Kerberos - Installer les KDC

Introduction à la configuration initiale des KDC

En implémentant Kerberos dans un environnement de production, il est préférable d'avoir plusieurs KDC esclave avec un KDC maître pour s'assurer de la disponibilité continue des service kerberisés. Chaque KDC contient une copie de la base de donnée Kerberos. Le KDC maître contient la copie modifiable de la base, qui est répliquée au esclaves à intervalle régulier. Tous les changements de base sont faites sur le maître. Les esclave fournissent les services TGS, mais pas d'administration de la base, quand le KDC maître n'est pas disponible. Le MIT recommande d'installer tous les KDC pour être en mesure de fonctionner soit en tant que maître ou un esclave. Celà permet de facilement basculer un esclave en maître si nécessaire.

Attention

Le système Kerberos s'appuyent du la disponibilité des informations de temps correcte, assurez vous que le maître et les esclaves ont une horloge synchronisée correctement. Il est préférable d'installer les KDC sur du hardware dédié et sécurisé avec un accès limité.

Installer et configurer le KDC maître

Dans ce document, nous utilisons les noms suivants :

```
kerberos.mit.edu____-_master KDC
kerberos-1.mit.edu__-_slave KDC
ATHENA.MIT.EDU______-_realm name
.k5.ATHENA.MIT.EDU__-_stash file
admin/admin_________-_admin principal
```

Éditer les fichiers de configuration du KDC

Modifier les fichiers de configuration, **krb5.conf** et **kdc.conf**, pour refléter les informations telles que le mappage domain-realm et les noms des serveurs kerberos. Beaucoup de tags dans la configuration ont des valeurs par défaut qui sont adéquat à la plupart des sites. Les variables **KRB5_CONFIG** et **KRB5_KDC_PROFILE** permettent de spécifier les fichiers altérnatifs :

```
export KRB5_CONFIG=/yourdir/krb5.conf
export KRB5_KDC_PROFILE=/yourdir/kdc.conf
```

krb5.conf

Si vous n'utilisez pas les enregistrements DNS TXT, vous devez spécifier le **default_realm** dans la section **[libdefault]**. Si vous n'utilisez par les enregistrements DNS SRV, vous devez inclure le tag **kdc** pour chaque realm dans la section **[realms]**. Pour communiquer avec le serveur kadmin dans chaque realm, le tag **admin_server** doit être définis dans la section **[realms]**.

Exemple de fichier krb5.conf

```
[libdefaults]
 default_realm = ATHENA.MIT.EDU

[realms]
 ATHENA.MIT.EDU = {
  kdc = kerberos.mit.edu
  kdc = kerberos-1.mit.edu
  admin_server = kerberos.mit.edu
 }
```

kdc.conf

Ce fichier peut être utilisé pour contrôler les ports d'écoute du KDC en de kadmind, et les paramètres par défaut spécifique au realm, le type de base et son emplacement et le logging.

Exemple de fichier kdc.conf

```
[kdcdefaults]
 kdc_ports = 88,750
[realms]
 ATHENA.MIT.EDU = {
  kadmind_port = 749
  max_life = 12h 0m 0s
  max_renewable_life = 7d 0h 0m 0s
  master_key_type = aes256-cts
  supported_enctypes = aes256-cts:normal aes128-cts:normal
  # If the default location does not suit your setup,
  # explicitly configure the following values:
  # database_name = /var/krb5kdc/principal
  # key_stash_file = /var/krb5kdc/.k5.ATHENA.MIT.EDU
  # acl_file = /var/krb5kdc/kadm5.acl
 }
[logging]
 # By default, the KDC and kadmind will log output using
 # syslog. You can instead send log output to files like this:
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmin.log
 default = FILE:/var/log/krb5lib.log
```

Remplacer **ATHENA.MIT.EDU** et **kerberos.mit.edu** avec le nom de votre domaine et serveur Kerberos, respectivement.

Note : vous devez avoir les droits d'écriture sur les répertoires cibles (et doivent exister) utilisés par **database_name**, **key_stash_file**, et **acl_file**.

Créer la base KDC

Il faut utiliser la commande **kdb5_util** sur le KDC maître pour créer la base Kerberos et le fichier optionnel **stash**.

Note : Si vous choisissez de ne pas installer un fichier stash, le KDC va vous demander la clé maître chaque fois qu'il démarre.

kdb5_util va vous demander le mot de passe maître pour la base Kerberos. L'exemple suivant montre comment créer une base Kerberos et le fichier stash sur le KDC maître.

```
shell% kdb5_util create -r ATHENA.MIT.EDU -s

Initializing database '/usr/local/var/krb5kdc/principal' for realm 'ATHENA.MIT.EDU',
master key name 'K/M@ATHENA.MIT.EDU'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: <= Type the master password.
Re-enter KDC database master key to verify: <= Type it again.
shell%
```

Cela va créer 5 fichiers dans **LOCALSTATEDIR/krb5kdc** (ou l'emplacement spécifié dans kdc.conf) :

- 2 fichiers de base de données, **principal** et **principal.ok**
- Le fichier de base de données administrative, **principal.kadm5**
- Le fichier de lock de la base administrative, **principal.kadm5.lock**
- Le fichier stash, dans cet exemple **.k5.ATHENA.MIT.EDU**. utiliser l'option **-s** pour ne pas générer ce fichier.

