LES ANNUAIRES - TD

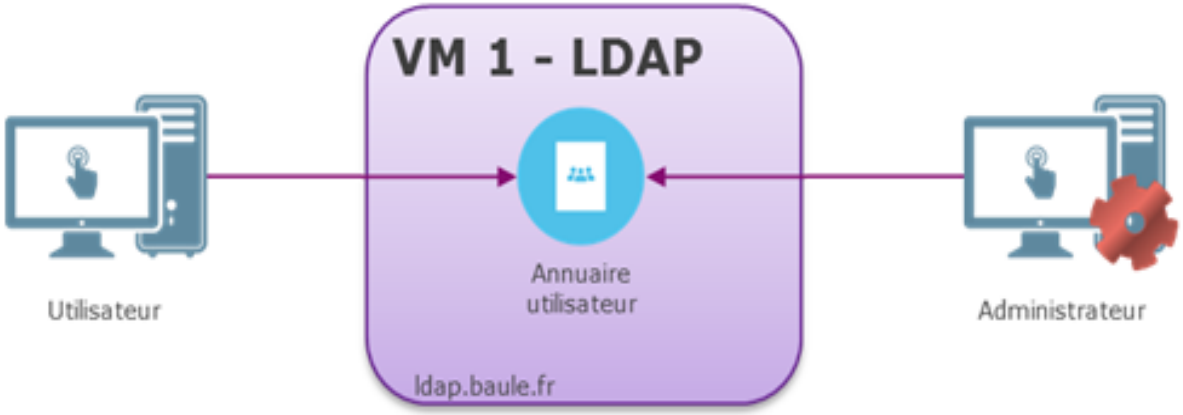
OBJECTIFS

L’objectif de ce TD est d’installer un annuaire LDAP “OpenLdap” sur la VM TD-OpenLDAP

A la fin du TD on devra pouvoir s’authentifier avec des comptes utilisateurs

Cet annuaire sera ensuite utilisé pour réaliser les authentifications locales lors du TD suivant (AM)

ARCHITECTURE CIBLE



- Annuaire utilisateur
  - Stocke
    - tous les comptes utilisateurs
    - Les groupes
    - Les informations applicatives
    - Autres données
- Utilisateur
- Administrateur

ETAPES

La réalisation du TD se fera en suivant les étapes ci-dessous:

- Installer l'annuaire OpenLDAP en utilisant les commandes de gestion de paquets de la distribution
- Configurer le super Administrateur (Vérification du mot de passe et des ACL)
- Valider le bon fonctionnement de l'annuaire
- Importer la racine de l'annuaire
- Importer le DIT
- Importer les groupes et les utilisateurs
- Configurer un client LDAP graphique (ldapadmin, Apache Directory Studio)
- Tester une authentification avec un compte utilisateur

INSTALLER L'ANNUAIRE OPENLDAP

PACKAGES D'INSTALLATION DEBIAN

Installer les packages OpenLDAP suivants : slapd ldap-utils

- slapd
  - Server OpenLDAP

- ldap-utils
  - ldapsearch - search for and display entries
  - ldapmodify - modify an entry
  - ldapadd - add a new entry
  - ldapdelete - remove and entry
  - ldapmodrdn - rename an entry
  - ldappasswd - change the password for an entry *NOTE: This is not a replacement for passwd
  - ldapwhoami: display with which entry I am bound to the server
  - ldapcompare: compare a field in the entry to some value
  - ldapmodrdn (Modifie le RDN des entrées passées en paramètre)

CONFIGURER LE SUPER ADMINISTRATEUR

POINT D'ATTENTION

Vous avez déjà renseigné le mot de passe durant l'installation d'OpenLdap ☺

Vous pouvez toutefois analyser où est stocké le login et mdp du super admin.

Pour cela, éditez le fichier "/etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif" pour en analyser sa structure

CONFIGURER LE BASEDN

CONFIGURATION DU BASEDN

A l'installation des paquets OpenLDAP, le serveur LDAP est configuré automatiquement avec les paramètres systèmes (nom du serveur, etc.), cela ne correspond pas forcément à ce que l'on souhaite. (Voir les fichiers LDIF fournis)

Editer le fichier **/etc/ldap/slapd.d/cn=config/olcDatabase\=\{1\}mdb.ldif**

Vérifier la valeur des attributs: olcSuffix, olcRootDN et olcRootPW

Adapter la configuration pour répondre à notre besoin

- Vous pouvez effectuer une reconfiguration du serveur pour que les valeurs soient celles attendu (recommandé)
- Vous pouvez modifier la configuration en utilisant des fichiers LDIF (recommandé)
- Vous pouvez également éditer directement le fichier pour mettre à jour les attributs (déconseillé)

