentification

On travaillera sur le réseau ci-dessous :



Dans ce TP nous allons voir comment l'authentification peut être déléguée à un serveur LDAP. L'objectif est que l'authentification des utilisateurs sur le poste client et sur le serveur web www repose sur le serveur LDAP.

Sur le client, il est nécessaire d'installer un certain nombre de paquets. Comme l'opération est un peu longue, on partira du projet disponible à l'adresse ci-dessous dans lequel les paquets nécessaires ont déjà été installés sur le client :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/R304-tp2.mar`

Exercice 1 — Travail préparatif

Aucun compte-rendu n'est demandé pour cet exercice.

I 1.1 Téléchargez et ouvrez le projet marionnet.
I 1.2 Ajoutez les équipements pour avoir le réseau de la figure en introduction.
I 1.3 Démarrez tous les équipements, et ouvrez une session root sur chaque hôte.
I 1.4 Attribuez à chaque hôte une IP dans le réseau 10.0.0.0/24.

Exercice 2 — Configuration du serveur

Nous allons repartir de l'annuaire du TP précédent. Il est disponible ici :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/tp2/iutv.ldif`

Toutes les instructions de cet exercice doivent être suivies sur le serveur LDAP.

I 2.1 Suivez l'instruction I 1.5 du TP précédent pour configurer le paquet `slapd`.
I 2.2 Récupérez le fichier `iutv.ldif`.

Nous allons ajouter à notre annuaire des informations de groupe et de connexion aux objets `cn=alice` et `cn=aicha` pour qu'elles puissent se connecter sur le poste client en s'authentifiant auprès du serveur LDAP. Vous trouverez la définition des classes `posixAccount` et `posixGroup` utilisées dans cet exercice dans le fichier `/etc/ldap/schema/nis.schema`.

I 2.3 Dans le fichier `iutv.ldif`, ajoutez la définition de deux objets pour représenter les groupes d'utilisateurs de nos deux domaines :
- `cn=grt,dc=rt,dc=iutv,dc=edu` de gid 1010 ;
- et `cn=ginfo,dc=info,dc=iutv,dc=edu` de gid 1020.

Ces deux objets ont pour classe `top` et `posixGroup`.

I 2.4 Dans le fichier `iutv.ldif`, ajoutez aux objets `cn=alice` et `cn=aicha` la classe `posixAccount` ainsi que tous les attributs définis par cette classe permettant de représenter les informations suivantes :
- Alice a le numéro d'utilisateur 11001 et Aïcha a le numéro 12001.
- Leurs répertoires personnels sont respectivement `/home/alice` et `/home/aicha`.
- Elles utilisent `/bin/bash` comme shell.
- Elles ont toutes les deux un mot de passe.
- Elles appartiennent aux groupes `cn=grt` et `cn=ginfo` respectivement.

Pour le mot de passe, vous suivrez la même procédure que dans le TP précédent (utilisez `slappasswd` pour chiffrer un mot de passe puis insérez ce mot de passe chiffré dans le fichier).

I 2.5 Ajoutez le contenu du fichier à votre annuaire avec `ldapadd`.
I 2.6 Vérifiez le contenu de votre annuaire avec `slapcat`.

Exercice 3 — Configuration du client

Maintenant que les groupes et comptes utilisateurs ont été créés sur le serveur, nous allons configurer le poste client pour que, lorsqu'un utilisateur se connecte, l'authentification puisse se faire via le serveur LDAP. C'est le service `nslcd` (*Name Service LDAP Connection Daemon*) qui interroge le serveur LDAP lorsqu'un utilisateur se connecte. Les réponses du serveur peuvent ensuite être mises en cache par le service `nscd` (*Name Service Cache Daemon*).

Toutes les instructions de cet exercice doivent être suivies sur le client.

I 3.1 Modifiez dans le fichier `/etc/nslcd.conf` les paramètres `base` et `uri`.