Ajouter les administrateurs au fichier d'ACL

Ensuite, vous devez créer un fichier d'acl et y placer le principal Kerberos d'au moins un administrateur. Ce fichier est utilisé par **kadmind** pour contrôler quel principaux peuvent voir et effectuer des modifications privilégiées dans les fichiers de base Kerberos. Le nom du fichier d'acl est déterminé par la variable **acl_file** dans **kdc.conf** (défaut : LOCALSTATEDIR/krb5kdc/kadm5.acl)

Ajouter les administrateurs à la base kerberos

Vous devez ajouter les principaux administratifs à la base de données Kerberos. Vous devez ajouter au moins un principal pour permettre la communication entre **kadmind** et **kadmin** sur le réseaux. Pour cela, utiliser l'utilitaire **kadmin.local** sur le KDC maître. Il est conçus pour être lancé sur un KDC maître sans utiliser d'authentification Kerberos. Vous devez avoir un accès en lecture/écriture à la base Kerberos.

Les principaux administratifs que vous créez devraient être ceux ajoutés dans le fichier d'acl.

Dans l'exemple suivant, le principal administratif admin/admin est créé :

```
shell% kadmin.local

kadmin.local: addprinc admin/admin@ATHENA.MIT.EDU

WARNING: no policy specified for "admin/admin@ATHENA.MIT.EDU";
assigning "default".
Enter password for principal admin/admin@ATHENA.MIT.EDU: <= Enter a password.
Re-enter password for principal admin/admin@ATHENA.MIT.EDU: <= Type it again.
Principal "admin/admin@ATHENA.MIT.EDU" created.
kadmin.local:
```

Démarrer le service Kerberos sur le KDC maître

À ce point, vous êtes prêt à démarrer le KDC (krb5kdc) et les services administratifs sur le KDC maître :
shell% krb5kdc
shell% kadmind

Chaque service va se forker en tâche de fond.

Vous pouvez vérifier qu'ils sont lancés correctement en vérifiant les messages de démarrage dans les emplacement le logging spécifiés dans krb5.conf :

```
shell% tail /var/log/krb5kdc.log
Dec 02 12:35:47 beeblebrox krb5kdc[3187](info): commencing operation
shell% tail /var/log/kadmin.log
Dec 02 12:35:52 beeblebrox kadmind[3189](info): starting
```

En vérification additionnelle, vérifier si kinit réussit avec les principaux administratifs :

```
shell% kinit admin/admin@ATHENA.MIT.EDU
```

Installer les KDC esclave

Maintenant vous être prêt à configurer les KDC esclaves.

Note : en assumant que vous paramètrez le KDC de manière à facilement basculer le maître avec un des esclaves, vous devriez effectuer chaque étape sur de maître sur les esclaves, sauf les ces instructions spécifient le contraire.

Créer les keytabs pour les KDC esclave

Chaque KDC a besoin d'un clé **host** dans la base Kerberos. Ces clés sont utilisée pour l'authentification mutuelle lors de la propagation des dump de la base de donnée depuis le maître.

Sur le KDC maître, se connecter à l'interface administrative et créer le principal de l'hôte pour chaque service **host** des KDC. Par exemple, si le maître s'appel **kerberos.mit.edu**, et l'esclave s'appel **kerberos-1.mit.edu** :

```
shell% kadmin
kadmin: addprinc -randkey host/kerberos.mit.edu
NOTICE: no policy specified for "host/kerberos.mit.edu@ATHENA.MIT.EDU"; assigning "default"
Principal "host/kerberos.mit.edu@ATHENA.MIT.EDU" created.

kadmin: addprinc -randkey host/kerberos-1.mit.edu
NOTICE: no policy specified for "host/kerberos-1.mit.edu@ATHENA.MIT.EDU"; assigning "default"
Principal "host/kerberos-1.mit.edu@ATHENA.MIT.EDU" created.
```

Il n'est pas nécessaire d'avoir le maître dans la base Kerberos, mais peut être nécessaire si vous souhaitez basculer le maître en esclave. Ensuite, extraire chaque clé **host** pour tous les KDC participants et les stocker dans chaque fichier keytab de l'hôte. Idéalement, vous devriez extraire chaque keytab localement dans son propre KDC. Si cela n'est pas faisable, vous devriez utiliser une session chiffrée pour les envoyer sur le réseau. Pour extraire un keytab sur un serveur esclave :

```
kadmin: ktadd host/kerberos-1.mit.edu
Entry for principal host/kerberos-1.mit.edu with kvno 2, encryption
 type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kerberos-1.mit.edu with kvno 2, encryption
 type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kerberos-1.mit.edu with kvno 2, encryption
 type des3-cbc-sha1 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kerberos-1.mit.edu with kvno 2, encryption
```

```
type arcfour-hmac added to keytab FILE:/etc/krb5.keytab.
```

