Université de Bordeaux — année 2019-2020

Master CSI/Master Info. — Sécurité des réseaux

TD - Kerberos + NFS4

Le but de ce TP est de mettre en place l'authentification au dessus de Kerberos entre deux machines : immortal (le client) et opeth (le serveur). Nous allons ensuite utilisé Kerberos dans le context de NFSv4 pour avoir un système de fichier partagé sur le réseau (et qui de plus assure l'authentification).

La topologie réseau correspondante peut être obtenue en lançant le script de démarrage `/net/stockage/aguermou/SR/TP/10/qemunet.sh` en lui fournissant la description de la topologie réseau à l'aide de l'option `-t` ainsi que l'archive contenant la configuration initialte des machines à l'aide de l'option `-a`. Ceci revient à lancer les commandes suivantes :

```
cd /net/stockage/aguermou/SR/TP/10/; ./qemunet.sh -x -t topology -a archive_tp10.tgz
```

1. Configurer tout d'abord un serveur DNS dans le réseau immortal/opeth (cette fois-ci j'ai tout fait :-)).
2. Configurer le serveur Kerberos sur opeth via le fichier krb5.conf. Attention, ce fichier devra être copié sur toutes les machines devant faire partie du royaume.

```
[libdefaults]
        default_realm = METAL.FR

# The following krb5.conf variables are only for MIT Kerberos.
        krb4_config = /etc/krb.conf
        krb4_realms = /etc/krb.realms
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following libdefaults parameters are only for Heimdal Kerberos.
        v4_instance_resolve = false
        v4_name_convert = {
                host = {
                        rcmd = host
                        ftp = ftp
                }
                plain = {
                        something = something-else
                }
        }
        fcc-mit-ticketflags = true

[realms]
    METAL.FR = {
        # specifies where the servers are and on
        # which ports they listen (88 and 749 are
        # the standard ports)
        kdc = opeth.metal.fr:88
        admin_server = opeth.metal.fr:749
    }
```

```
[domain_realm]
        .metal.fr = METAL.FR
[login]
        krb4_convert = true
        krb4_get_tickets = false

[logging]
    # determines where each service should write its
    # logging info
    kdc = SYSLOG:INFO:DAEMON
    admin_server = SYSLOG:INFO:DAEMON
    default = SYSLOG:INFO:DAEMON


[appdefaults]
  pam = {
     debug = true
     ticket_lifetime = 36000
     renew_lifetime = 36000
     forwardable = true
     krb4_convert = false
     max_timeout = 30
     timeout_shift = 2
     initial_timeout = 1
  }
```

3. Ajouter le nom de votre royaume dans `/etc/krb5kdc/kdc.conf`.

```
[kdcdefaults]
    kdc_ports = 749,88

    [realms]
        metal.fr = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        kdc_ports = 749,88
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = aes256-cts
        supported_enctypes = aes256-cts:special aes256-cts:normal des3:special des3:normal
        }

    [logging]
        kdc = FILE:/var/log/kdc.log
        admin_server = FILE:/var/log/kadmin.log
```

4. Créer la base Kerberos à l'aide de : `kdb5_util create -s`
5. Éditer le fichier `kadm5.acl` (le chemin du fichier est spécifié dans le fichier de configuration `kdc.conf`)et y ajouter : `*/admin@METAL.FR *` pour permettre aux administrateurs de modifier la base.
6. Lancer le serveur Kerberos sur opeth : `/etc/init.d/krb5-kdc restart`.

