Mise en place d’un Serveur Kerberos

Kerberos est un système d'authentification réseau basé sur le principe d'un tiers de confiance. Les deux autres parties sont l'utilisateur et le service sur lequel l'utilisateur veut s'authentifier. Tous les services et applications ne savent pas utiliser Kerberos, mais pour ceux qui en sont capables, cela rapproche l'environnement réseau d'un système à authentification unique (Single Sign On ou SSO).
Cette section couvre l'installation et la configuration d'un serveur Kerberos, et propose quelques exemples de configurations de clients.

Aperçu

Si vous débutez avec Kerberos, il y a quelques termes qu'il est bon de comprendre avant de paramétrer un serveur Kerberos. La plupart des termes sont proches d'éléments qui peuvent vous être familiers dans d'autres environnements.

1. **Donneur d'ordre :** tous les utilisateurs, ordinateurs et services fournis par des serveurs doivent être définis comme « donneurs d'ordre » Kerberos.
2. **Instances :** sont utilisés pour les donneurs d'ordre de service et les donneurs d'ordre administratifs spéciaux.
3. **Realms:** le domaine de contrôle unique fourni par l'installation Kerberos. Considérez-le comme le domaine ou le groupe auquel appartiennent vos hôtes et utilisateurs. La convention veut que le domaine soit en majuscule. Par défaut, Ubuntu utilisera le domaine DNS converti en majuscules (EXAMPLE.COM) comme domaine.
4. **Centre de distribution de clé :** (KDC) se compose de trois parties, une base de données de tous les donneurs d'ordre, le serveur d'authentification et le serveur accordant les tickets. Pour chaque domaine, il doit y avoir au moins un KDC.
5. **Ticket d'octroi de ticket :** émis par le serveur d'authentification (AS), le ticket d'octroi du ticket (TGT) est chiffré avec le mot de passe utilisateur qui n'est connu que par l'utilisateur et le KDC.
6. **Serveur d'octroi de ticket :** (TGS) génère sur demande des tickets de service aux clients.
7. **Tickets :** confirment l'identité des deux donneurs d'ordre. Un donneur d'ordre étant un utilisateur et l'autre un service demandé par l'utilisateur. Les tickets établissent une clé de chiffrage utilisée pour la communication sécurisée pendant la session authentifiée.
8. **Fichiers Keytab :** ce sont des fichiers extraits de la base de données KDC des « principals » et qui contiennent la clé de chiffrement pour un service ou un hôte.

Un Realm possède au moins un KDC, de préférence davantage pour la redondance, qui contient une base de données de principaux. Lorsqu'un utilisateur principal se connecte à un poste de travail configuré pour l'authentification Kerberos, le KDC émet un Ticket Granting Ticket (TGT). Si les informations d'identification fournies par l'utilisateur correspondent, l'utilisateur est authentifié et peut ensuite demander des tickets pour les services Kerberisés auprès du Ticket Granting Server (TGS). Les tickets de service permettent à l'utilisateur de s'authentifier auprès du service sans saisir un autre nom d'utilisateur et un autre mot de passe.

Serveur Kerberos

Installation

Pour cette discussion, nous allons créer un domaine MIT Kerberos avec les caractéristiques suivantes (les modifier en fonction de vos besoins) :

1. *Domaine :* EXEMPLE.COM
2. *KDC primaire :* kdc01.example.com (192.168.0.1)
3. *KDC secondaire :* kdc02.example.com (192.168.0.2)
4. *Utilisateur principal :* steve
5. *Administrateur principal :* steve/admin

Il est fortement recommandé que vos utilisateurs authentifiés sur le réseau aient leur identifiant dans une plage différente (par exemple, commençant à 5 000) que celle de vos utilisateurs locaux.

Avant d'installer le serveur Kerberos, un serveur DNS correctement configuré est nécessaire pour votre domaine. Puisque le domaine Kerberos correspond par convention au nom de domaine, cette section utilise le domaine EXAMPLE.COM configuré dans Maitre primaire de la documentation DNS.
De plus, Kerberos est un protocole sensible au temps. Ainsi, si l'heure système locale entre une machine client et le serveur diffère de plus de cinq minutes (par défaut), le poste de travail ne pourra pas s'authentifier. Pour corriger le problème, l'heure de tous les hôtes doit être synchronisée à l'aide du même serveur NTP (Network Time Protocol).