I 3.2 Redémarrez les services `nslcd` et `nscd` :

```
$ /etc/init.d/nslcd restart
$ /etc/init.d/nscd restart
```

Le service `nslcd` est maintenant configuré pour interroger notre serveur LDAP. Un autre fichier doit être modifié pour que le serveur LDAP soit contacté à la connexion d'un utilisateur : `/etc/nsswitch.conf`. Ce fichier indique les bases de données dans lesquelles le système va rechercher certaines informations comme les noms d'utilisateurs, les noms de groupes, les adresses IP, … Prenons par exemple la ligne suivante :

```
hosts:    files  dns
```

Elle signifie que pour résoudre un nom d'hôte en adresse IP on regarde d'abord dans les fichiers locaux (soit `/etc/hosts` dans ce cas) puis, si le nom n'y apparaît pas, on contacte un serveur DNS.

I 3.3 Dans `/etc/nsswitch.conf` ajoutez le mode de résolution `ldap` pour les informations de type `passwd`, `group` et `shadow`.

I 3.4 Vérifiez que le client peut récupérer des informations sur les utilisateurs et groupes définis sur le serveur LDAP :

```
$ getent passwd
$ getent group
```

I 3.5 Créez le répertoire `/home/alice` et attribuez ce répertoire à l'utilisatrice `alice` et au groupe `grt`.

I 3.6 Fermez la session courante.

I 3.7 Tout en capturant les trames sur le serveur LDAP, connectez vous avec le compte `alice`. Si votre configuration est correct vous devriez alors capturer des messages LDAP lors de la connexion.

I 3.8 Dans la capture, ajoutez le filtre `ldap`, puis trouvez la première requête de recherche (*searchRequest*) envoyée par le client.

Q 3.1 Quel est le filtre de recherche dans la requête envoyée par le client ?

I 3.9 Toujours dans la capture, retrouvez la requête *bind* envoyée par le client après sa requête de recherche pour se connecter au serveur LDAP avec le compte `alice`. Vous devriez voir le mot de passe d'Alice en clair dans le message. (On utilise LDAP, pas LADPS, les communications ne sont donc pas chiffrées…)

I 3.10 Vérifiez l'uid et le gid d'Alice :

```
$ id
```

Exercice 4 — Configuration du serveur web

Nous allons maintenant configurer le serveur web pour que son contenu soit restreint aux utilisateurs définis sur le serveur LDAP. Pour cela, il faut activer les modules `ldap` et `authnz_ldap` (authnz pour *authorization*) d'apache. Pour rappel, les modules disponibles se trouvent dans le répertoire `/etc/apache2/mods-available/`. L'activation d'un module se fait par l'ajout d'un lien symbolique dans le répertoire `/etc/apache2/mods-enabled/` pointant sur un fichier du répertoire `mods-available`.

Toutes les instructions de cet exercice doivent être suivies sur le serveur www, sauf la dernière.

I 4.1 Créez les liens symboliques pour les deux modules à activer :

`/etc/apache2/mods-enabled/ldap.load` → `/etc/apache2/mods-available/ldap.load`

`/etc/apache2/mods-enabled/authnz_ldap.load` → `/etc/apache2/mods-available/authnz_ldap.load`

La racine du serveur web se trouve dans le répertoire `/var/www/`. Ainsi, l'URL `http://IP-DU-SERVEUR-WWW/rep/fic.html` renvoie le fichier `/var/www/rep/fic.html`. Nous allons configurer apache pour que le contenu de ce répertoire soit accessible uniquement aux utilisateurs définis dans le serveur LDAP. La configuration à utiliser pour ce répertoire est la suivante :

```
AuthBasicProvider          ldap
AuthType                   Basic
AuthName                   "Acces restreint"
AuthLDAPURL                ldap://IP-DU-SERVEUR-LDAP/DN-DE-RECHERCHE
AuthzLDAPAuthoritative     on
Require                    valid-user
```

Q 4.1 Trouvez et donnez les significations des deux dernières lignes.

La configuration du site web est dans le fichier `/etc/apache2/sites-available/default`.

I 4.2 Dans ce fichier, ajoutez à l'intérieur de la balise `<Directory /var/www/>` les lignes de configuration données plus haut.

I 4.3 Redémarrez le service `apache2`.

I 4.4 Créez un fichier `/var/www/test.txt` contenant un texte quelconque.

