Nicolas Yang

Ubuntu 18.04 LTS Serveur

Contexte :

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole permettant d'interroger et de modifier un service d'annuaire basé sur X.500 s'exécutant sur TCP / IP.
Ainsi, le protocole LDAP accède aux répertoires LDAP. Voici quelques concepts et termes clés:

1. Un répertoire LDAP est une arborescence d'entrées de données de nature hiérarchique qui est appelée arborescence du répertoire d'information (DIT).
2. Une entrée se compose d'un ensemble d'attributs.
3. Un attribut possède un type (un nom/description) et une ou plusieurs valeurs.
4. Chaque attribut doit être défini dans au moins une classe d'objet.
5. Les attributs et classes d'objets sont définis dans les schémas (une classe d'objet est en fait considérée comme un type particulier d'attribut).
6. Chaque entrée a un identifiant unique: son nom unique (DN ou dn). Celui-ci, à son tour, consiste en un nom distinctif relatif (RDN) suivi du DN de l'entrée parent.
7. Le DN de l'entrée n'est pas un attribut. Il n'est pas considéré comme faisant partie de l'entrée elle-même.

Prérequis :

- USB bootable avec Ubuntu 18.04 LTS Serveur
- Processeur 1 gigahertz minimum
- Ram 512 mégaoctets minimum
- Capacité de disque dur 4gb minimum

Nicolas Yang

Tutoriel :

Installation Ubuntu 18.04 LTS Serveur.

1. Télécharger l'ISO approprier sur le site ubuntu.com.
2. Booter la clé USB avec Ubuntu serveur.
3. Au démarrage, il vous sera demandé de sélectionner une langue.
4. Dans le menu de démarrage principal, il y a des options supplémentaires pour installer Ubuntu édition serveur. Vous pouvez installer un serveur Ubuntu de base, vérifier si le CD-ROM a des défauts, vérifier la RAM du système, démarrer sur le premier disque dur ou dépanner un système endommagé. Le reste de cette section couvrira l'installation du serveur Ubuntu de base.
5. L'installateur vous demande quelle langue vous souhaitez utiliser. Ensuite sélection votre position.
6. Le processus d'installation commence par demander la disposition de votre clavier. Vous pouvez demander à l'installateur de tenter l'auto-détections, ou vous pouvez le sélectionner manuellement dans une liste.
7. L'installateur découvre alors votre configuration matérielle, et configure les paramètres de réseau en utilisant le protocole DHCP. Si vous ne souhaitez pas utiliser DHCP, choisissez « Retour » à l'écran suivant, et apparaît alors l'option « Configurer le réseau manuellement ».
8. Ensuite, l'installateur demande le nom de l'hôte. Un nouvel utilisateur est créé, il aura l'accès root via l'utilitaire sudo.
9. Une fois les réglages utilisateur terminés, il vous sera demandé si vous souhaitez crypter votre répertoire personnel.
10. Ensuite, le programme d'installation demande le fuseau horaire du système. Vous pouvez ensuite choisir parmi plusieurs options pour configurer la disposition du disque dur.
11. Ensuite, il vous est demandé sur quel disque installer. Vous pouvez obtenir des invites de confirmation avant de réécrire la table de partition ou de configurer LVM en fonction de la disposition du disque. Si vous choisissez LVM, il vous sera demandé la taille du volume logique racine.
12. Le système Ubuntu de base est maintenant installé.
13. La prochaine étape vous proposera de mettre à jour le système. Trois options sont possibles : Pas de mises à jour automatiques : un administrateur devra se connecter à la machine et effectuer les mises à jour manuellement. Installez les mises à jour de sécurité automatiquement : ceci installera le paquet unattended-upgrades, qui installera les mises à jour de sécurité sans l'aide d'un administrateur. Gérer le système avec Landscape : Landscape est un service payant fourni par Canonical pour vous aider à gérer vos machines Ubuntu.
14. Vous avez maintenant la possibilité d'installer ou de ne pas installer plusieurs paquets de tâches. Il existe aussi une option pour lancer aptitude afin de choisir les paquets à installer.

15. Finalement, la dernière étape avant de redémarrer le système est d'initialiser l'horloge sur UTC.

Installation LDAP

Installez le démon du serveur OpenLDAP et les utilitaires de gestion traditionnels de LDAP. On les trouve respectivement dans les paquets slapd et ldap-utils.
L'installation de slapd créera une configuration de travail. En particulier, il créera une instance de base de données que vous pourrez utiliser pour stocker vos données. Cependant, le suffixe (ou DN de base) de cette instance sera déterminé à partir du nom de domaine de l'hôte. Si vous voulez quelque chose de différent, vous pouvez le changer juste après l'installation lorsque vous n'avez toujours pas de données utiles.
Ce guide utilisera un suffixe de base de données tel que dc=exemple,dc=com.
Procédez à l'installation :

```
sudo apt install slapd ldap-utils
```

Si vous voulez changer votre suffixe DIT, ce serait le bon moment, car le changer annule votre existant. Pour modifier le suffixe, exécutez la commande suivante:

```
sudo dpkg-reconfigure slapd
```