CONFIGURATION DES ACLS

Editer le fichier **/etc/ldap/slapd.d/cn\=config/olcDatabase\=\{1\}mdb.ldif**

Vérifier les ACL olcAccess existantes

Editer le fichier **/etc/ldap/slapd.d/cn\=config/olcDatabase\=\{0\}config.ldif**

Vérifier les ACL olcAccess existantes et donner les droits d'écriture au compte d'admin vu précédemment si nécessaire

On utilisera ce compte pour effectuer les modifications de la base contenant les données et la base config

VALIDER LE BON FONCTIONNEMENT DE L'ANNUAIRE

(RE)DÉMARRAGE D'OPENLDAP

- Tester la configuration de l'annuaire avec la commande : **slaptest**
  - Il faut avoir : "config file testing succeeded"
  - et non : "slaptest: bad configuration directory!"
  - Si vous avez choisi de modifier les fichiers de config manuellement, vous pouvez avoir le message « checksum error on"
- Démarrer l'annuaire (Service slapd) (s'il est arrêté)
- Forcer le démarrage de l'annuaire au démarrage de la machine
- Vérifier que l'annuaire est bien démarré

IMPORTER LES DONNÉES DANS L'ANNUAIRE

INITIALISATION DE L'ANNUAIRE

Récupérer le fichier **racine.ldif**

Importer le fichier dans l'annuaire :

ldapadd -D **cn=admin,dc=baule,dc=fr -W -f racine.ldif**

Enter LDAP Password:

adding new entry "...

Vérifier que la configuration a bien été appliquée :

ldapsearch -x -H ldap://localhost -LL -b "dc=baule,dc=fr" -D "cn=admin,dc=baule,dc=fr" -W

Observer les deux entrées créées

CONFIGURATION DU DIT

Importer le fichier DIT.ldif

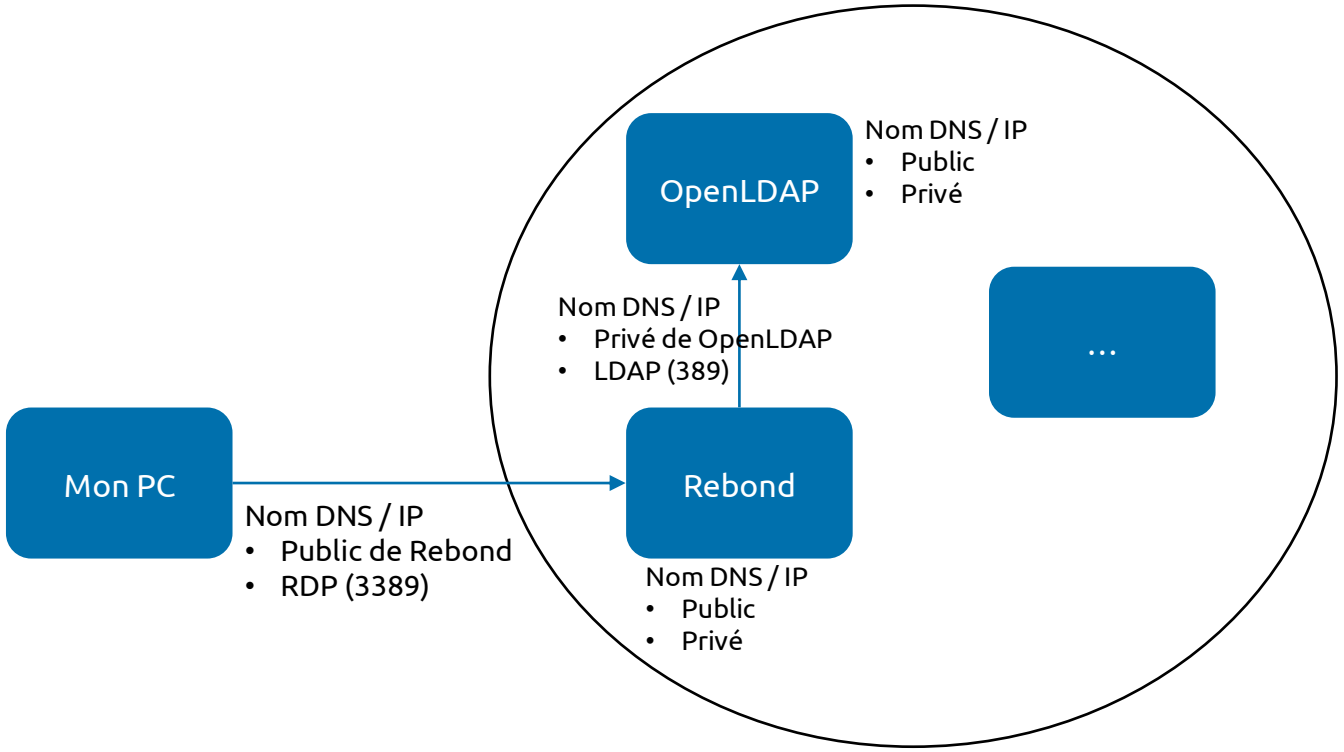
Vérifier que la configuration a bien été appliquée