I 4.5 Sur le client, lancez le navigateur web `epiphany` et rentrez l'URL `http://IP-DU-SERVEUR-WWW/test.txt` et vérifiez que vous pouvez accéder au contenu du fichier avec le login/mot de passe d'Aïcha.

Exercice 5 — Extensions

Dans cet exercice, on se propose d'ajouter deux extensions à notre configuration actuelle :

Extension 1 — Création automatique des comptes sur le poste client

La première extension consiste a faire en sorte que les répertoires personnels des utilisateurs sur le poste client soient automatiquement créés à la première connexion. Ainsi les commandes de l'instruction I 3.5 seront exécutées automatiquement à la première connexion d'Alice.

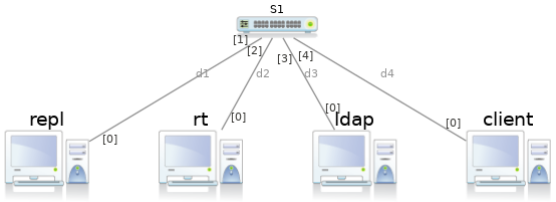
Extension 2 — Affinage des droits d'accès au serveur web

La deuxième extension consiste à affiner les droits d'accès au contenu du serveur web. Vous créerez deux répertoires à la racine de votre serveur web : `info` et `rt`. Le premier sera accessible par les membres du groupe `ginfo` seulement, et le second par ceux du groupe `grt` seulement.

Expliquez bien, dans votre compte-rendu, la démarche suivie et les différentes étapes réalisées. Si vous ne parvenez pas à réaliser les extensions, détaillez les problèmes rencontrés en donnant votre interprétation de ces problèmes ainsi que les pistes de résolution envisagées.

TP 3 — LDAP : réplication et distribution

On travaillera sur le réseau ci-dessous :



et on repartira du projet marionnet utilisé dans le TP 2 (avec les paquets nécessaires déjà installés sur le client) :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/R304-tp2.mar`

Dans ce TP nous allons voir comment fonctionne la réplication et la distribution.

La première technique permet d'avoir plusieurs serveurs LDAP avec un contenu identique. Si un des serveurs tombe en panne, le deuxième peut ainsi prendre le relai. Dans notre cas, le contenu du serveur ldap est répliqué sur l'hôte repl.

La seconde technique permet de distribuer l'annuaire sur deux (ou plus) serveurs, chaque serveur ayant un fragment de l'annuaire. Dans notre cas, l'hôte rt aura la branche `dc=rt,dc=iutv,dc=edu` et le serveur ldap aura le reste de l'arbre.

Vous trouverez dans ce répertoire un certain nombre de fichiers à récupérer durant le TP :

`https://www-lipn.univ-paris13.fr/~evangelista/cours/R304/tp3`

Exercice 1 — Travail préparatif

Aucun compte-rendu n'est demandé pour cet exercice.

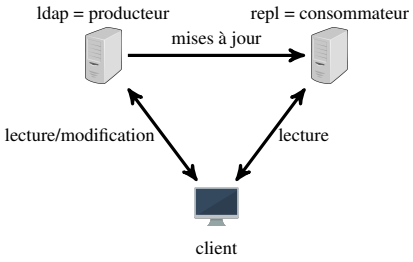
I 1.1 Téléchargez et ouvrez le projet marionnet.
I 1.2 Ajoutez les équipements pour avoir le réseau de la figure en introduction.
I 1.3 Démarrez tous les équipements, et ouvrez une session root sur chaque hôte.
I 1.4 Attribuez à chaque hôte une IP dans le réseau 10.0.0.0/24.
I 1.5 Sur ldap : suivez l'instruction I 1.5 du TP 1 pour reconfigurer le paquet `slapd`.
I 1.6 Sur ldap : récupérez le contenu du fichier `iutv.ldif` et ajoutez le à l'annuaire.

On se retrouve alors avec un serveur ldap dont le contenu est le même qu'en fin de TP 2.

Exercice 2 — Réplication de l'annuaire

Nous allons, dans cet exercice, configurer les serveurs ldap et repl pour que repl soit un réplicat de ldap et puisse être contacté par le client en cas de panne de ldap.

