TP : Kerberos et OpenLDAP comme backend

1. Kerberos et LDAP

Kerberos prend en charge quelques backends de base de données. Celui par défaut est ce que nous avons utilisé jusque-là, est appelé db2. La documentation Types de bases de données présente toutes les options, dont l'une est LDAP.

Il existe plusieurs raisons pour lesquelles il faudrait que les principaux Kerberos soient stockés dans LDAP plutôt que dans une base de données locale sur disque. Il y a aussi des cas où ce n'est pas une bonne idée. Chaque site doit évaluer les avantages et les inconvénients. En voici quelques-unes :

- la réplication OpenLDAP est plus rapide et plus robuste que la réplication Kerberos native, basée sur une tâche cron
- La configuration des choses avec le backend LDAP n'est pas vraiment triviale et ne devrait pas être tentée par les administrateurs sans connaissance préalable d'OpenLDAP
- il peut y avoir une latence plus élevée dans la gestion des demandes lors de l'utilisation du backend OpenLDAPkrb5kdc
- si on a déjà configuré OpenLDAP pour d'autres choses, comme le stockage d'utilisateurs et de groupes, l'ajout des attributs Kerberos au même mélange peut être bénéfique et peut fournir une belle histoire intégrée

Cette séquence traite de la configuration d'un serveur Kerberos utilisant OpenLDAP comme base de données.

Configuration d'OpenLDAP

Nous devons installer le serveur OpenLDAP sur le même hôte que le KDC, pour simplifier la communication entre eux (déjà fait). Dans une telle configuration, nous pouvons utiliser le transport ldapi:///, qui se fait via un socket unix, et nous n'avons pas besoin de configurer des certificats SSL pour sécuriser la communication entre les services Kerberos et OpenLDAP.

Quand on souhaite utiliser un serveur OpenLDAP distant, ce qui est également possible, alors on faudra utiliser SSL pour la communication entre le KDC et ce serveur OpenLDAP.

Tout d'abord, le schéma nécessaire doit être chargé sur un serveur OpenLDAP disposant d'une connectivité réseau aux KDC.

2. Installation et configuration

- Installez les paquets nécessaires (il est supposé qu'OpenLDAP est déjà installé) :

sudo apt install krb5-kdc-ldap krb5-admin-server (on déjà installer un seveur LDAP et kerberos voir les autres TPs)

```
root@mame:~# apt install slapd ldap-utils krb5-kdc-ldap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

- Copier le schema dans /etc/ldap/schema

#sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz /etc/ldap/schema/

```
root@mame:/usr/share/doc/krb5-kdc-ldap# cp kerberos.schema.gz /etc/ldap/schema/
root@mame:/usr/share/doc/krb5-kdc-ldap#
```

- Ensuite, extraire le fichier : kerberos.schema.gz

#sudo gunzip /etc/ldap/schema/kerberos.schema.gz

```
root@mame:/etc/ldap/schema# gunzip kerberos.schema.gz
root@mame:/etc/ldap/schema#
```

Le schéma kerberos doit être ajouté à l'arborescence cn=config. Ce fichier de schéma doit être converti au format LDIF avant de pouvoir être ajouté. Pour cela, nous utiliserons un outil d'aide : schema2ldif

#sudo apt install schema2ldif

```
root@mame:~# apt install schema2ldif
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Pour importer le schéma, on exécute : ldap-schema-manager -i kerberos.schema

```
root@mame:/etc/ldap/schema# ldap-schema-manager -i kerberos.schema

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/kerberos.ldif'
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=kerberos,cn=schema,cn=config"

root@mame:/etc/ldap/schema#
```

Une fois le nouveau schéma chargé, indexons un attribut souvent utilisé dans les recherches :

```
root@mame:/etc/ldap/schema# ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
> dn: olcDatabase={1}mdb,cn=config
> add: olcDbIndex
> olcDbIndex: krbPrincipalName eq,pres,sub
> EOF
modifying entry "olcDatabase={1}mdb,cn=config"

root@mame:/etc/ldap/schema#
```

On crée des entrées LDAP pour les entités administratives Kerberos qui contacteront le serveur openLDAP pour effectuer des opérations. Il y en a deux :