Observer que les entrées ont bien été créées

INSTALLATION ET UTILISATION D'UN CLIENT LDAP

Réaliser les actions suivantes

- **Télécharger** un client LDAP (Apache Directory Studio / LDAP Browser / JExplorer / LDAPadmin / …)
- **Installer** le client
- **Configurer** une connexion sur notre annuaire
  - Avec le compte administrateur



IMPORTATION DES UTILISATEURS

Récupérer le fichier **groups.ldif** et l'importer

- Vérifier que les données soient présentes en ligne de commande et avec un client LDAP

Récupérer le fichier **users.ldif** et l'importer

- Si vous êtes sur CentOs
  - Que se passe-t-il ?
  - Pourquoi est-ce que ça ne fonctionne pas ?
  - Que faire pour que ça fonctionne ?

Réussir à importer tous les utilisateurs

IMPORTATION DES UTILISATEURS

Réaliser les actions suivantes avec le Client LDAP précédemment utilisé

- Configurer une connexion sur votre annuaire avec le compte utilisateur
- Valider l'authentification

POUR ALLER PLUS LOIN

CONFIGURATION DU SSL

Objectif : Générer un certificat SSL, le déposer et configurer pour mettre en oeuvre le ldaps sur l'annuaire

- Prérequis : Disposer d'OpenSSL

- Génération du certificat :
  - Générer une clé privée
    - openssl genrsa –aes256 -out macle.key 2048
  - Génération d'un certificat auto-signé (Attention, le CN doit correspondre au FQDN de votre annuaire. Ex : ldap.baule.fr)
    - openssl req -new -x509 -days 3650 -key macle.key -sha256 -extensions v3_ca -out moncert.crt
  - Supprimer la passphrase
    - mv macle.key macle.key.avecpass
    - openssl rsa -in macle.key.avecpass -out maclesanspass.key

CONFIGURATION DU SSL

Editer le fichier cn=config.ldif et ajouter ces 3 lignes :

*olcTLSCACertificateFile: /home/user/**moncert.crt***
*olcTLSCertificateFile: /home/user/**moncert.crt***
olcTLSCertificateKeyFile: /home/user/maclesanspass.key

Editer le fichier /etc/default/slapd et modifier la ligne suivante pour obtenir :

*SLAPD_SERVICES="ldap:/// ldapi:/// **ldaps:///"***

Redémarrer l'annuaire

Vérifier que le port LDAPS est ouvert sur votre serveur

Tester l'accès en SSL à l'annuaire depuis un client LDAP

ANNEXES

QUELQUES COMMANDES UTILES

Mettre à jour l'OS	yum update & yum upgrade
Installer OpenLDAP sur Centos	yum -y install openldap openldap-clients openldap-servers
Installer OpenLDAP sur Debian / Ubuntu	apt install slapd ldap-utils
Reconfigurer OpenLDAP	dpkg-reconfigure slapd
Gestion des mots de passe (voir le man)	slappasswd
Démarrer l'annuaire	service slapd start
	systemctl start slapd
Démarrage automatiquement au démarrage de la machine	systemctl enable sldap
Vérifier que l'annuaire est démarré	netstat –ntlp
	Netstat –ntlp | grep 389
	ss -autn
Test de la configuration de l'annuaire Centos	slaptest -F /etc/openldap/slapd.d/
Test de la configuration de l'annuaire Ubuntu / Debian	slaptest -F /etc/ldap/slapd.d/
Importer un fichier dans l'annuaire	ldapadd -D <DN Admin> -W -f <ldif file>
Recherche dans l'annuaire	ldapsearch -D <DN Admin> -W –b <baseDN> <filtre>


QUESTIONS ?