Il y a plusieurs modes de réplication. Dans le mode que nous allons utiliser, appelé *Sync Replication* (ou réplication par synchronisation), on a un serveur *fournisseur* (ldap dans notre cas) sur lequel des serveurs *consommateurs* (un seul, repl, dans notre cas) se synchronisent (i.e., ils récupérent les mises à jour de l'annuaire du fournisseur pour les appliquer sur les leurs). Seul l'annuaire du fournisseur peut être modifié. Les autres annuaires sont accessibles en lecture uniquement. Ce fonctionnement est résumé par la figure ci-dessous :



Pour mettre en place ce mode de réplication, nous allons dans un premier temps recopier la configuration du serveur ldap vers le serveur repl. Pour rappel, la configuration est stockée comme une branche de l'annuaire de DN `cn=config`. La configuration peut être modifiée seulement si le serveur est à l'arrêt.

Nous allons manipuler deux répertoires sur repl :

— `/etc/ldap/slapd.d/` qui contient les fichiers de configuration du serveur slapd ;
— et `/var/lib/ldap/` qui contient la base de données de l'annuaire (exceptée la configuration).

I 2.1 Sur ldap : sauvegardez la configuration actuelle du serveur dans un fichier `config.ldif` et le contenu de l'arbre `dc=iutv,dc=edu` dans un fichier `annuaire.ldif` :

```
$ slapcat -b "cn=config" > config.ldif
$ slapcat -b "dc=iutv,dc=edu" > annuaire.ldif
```

I 2.2 Sur ldap : avec `scp` copiez ces deux fichiers vers le serveur repl. Pour rappel, il faut que le service `ssh` soit démarré sur le serveur de réception.

I 2.3 Sur repl : arrêtez le service `slapd`.

I 2.4 Sur repl : supprimez les contenus des répertoires `/etc/ldap/slapd.d` et `/var/lib/ldap` (*sans les supprimer*).

I 2.5 Sur repl : ajoutez les contenus des fichiers à votre annuaire :

```
$ slapadd -F /etc/ldap/slapd.d/ -l config.ldif   -b "cn=config"
$ slapadd -F /etc/ldap/slapd.d/ -l annuaire.ldif -b "dc=iutv,dc=edu"
```

I 2.6 Sur repl : attribuez les répertoires `/etc/ldap/slapd.d` et `/var/lib/ldap` (et, récursivement, tout leurs contenus) à l'utilisateur système `openldap`. (Suite à l'instruction précédente, ces répertoires appartiennent à `root`. Or l'utilisateur système `openldap` doit pouvoir lire et modifier leurs contenus.)

I 2.7 Sur repl : redémarrez le service `slapd`.

Q 2.1 On utilise tantôt `ldapadd`, tantôt `slapadd` pour ajouter des objets. Trouvez et expliquez leurs différences.

Pour activer la réplication, il faut charger un module appelé `syncprov` en ajoutant deux objets de configuration :

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: syncprov.la

dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100
```

Le module doit être activé sur les deux serveurs (ldap et repl).

I 2.8 Sur ldap et repl : récupérez le contenu du fichier `module.ldif` et ajoutez le à l'annuaire :

```
$ ldapadd -Y EXTERNAL -H ldapi:// -f module.ldif  -c
```

Le module de réplication est maintenant activé sur les deux serveurs. La dernière étape consiste à indiquer sur le serveur repl l'adresse de son fournisseur et le DN de la racine qui sera répliquée chez lui. Cela se fait par l'ajout d'un attribut `olcSyncRepl`, qui spécifie les paramètres de synchronisation, à la configuration d'un notre annuaire :

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=001
  provider=ldap://IP-DE-LDAP
  bindmethod=simple
  searchbase="DN-RACINE"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
```

I 2.9 Sur repl : récupérez le contenu du fichier `sync.ldif`, modifiez le, et ajoutez le à l'annuaire :

```
$ ldapmodify -Y EXTERNAL -H ldapi:// -f sync.ldif  -c
```

I 2.10 Sur repl : affichez les connexions TCP ouvertes :

```
$ netstat -tna
```

Vous devriez voir une nouvelle connexion par laquelle seront reçues les mises à jour de l'annuaire.