Configurer les KDC esclave

La propagation de la base de données copie le contenu de la base du maître, mais ne propage pas les fichiers de configuration, les fichiers stash, ou le fichier d'acl. Les fichiers suivants doivent être copiés à la main pour chaque esclave :

- krb5.conf
- kdc.conf
- kadm5.acl
- master key stash file

Déplacer les fichiers copiés dans leur répertoires appropriés, exactement comme sur le KDC maître. La base est propagée du maître vers les esclaves via le service **kpropd**. Vous devez explicitement spécifier les principaux qui sont autorisé à fournir les mises à jours Kerberos sur les esclaves avec une nouvelle base de données. Créer un fichier nommé **kpropd.acl** dans le répertoire d'état KDC contenant les principaux **host** pour chaque KDC :

```
host/kerberos.mit.edu@ATHENA.MIT.EDU
host/kerberos-1.mit.edu@ATHENA.MIT.EDU
```

Note : si vous souhaitez que le maître et l'esclave puis être inversés, listez les principaux hôtes depuis tous les KDC participants dans les fichiers **kpropd.acl** dans tous les KDC. Sinon, vous avez seulement besoin de lister le principal de l'hôte du KDC maître dans **kpropd.acl** des KDC esclaves.

Ensuite, ajoutez la ligne suivante dans **/etc/inetd.conf** dans chaque KDC :

```
krb5_prop 754/tcp # Kerberos slave propagation
```

Redémarrez inetd. Alternativement, démarrer **kpropd** comme service standalone. Cela est nécessaire quand la propagation incrémental est activé.

Maintenant que le KDC est capable d'accepter la propagation de la base, vous avez besoin de propager la base depuis le maître. Note : Ne pas démarrer le KDC esclave avant d'avoir une copie du maître.

Propager la base à chaque esclave

Premièrement, créer un fichier dump de la base sur le maître :
shell% kdb5_util dump /usr/local/var/krb5kdc/slave_datatrans
Puis, propager manuellement la base à chaque esclave :
shell% kprop -f /usr/local/var/krb5kdc/slave_datatrans kerberos-1.mit.edu
Database propagation to kerberos-1.mit.edu : SUCCEEDED
Vous aurez besoin d'un script pour dumper et propager la base. voici un exemple de script shell. Rappelez vous que vous avez besoin de remplacer **/usr/local/var/krb5kdc** avec le nom du répertoire d'état KDC.

```
#!/bin/sh

kdclist = "kerberos-1.mit.edu kerberos-2.mit.edu"

kdb5_util dump /usr/local/var/krb5kdc/slave_datatrans
```

```
for kdc in $kdclist
do
 kprop -f /usr/local/var/krb5kdc/slave_datatrans $kdc
done
```

Vous avez besoin du définir un cron pour lancer ce script à intervalle régulier. Maintenant que l'esclave a une copie de la base Kerberos, vous pouvez démarrer krb5kdc :

```
shell% krb5kdc
```

Erreurs de propagation

kprop : No route to host while connecting to server
Assurez vous que le nom d'hôte de l'esclave est correct et que les firewalls entre le maître et l'esclave autorisent le port 754.
kprop : Connection refused while connecting to server
Si l'esclave tente de lancer kpropd via inetd, assurez vous que inetd est configuré pour accepter les connections krb5_prop. inetd a besoin de relire sa configuration pour qu'un changement soit pris en compte.
kprop : Server rejected authentication (during sendauth exchange) while authenticating to server
assurez vous que :

1. L'heure est synchonisée
2. Le fichier stash du maître a été copié sur l'esclave à l'emplacement attendu
3. L'esclave a un fichier keytab contenant un principal **host** pour le nom d'hôte de l'esclave.

Ajouter des principaux à la base

Une fois les KDC définis et fonctionnels, vous êtes prêt à utiliser **kadmin** pour charger les principaux pour vos utilisateurs, hôtes, et autres services dans la base kerberos. Vous pouvez occasionnellement utiliser un des esclaves comme maître. Cela peut se produire si vous mettez à jour le maître, ou si le maître crash.

Basculer de maître et d'esclave

Si le KDC maître fonctionne, effectuez les étapes suivantes sur l'ancien maître :

1. Tuer kadmind
2. Désactiver le job cron qui propage la base
3. Lancer le script de propagation manuellement, pour s'assurer que tous les esclaves ont la dernière copie de la base.

Sur le nouveau maître :

1. Démarrer **Kadmind**
2. Définir un cron pour propager la base
3. Bascules les CNAME de l'ancien vers le nouveau maître. Si vous ne pouvez pas le faire, vous aurez besoin de changer le fichier **krb5.conf** sun chaque client dans le domaine kerberos.