La première étape dans la création d'un domaine Kerberos est d'installer les paquets *krb5-kdc* et *krb5-admin-server*. Dans un terminal saisissez :

```
sudo apt install krb5-kdc krb5-admin-server
```

À la fin de l'installation, il vous sera demandé de fournir le nom d'hôte des serveurs Kerberos et Admin, qui peuvent ou non être le même serveur, pour le domaine.

Par défaut, le domaine est créé à partir du nom de domaine du KDC.

Ensuite, créez le nouveau domaine à l'aide de l'utilitaire *kdb5_newrealm* :

```
sudo krb5_newrealm
```

Configuration

Les questions posées lors de l'installation permettent de configurer le fichier /etc/krb5.conf. Si vous devez ajuster les paramètres du centre de distribution de clés (KDC), modifiez simplement le fichier et redémarrez le démon krb5-kdc. Si vous devez reconfigurer Kerberos à partir de zéro, peut-être pour changer le nom du domaine, vous pouvez le faire en tapant

```
sudo dpkg-reconfigure krb5-kdc
```

1. 1. Une fois que le KDC fonctionne correctement, un utilisateur administrateur -- l'administrateur principal -- est nécessaire. Il est recommandé d'utiliser un nom d'utilisateur différent de votre nom d'utilisateur quotidien. À l'aide de l'utilitaire kadmin.local dans une invite de terminal, saisissez :
2.

```
3. sudo kadmin.local
```

```
4. Authentification en tant que donneur d'ordre root/admin@EXEMPLE.COM avec un
   mot de passe.
5. kadmin.local: addprinc steve/admin
```

```
6. WARNING: no policy specified for steve/admin@EXAMPLE.COM; defaulting to no
   policy
7. Enter password for principal "steve/admin@EXAMPLE.COM":
8. Re-enter password for principal "steve/admin@EXAMPLE.COM":
9. Principal "steve/admin@EXAMPLE.COM" created.
10.kadmin.local: quit
```

Dans l'exemple ci-dessus, Steve est le principal, /admin est une instance et @EXAMPLE.COM signifie le domaine. Le principal "tous les jours", c'est-à-dire le principal utilisateur, serait steve@EXAMPLE.COM et ne devrait disposer que des droits d'utilisateur normaux.

Remplacez *EXEMPLE.COM* et *steve* par votre nom d'utilisateur de domaine et d'administrateur.

11. Ensuite, le nouvel utilisateur admin a besoin des permissions ACL (Access Control List) appropriées. Les permissions sont configurées dans le fichier /etc/krb5kdc/kadm5.acl :

```
12.steve/admin@EXAMPLE.COM        *
```

Cette entrée accorde à steve/admin la possibilité d'effectuer n'importe quelle opération sur tous les principaux du domaine. Vous pouvez configurer des mandataires avec des privilèges plus restrictifs, ce qui est pratique si vous avez besoin d'un mandataire administrateur que le personnel junior peut utiliser dans les clients Kerberos.

13. Redémarrez maintenant *krb5-admin-server* pour que les nouvelles ACL soient prises en compte :

```
14.sudo systemctl restart krb5-admin-server.service
```

15. Le nouveau « principal » d'utilisateur peut être testé en utilisant *kinit utility* :

```
16.kinit steve/admin
17.Mot de passe de steve/admin@EXAMPLE.COM :
```

Après avoir saisi le mot de passe, utilisez *klist* pour afficher les informations du TGT (Ticket Granting Ticket, ticket d'octroi de tickets) :

```
klist
Credentials cache: FILE:/tmp/krb5cc_1000
        Principal: steve/admin@EXAMPLE.COM

  Issued           Expires          Principal
Jul 13 17:53:34  Jul 14 03:53:34  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Où le nom de fichier de cache krb5cc_1000 est composé du préfixe krb5cc_ et de l'identifiant utilisateur (uid), qui dans ce cas est 1000. Vous devrez peut-être ajouter une entrée dans le fichier /etc/hosts pour le KDC afin que le client puisse trouver le KDC. Par exemple:

```
192.168.0.1   kdc01.example.com       kdc01
```

Replacing *192.168.0.1* with the IP address of your KDC. This usually happens when you have a Kerberos realm encompassing different networks separated by routers.

18. La meilleure façon de permettre aux clients de déterminer automatiquement le KDC pour le domaine est d'utiliser les enregistrements DNS SRV. Ajoutez ce qui suit à /etc/named/db.exemple.com :