7. Pour authoriser immortal à faire de l'authentification Kerberos, il est nécessaire de lancer la console d'administration locale (`kadmin.local`). Puis, il faut :
   — ajouter un principe Kerberos pour l'hôte immortal.metal.fr :
   `kadmin : addprinc -randkey host/immortal.metal.fr`
   L'option -randkey sert à générer une clé aléatoire (en lien et place de la saisie du mot de passe). Répéter cette même étape pour ajouter opeth à la base Kerberos (et pour stocker sa clé privée).
   — extraire la clé de la base Kerberos :
   `kadmin: ktadd -k /tmp/tmp.keytab host/immortal.metal.fr`
   — copier le fichier `/tmp/tmp.keytab` sur immortal et écraser le fichier `/etc/krb5.keytab`.
   Bien entendu toutes ses étapes doivent être faites sur la machine hébergeant le serveur Kerberos (opeth). Répeter les étapes précédentes pour permettre aux autres machines de dialoguer avec le serveur Kerberos.
8. Sur opeth, lancer `kadmin.local` pour y ajouter un utilisateur toto `addprinc toto@METAL.FR`.
9. Sur immortal, initialiser un ticket en tant que toto à l'aide de commande `kinit toto@METAL.FR`.
10. Faire un ssh sur opeth à partir d'immortal en utilisant comme identifiant toto. Constater qu'on ne vous demande aucun mot de passe
11. modifier sur le client `/etc/pam.d/common-*` pour permettre l'authentification au dessus de Kerberos. Utiliser la commande `pam-auth-update` pour ce faire. Ceci permettra lors du login d'un utilisateur de lui attribuer automatiquement un ticket si ce dernier réussit son authentification.

NFS4

Nous allons maintenant nous intéresser à la configuration de NFSv4 avec une authentification au dessus de Kerberos.

12. Pour authoriser les deux machines à utiliser NFS4 au dessus de Kerberos, il est nécessaire de :
   — Ajouter un principe Kerberos spécifique à NFS pour l'hôte immortal.metal.fr :
   `kadmin : addprinc -randkey nfs/immortal.metal.fr`
   L'option -randkey sert à générer une clé aléatoire (en lien et place de la saisie du mot de passe). Répéter cette même étape pour ajouter opeth à la base Kerberos (et pour stocker sa clé privée).
   — extraire la clé de la base Kerberos :
   `kadmin: ktadd -k /tmp/tmp.keytab nfs/immortal.metal.fr`
   — copier le fichier `/tmp/tmp.keytab` sur immortal et écraser le fichier `/etc/krb5.keytab`.
   — Attention, il ne faut pas enlever l'ancien contenu du fichier listant les clés.
13. configurer nfs-common et nfs-kernel-server en ajoutant les lignes suivantes aux fichiers indiqués :

Avec Kerberos	Sans Kerberos

`/etc/default/nfs-common :`
`NEED_IDMAPD=yes`
`NEED_GSSD=yes`
`RPCGSSDOPTS=""`
 	
`/etc/default/nfs-kernel-server :`
`NEED_SVCGSSD=yes`
`RPCSVCGSSDOPTS=""`
	`/etc/default/nfs-common :`
	`NEED_IDMAPD=yes`
	`NEED_GSSD=`
	
	`/etc/default/nfs-kernel-server :`
	`NEED_SVCGSSD=`

14. mettre-à-jour le répertoire de partage (`/etc/exports`) :

Avec Kerberos		Sans Kerberos	
`/public`	`gss/krb5(fsid=0,rw, no_subtree_check)`	`/public`	`*(fsid=0,rw,insecure, no_subtree_check)`
`/public/test`	`gss/krb5(rw,no_subtree_check)`	`/public/test`	`*(rw,no_subtree_check)`

15. Éditer le fichier `/etc/idmapd.conf` pour y ajouter la ligne suivante dans la section *General* pour y spécifier le nom de notre domaine :

    ```
    Domain = metal.fr
    ```

16. Démarrer les services nécessaires au bon fonctionnement de NFS :
    — sur le serveur : `service nfs-server restart`
    — sur le client : `service nfs-idmapd restart; service auth-rpcgss-module restart`
17. Monter le dossier distant sur la machine cliente et vérifier que tout marche :
    `mount -t nfs4 -o sec=krb5 server:/test /tmp/toto`
    (dans le cas où on n'utilise pas Kerberos pour authentifier le client, les options lors du montage vont etre différentes).
18. Vérifier que tout marche dans les deux cas.