On va maintenant tester que la réplication est fonctionnelle en lançant plusieurs requêtes depuis le client.

I 2.11 Sur le client, envoyez les cinq requêtes suivantes :
(a) vers ldap : ajout d'un objet `uid=eve,dc=rt,dc=iutv,dc=edu` avec des attributs quelconques
(b) vers ldap : lecture de l'objet `uid=eve,dc=rt,dc=iutv,dc=edu`
(c) vers repl : lecture de l'objet `uid=eve,dc=rt,dc=iutv,dc=edu`
(d) vers repl : suppression de l'objet `uid=eve,dc=rt,dc=iutv,dc=edu`
(e) vers ldap : suppression de l'objet `uid=eve,dc=rt,dc=iutv,dc=edu`

Q 2.2 Expliquez les résultats observés à l'exécution de ces requêtes.

Pour que la réplication soit utile il est nécessaire de configurer les services qui font appel au serveur ldap pour qu'ils puissent contacter repl en cas de panne. C'est ce que nous allons faire sur le poste client pour le service d'authentification.

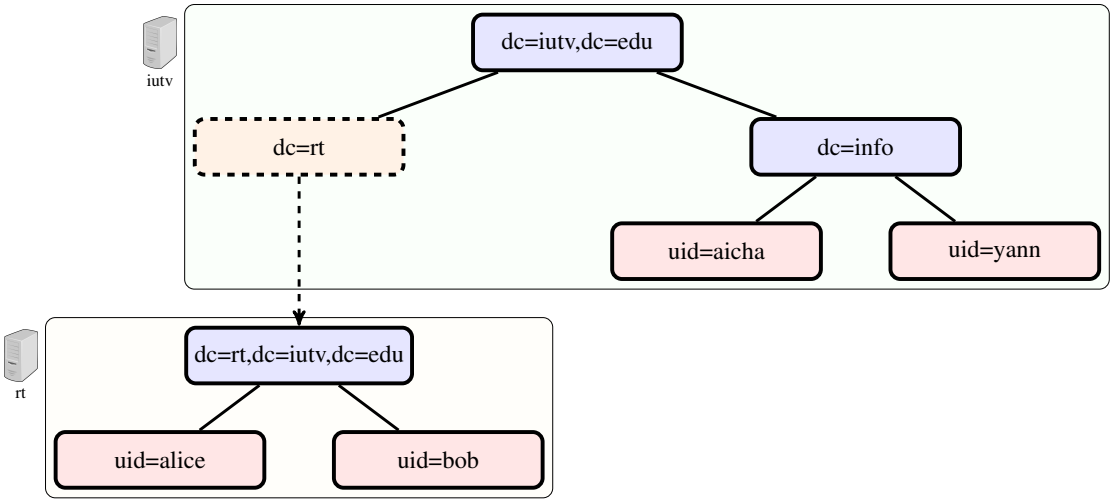
I 2.12 Sur le client : suivez les instructions I 3.1 à I 3.5 du TP 2 pour configurer l'authentification LDAP sur le poste client. Attention, dans le fichier `/etc/nslcd.conf` il faut bien préciser les URI des deux serveurs (celle de ldap en premier, puis celle de repl). (Aucune copie d'écran n'est demandée pour cette instruction.)
I 2.13 Sur le client : ouvrez une session `alice` (mot de passe = `alice`) puis fermez la session.

Nous allons maintenant simuler une panne du serveur ldap pour vérifier que le serveur repl peut prendre le relai.

I 2.14 Supprimez le câble qui connecte le serveur ldap au switch.
I 2.15 Sur le client : vérifiez que vous pouvez toujours vous connecter avec le compte d'Alice. (L'opération devrait être plus longue, autour de dix secondes, car le client tente d'abord de contacter ldap avant de se rabattre sur repl.)
I 2.16 Ajoutez à nouveau un câble entre le serveur ldap et le switch puis repassez en root sur le client.