```
19._kerberos._udp.EXAMPLE.COM.     IN SRV 1  0 88  kdc01.example.com.
20._kerberos._tcp.EXAMPLE.COM.     IN SRV 1  0 88  kdc01.example.com.
21._kerberos._udp.EXAMPLE.COM.     IN SRV 10 0 88  kdc02.example.com.
22._kerberos._tcp.EXAMPLE.COM.     IN SRV 10 0 88  kdc02.example.com.
23._kerberos-adm._tcp.EXAMPLE.COM. IN SRV 1  0 749 kdc01.example.com.
24._kpasswd._udp.EXAMPLE.COM.      IN SRV 1  0 464 kdc01.example.com.
```

Remplacez *EXAMPLE.COM*, *kdc01*, et *kdc02* par vos noms de domaine, de serveur KDC primaire et secondaire.

KDC secondaire

Une fois que vous avez un centre de distribution de clés (KDC) sur votre réseau, il est conseillé d'avoir un KDC secondaire au cas où le principal deviendrait indisponible. En outre, si vous avez des clients Kerberos dans des réseaux différents (éventuellement séparés par des routeurs utilisant NAT), il est judicieux de placer un KDC secondaire dans chacun de ces réseaux.

1. Tou d'abord, installez les paquets, et lors de la demande des noms de serveurs Kerberos et Admin, saisiissez le nom du serveur KDC primaire :

```
2. sudo apt install krb5-kdc krb5-admin-server
```

3. Une fois les paquets installés, créez un « principal » du KDC secondaire. Dans un terminal, saisissez :

```
4. kadmin -q "addprinc -randkey host/kdc02.example.com"
```

Ensuite, l'exécution de n'importe quelle commande *kadmin* nécessitera l'introduction du mot de passe du « principal » *username/admin@EXAMPLE.COM*.

5. Extrayez le fichier *keytab* :

```
6. kadmin -q "ktadd -norandkey -k keytab.kdc02 host/kdc02.example.com"
```

7. Il devrait y avoir un fichier keytab.kdc02 dans le dossier actuel. Déplacez le vers /etc/krb5.keytab :

```
8. sudo mv keytab.kdc02 /etc/krb5.keytab
```

Si l'emplacement du fichier keytab.kdc02 est différent, adaptez le en conséquence.

Vous pouvez également lister les « principals » d'un fichier Keytab à l'aide de *klist*, ce qui peut être utile au dépannage :

```
sudo klist -k /etc/krb5.keytab
```

L'option *-k* indique qu'il s'agit d'un fichier keytab.

9. Ensuite, il doit exister un fichier kpropd.acl sur chaque KDC qui liste tous les KDC du domaine. Par exemple, sur les serveurs primaire et secondaire, créez le fichier /etc/krb5kdc/kpropd.acl :

```
10.host/kdc01.example.com@EXAMPLE.COM
11.host/kdc02.example.com@EXAMPLE.COM
```

12. Créez une base de données vide sur le *KDC secondaire* :

```
13.sudo kdb5_util -s create
```

14. Lancez maintenant le démon *kpropd*, qui écoute les connexions depuis l'utilitaire *kprop*. *kprop* est utilisé pour transférer des fichiers de sauvegarde :

```
15.sudo kpropd -S
```

16. Depuis un terminal sur le *KDC primaire*, créez un fichier de sauvegarde de la base de données des « principals » :

```
17.sudo kdb5_util dump /var/lib/krb5kdc/dump
```

18. Décompressez le fichier *keytab* du KDC primaire et copiez le dans /etc/krb5.keytab :

```
19.kadmin -q "ktadd -k keytab.kdc01 host/kdc01.example.com"
20.sudo mv keytab.kdc01 /etc/krb5.keytab
```

Assurez-vous qu'il y ait un *hôte* pour *kdc01.example.com* avant d'extraire le Keytab.

21. L'utilitaire *kprop* envoie la base de données vers le serveur KDC secondaire :

```
22.sudo kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

Il devrait y avoir un message de *succès* si le transfert s'est bien passé. S'il y a un message d'erreur, vérifiez /var/log/syslog sur le KDC secondaire pour plus d'informations.