Pour passer votre suffixe DIT à dc = exemple, dc = com , par exemple, afin que vous puissiez suivre ce guide de plus près, répondez à example.com lorsque vous êtes interrogé sur le nom de domaine DNS.
Depuis Ubuntu 8.10 slapd est conçu pour être configuré dans slapd lui-même en dédiant un DIT séparé à cet effet. Cela permet de configurer dynamiquement slapd sans avoir à redémarrer le service. Cette base de données de configuration consiste en une collection de fichiers LDIF textuels situés sous /etc/ldap/slapd.d . Cette façon de travailler est connue sous plusieurs noms: la méthode slapd-config, la méthode RTC (Real Time Configuration) ou la méthode cn = config. Vous pouvez toujours utiliser la méthode traditionnelle des fichiers plats (slapd.conf) mais ce n'est pas recommandé; la fonctionnalité sera finalement supprimée.
Ubuntu utilise maintenant la méthode slapd-config pour la configuration de slapd et ce guide reflète cela.
Pendant l'installation, vous avez été invité à définir les informations d'identification administratives. Ce sont des informations d'identification basées sur LDAP pour le rootDN de votre instance de base de données. Par défaut, le DN de cet utilisateur est cn = admin, dc = example, dc = com . De plus, par défaut, aucun compte administratif n'est créé pour la base de données slapd-config et vous devrez donc vous authentifier en externe auprès de LDAP pour y accéder. Nous verrons comment procéder plus tard.
De nos jours, certains schémas classiques (cosine, nis, inetorgperson) sont intégrés avec slapd. Il y a aussi un schéma « de base », un pré-requis pour que les schémas puissent fonctionner.

Nicolas Yang

Mode opératoire :

Recherche dans l'annuaire LDAP

```
$ ldapsearch -x -h localhost -p 389 -LL -b "ou=Users,dc=openstack,dc=org" -D "cn=admin,dc=openstack,dc=org" -w password

## ou

$ ldapsearch -x -H ldap://localhost -LL -b "ou=Users,dc=openstack,dc=org" -D "cn=admin,dc=openstack,dc=org" -w password
version: 1

dn: ou=Users,dc=openstack,dc=org
objectClass: organizationalUnit
ou: Users

dn: cn=Robert Smith,ou=Users,dc=openstack,dc=org
objectClass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
uid: rjsmith
userPassword:: ckpzbWl0SA==
carLicense: HISCAR 123
homePhone: 555-111-2222
mail: r.smith@example.com
mail: rsmith@example.com
mail: bob.smith@example.com
description: swell guy
ou: Human Resources

dn: cn=Larry Cai,ou=Users,dc=openstack,dc=org
objectClass: inetOrgPerson
cn: Larry Cai
sn: Cai
```

```
uid: larrycai
userPassword:: TGFycnlDYWk=
carLicense: HISCAR 123
homePhone: 555-111-2222
mail: larry.caiyu@gmail.com
description: hacker guy
```

Options :

- -b : Base DN, point dans l'arbre LDAP ou l'on se positionne pour commencer la recherche
- -D : Bind DN, utilisateur avec lequel on se connecte à LDAP
- -s : Scope
- -w : Bind Password, on fournit le password dans la ligne de commande
- -W : Bind Password, on sera prompter lors du lancement de la commande
- -v : verbose

Suppression

Unitairement

```
$ ldapdelete -xv  -h localhost -D "cn=admin,dc=openstack,dc=org" -w password "cn=Robert Smith,ou=Users,dc=openstack,dc=org"
```

En masse

```
$ cat delete_masse.txt
cn=Larry Cai,ou=Users,dc=openstack,dc=org
cn=Robert Smith,ou=Users,dc=openstack,dc=org


$ ldapdelete -xv  -h localhost -D "cn=admin,dc=openstack,dc=org" -w password -f ./delete_masse.txt
```

Ajout

```
## Fichier LDIF à ajouter :
$ cat more.ldif
dn: cn=Robert Smith,ou=Users,dc=openstack,dc=org
objectclass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
```

```
uid: rjsmith
userpassword: rJsmitH
carlicense: HISCAR 123
homephone: 555-111-2222
mail: r.smith@example.com
mail: rsmith@example.com
mail: bob.smith@example.com
description: swell guy
ou: Human Resources

dn: cn=Larry Cai,ou=Users,dc=openstack,dc=org
objectclass: inetOrgPerson
cn: Larry Cai
sn: Cai
uid: larrycai
userpassword: LarryCai
carlicense: HISCAR 123
homephone: 555-111-2222
mail: larry.caiyu@gmail.com
description: hacker guy
ou: Development Department



$ ldapadd -x -D cn=admin,dc=openstack,dc=org -w password -c -f more.ldif
adding new entry "cn=Robert Smith,ou=Users,dc=openstack,dc=org"

adding new entry "cn=Larry Cai,ou=Users,dc=openstack,dc=org"
```

Note : si une entrée existe déjà elle ne sera pas remplacé ni modifié, il faudra utiliser ldapmodify.

Pour plus de ressources https://www.openldap.org/