Exercice 3 — Distribution de l'annuaire

Jusqu'à présent, tout l'annuaire se trouvait sur l'hôte ldap. Nous allons maintenant faire en sorte que l'annuaire du domaine `rt.iutv.edu` soit stocké sur l'hôte rt. On aura alors la répartition de la figure ci-dessous (les groupes `grt` et `ginfo` n'apparaissent pas) :



Tous les objets de la branche `dc=rt,dc=iutv,dc=edu` seront stockés sur l'hôte rt. Le lien entre les deux annuaires se fait par la création d'un objet de la classe `referral` sur ldap (l'objet en pointillé sur la figure). Cet objet sert uniquement à pointer vers le serveur rt pour indiquer que c'est lui qui possède la branche.

Pour cela, nous allons procéder en deux temps :
1. d'abord, sur l'hôte ldap, on supprimera la branche `dc=rt,dc=iutv,dc=edu` et on créera le *referral* vers l'hôte rt ;
2. puis on recréera la branche sur l'hôte rt.

I 3.1 Sur ldap : supprimez toute la branche de DN `dc=rt,dc=iutv,dc=edu`. Utilisez l'option `-r` de `ldapdelete` pour supprimer récursivement l'objet et ses fils.
I 3.2 Sur ldap : récupérez le contenu du fichier `ref.ldif`, modifiez le, et ajoutez le à l'annuaire. (Par la suite, si vous devez supprimer l'objet `referral` il faut donner l'option `-M` à `ldapdelete`.)

Nous allons maintenant recréer la branche `dc=rt,dc=iutv,dc=edu` sur rt mais avant cela il faut reconfigurer slapd.

I 3.3 Sur rt : suivez l'instruction I 1.5 du TP 1 pour configurer le paquet `slapd`. Adaptez vos réponses.
I 3.4 Sur rt : vérifiez que l'objet `dc=rt,dc=iutv,dc=edu` a bien été créé.
I 3.5 Sur rt : ajoutez à votre annuaire les trois objets manquants :
- `cn=grt,dc=rt,dc=iutv,dc=edu`
- `uid=alice,dc=rt,dc=iutv,dc=edu`
- `uid=bob,dc=rt,dc=iutv,dc=edu`

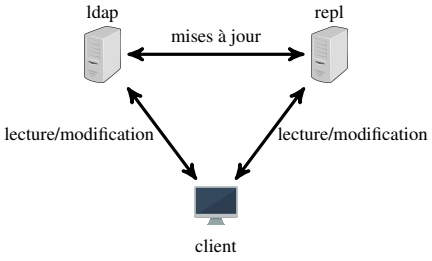
Nous allons maintenant tester que le lien referral fonctionne en envoyant des requêtes LDAP depuis le client :

I 3.6 Envoyez une requête `ldapsearch` vers le serveur ldap pour récupérer tous les comptes utilisateurs (objets de la classe `posixAccount`) du domaine `dc=rt,dc=iutv,dc=edu`.
I 3.7 Refaites la même opération en utilisant cette fois l'option `-C` de `ldapsearch` et en capturant les trames.

Q 3.1 Concluez sur l'utilité de l'option `-C`.
Q 3.2 Donnez une copie d'écran du graphique des flux capturés (Dans wireshark, utilisez `ldap` comme filtre puis allez dans *Statistiques* → *Graphique des flux*. Cochez ensuite *Limiter au Filtre d'Affichage*).
Q 3.3 Qui a contacté le serveur rt ? Est-ce le client ou le serveur ldap ?

Exercice 4 — Extension

Le mode de réplication *miroir* permet d'avoir deux serveurs identiques en lecture/écriture. Quand le contenu d'un des deux serveurs est modifié la modification est répercutée sur l'autres serveur. Ce fonctionnement est résumé par la figure ci-dessous :



Changez le mode de réplication actuel entre ldap et repl pour passer en mode miroir. Testez.

Expliquez bien, dans votre compte-rendu, la démarche suivie et les différentes étapes réalisées. Si vous ne parvenez pas à réaliser cette extension, détaillez les problèmes rencontrés en donnant votre interprétation de ces problèmes ainsi que les pistes de résolution envisagées.