- **ldap_kdc_dn :** doit disposer de droits de lecture sur le conteneur de domaine, le conteneur principal et les sous-arborescences de domaine.
- **ldap_kadmind_dn :** doit disposer de droits de lecture et d'écriture sur le conteneur de domaine, le conteneur principal et les sous-arborescences de domaine

Voici la commande pour créer ces entités :

```
root@mame:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=lita,dc=sn -W <<EOF
> dn: uid=kdc-service,dc=lita,dc=sn
> uid: kdc-service
> objectClass: account
> objectClass: simpleSecurityObject
> userPassword: {CRYPT}x
> description: Account used for the Kerberos KDC
>
> dn: uid=kadmin-service,dc=lita,dc=sn
> uid: kadmin-service
> objectClass: account
> objectClass: simpleSecurityObject
> userPassword: {CRYPT}x
> description: Account used for the Kerberos Admin server
> EOF
Enter LDAP Password:
adding new entry "uid=kdc-service,dc=lita,dc=sn"

adding new entry "uid=kadmin-service,dc=lita,dc=sn"

root@mame:/etc/ldap/schema#
```

Maintenant, définissons un mot de passe pour eux.

```
root@mame:/etc/ldap/schema# ldappasswd -x -D cn=admin,dc=lita,dc=sn -W -S uid=kdc-service,dc=lita,dc=sn
New password:
Re-enter new password:
Enter LDAP Password:
root@mame:/etc/ldap/schema# ldappasswd -x -D cn=admin,dc=lita,dc=sn -W -S uid=kadmin-service,dc=lita,dc=
sn
New password:
Re-enter new password:
Enter LDAP Password:
root@mame:/etc/ldap/schema#
```

On peut les tester avec : **ldapwhoami**

```
root@mame:/etc/ldap/schema# ldapwhoami -x -D uid=kdc-service,dc=lita,dc=sn -W
Enter LDAP Password:
dn:uid=kdc-service,dc=lita,dc=sn
root@mame:/etc/ldap/schema#
```

Enfin, mettons à jour les listes de contrôle d'accès (ACL).

Nous devons insérer les nouvelles règles avant la dernière, pour contrôler l'accès aux entrées et attributs liés à Kerberos

```
root@mame:/etc/ldap/schema# ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
> dn: olcDatabase={1}mdb,cn=config
> add: olcAccess
> olcAccess: {2}to attrs=krbPrincipalKey
>   by anonymous auth
>   by dn.exact="uid=kdc-service,dc=lita,dc=sn" read
>   by dn.exact="uid=kadmin-service,dc=lita,dc=sn" write
>   by self write
>   by * none
> -
> add: olcAccess
> olcAccess: {3}to dn.subtree="cn=krbContainer,dc=lita,dc=sn"
>   by dn.exact="uid=kdc-service,dc=lita,dc=sn" read
>   by dn.exact="uid=kadmin-service,dc=lita,dc=sn" write
>   by * none
> EOF
modifying entry "olcDatabase={1}mdb,cn=config"

root@mame:/etc/ldap/schema#
```

Vérifions les ACLs avec la commande sudo slapcat -b cn=config

```
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to attrs=krbPrincipalKey by anonymous auth by dn.exact="uid=kdc-
 service,dc=lita,dc=sn" read by dn.exact="uid=kadmin-service,dc=lita,dc=sn" wr
 ite by self write by * none
olcAccess: {3}to dn.subtree="cn=krbContainer,dc=lita,dc=sn" by dn.exact="uid=k
 dc-service,dc=lita,dc=sn" read by dn.exact="uid=kadmin-service,dc=lita,dc=sn"
  write by * none
olcAccess: {4}to * by * read
```

Voilà, notre annuaire LDAP est maintenant prêt à servir de base de données principale Kerberos.

Configuration KDC principale (LDAP)

Une fois OpenLDAP configuré, il est temps de configurer le KDC. Ici LDAP et Kerberos sont sur la même machine.