Vous pouvez également créer une tâche *cron* pour mettre à jour périodiquement la base de données sur le KDC secondaire. Par exemple, ce qui suit va mettre à jour la base de données

toutes les heures (notez que la grande ligne a été divisée pour l'adapter au format du document) :

```
# m h  dom mon dow   command
0 * * * * /usr/sbin/kdb5_util dump /var/lib/krb5kdc/dump &&
/usr/sbin/kprop -r EXAMPLE.COM -f /var/lib/krb5kdc/dump kdc02.example.com
```

23. De retour sur le *KDC secondaire*, créez un fichier *stash* qui contiendra la clé maîtresse de Kerberos :

```
24.sudo kdb5_util stash
```

25. Finalement, démarrez le service *krb5-kdc* sur le KDC secondaire :

```
26.sudo systemctl start krb5-kdc.service
```

Le KDC secondaire devrait désormais être en mesure d'émettre des tickets pour le Royaume. Vous pouvez tester cela en arrêtant le démon krb5-kdc sur le KDC principal, puis en utilisant kinit pour demander un ticket. Si tout se passe bien, vous devriez recevoir un ticket du KDC secondaire. Sinon, vérifiez /var/log/syslog et /var/log/auth.log dans le KDC secondaire.

Client Kerberos Linux

Cette section couvre la configuration d'un système Linux comme un client *Kerberos*. Ceci va autoriser l'accès à n'importe quel service gérant Kerberos une fois l'utilisateur correctement connecté au système.

Installation

Pour pouvoir s'authentifier sur un domaine Kerberos, les paquets *krb5-user* et *libpam-krb5* sont nécessaires, ainsi que quelques autres qui ne sont pas obligatoires mais vous faciliteront la tâche. Pour installer ces paquets tapez la commande suivante dans un terminal :

```
sudo apt install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

Le paquet *auth-client-config* permet une configuration simple de PAM pour l'authentification depuis plusieurs sources. *libpam-ccreds* va mettre en cache les références de l'authentification pour vous permettre de vous connecter si le KDC (Key Distribution Center) n'est pas disponible. Ce paquet est également utile pour les portables qui s'identifient via Kerberos sur leur réseau professionnel, mais doivent également rester accessibles en dehors ce réseau.

Configuration

Pour configurer le client, tapez dans un terminal :

```
sudo dpkg-reconfigure krb5-config
```

Il vous sera alors demandé de donner le nom du domaine Kerberos. Si vous n'avez pas de DNS configuré avec des enregistrements *SRV* Kerberos, le menu vous demandera le nom de l'hôte KDC et du serveur d'administration du domaine.
dpkg-reconfigure ajoute des entrées au fichier /etc/krb5.conf pour votre domaine. Vous devriez avoir des entrées similaires à :

```
[libdefaults]
        default_realm = EXEMPLE.COM
...
[realms]
        EXEMPLE.COM = {
                kdc = 192.168.0.1
                admin_server = 192.168.0.1
        }
```

Si vous définissez l'UID de chacun de vos utilisateurs authentifiés sur le réseau pour qu'il commence à 5 000, comme suggéré dans Installation, vous pouvez alors demander à pam d'essayer de s'authentifier uniquement en utilisant des utilisateurs Kerberos avec un UID > 5 000 :

```
# Kerberos should only be applied to ldap/kerberos users, not local ones.
for i in common-auth common-session common-account common-password; do
 sudo sed -i -r \
 -e 's/pam_krb5.so minimum_uid=1000/pam_krb5.so minimum_uid=5000/' \
 /etc/pam.d/$i
done
```

Cela permettra d'éviter une demande de mot de passe (inexistant) Kerberos d'un utilisateur authentifié localement lors du changement de son mot de passe à l'aide de la commande passwd.

Vous pouvez tester la configuration en demandant un ticket à l'aide de *kinit*. Par exemple :

```
kinit steve@EXAMPLE.COM
Mot de passe pour steve@EXAMPLE.COM :
```

Lorsqu'un ticket a été accordé, les détails peuvent être affichés avec *klist* :

```
klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: steve@EXAMPLE.COM

Valid starting     Expires            Service principal
07/24/08 05:18:56  07/24/08 15:18:56  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 07/25/08 05:18:57
```

```
Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Ensuite, utilisez *auth-client-config* pour configurer le module *libpam-krb5* pour demander un ticket lors de l'ouverture de session :

```
sudo auth-client-config -a -p kerberos_example
```

Vous devriez maintenant recevoir un ticket dès qu'une ouverture de session avec authentification est réussie.