On édite le fichier /etc/krb5.conf en rajoutant les paramètres suivants dans la section [realms]

default_domain = LITA.SN

database_module = openldap_ldapconf

```
[realms]
        LITA.SN = {
                kdc = server.lita.sn
                admin_server = server.lita.sn
                default_domain = LITA.SN
                database_module = openldap_ldapconf
        }
        ATHENA.MIT.EDU = {
                kdc = kerberos.mit.edu
                kdc = kerberos-1.mit.edu
```

Ensuite, on ajoute également ces nouvelles sections :

```
  GNU nano 6.2                                  /etc/krb5.conf *
[dbdefaults]
    ldap_kerberos_container_dn = cn=krbContainer,dc=lita,dc=sn

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap

                                # if either of these is false, then the ldap_kdc_dn needs to
                                # have write access
                                disable_last_success = true
                                disable_lockout = true

                # this object needs to have read rights on
                # the realm container, principal container and realm sub-trees
                ldap_krb_dn = "uid=kdc-service,dc=lita,dc=sn"

                # this object needs to have read and write rights on
                # the realm container, principal container and realm sub-trees
                ldap_kadmib_dn = "uid=kadmin-service,dc=lita,dc=sn"

                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldapi:///
                ldap_conns_per_server = 5
        }
```

On utilise l'utilitaire kdb5_ldap_util pour créer le domaine :

#kdb5_ldap_util -D cn=admin,dc=lita,dc=sn create -subtrees dc=lita,dc=sn -r LITA.SN -s -H

ldapi:///

```
root@mame:/etc/ldap/schema# kdb5_ldap_util -D cn=admin,dc=lita,dc=sn create -subtrees dc=lita,dc=sn -r LITA.SN -s -H ldapi:///
Password for "cn=admin,dc=lita,dc=sn":
Initializing database for realm 'LITA.SN'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
root@mame:/etc/ldap/schema#
```

On crée une réserve du mot de passe utilisé pour la liaison au serveur LDAP. On l'exécute une fois pour chaque ldap_kdc_dn et ldap_kadmin_dn.

#kdb5_ldap_util -D cn=admin,dc=lita,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kdc service,dc=lita,dc=sn

#kdb5_ldap_util -D cn=admin,dc=lita,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile

uid=kadmin-service,dc=lita,dc=sn

```
root@mame:/etc/ldap/schema# kdb5_ldap_util -D cn=admin,dc=lita,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kdc-service,
dc=lita,dc=sn
Password for "cn=admin,dc=lita,dc=sn":
Password for "uid=kdc-service,dc=lita,dc=sn":
Re-enter password for "uid=kdc-service,dc=lita,dc=sn":
root@mame:/etc/ldap/schema# kdb5_ldap_util -D cn=admin,dc=lita,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kadmin-servi
ce,dc=lita,dc=sn
Password for "cn=admin,dc=lita,dc=sn":
Password for "uid=kadmin-service,dc=lita,dc=sn":
Re-enter password for "uid=kadmin-service,dc=lita,dc=sn":
root@mame:/etc/ldap/schema#
```

Le fichier contient maintenant des versions en texte clair des mots de passe utilisés par le KDC pour contacter le serveur LDAP /etc/krb5kdc/service.keyfile

On redémarre le KDC Kerberos et le serveur d'administration :

On peut désormais ajouter des principaux Kerberos à la base de données LDAP.

Pour que le ldap_kadmin_dn puisse y écrire, nous devons d'abord mettre à jour les ACLs :

```
root@mame:/etc/ldap/schema# ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
> dn: olcDatabase={1}mdb,cn=config
> add: olcAccess
> olcAccess: {4}to dn.subtree="ou=People,dc=lita,dc=sn"
>   by dn.exact="uid=kdc-service,dc=lita,dc=sn" read
>   by dn.exact="uid=kadmin-service,dc=lita,dc=sn" write
>   by * break
> EOF
modifying entry "olcDatabase={1}mdb,cn=config"

root@mame:/etc/ldap/schema#
```

Et maintenant, nous pouvons spécifier le principal :

Avant cela on crée un utilisateur dans LDAP ou de prendre le fichier déjà cree.

Pour ajouter des principaux Kerberos à la base de données LDAP on utilise l'option –x

#kadmin.local

#addprinc –x dn=uid=gueye,ou=Clients,dc=lita,dc=sn gueye

Puis de saisir un le mot de passe

Les attributs **krbPrincipalName**, **krbPrincipalKey**, **krbLastPwdChange** et **krbExtraData** doivent maintenant être ajoutés à l'objet utilisateur uid=gueye,ou=Clients,dc=lita,dc=sn.