Année Universitaire 2016-2017
3ième année IMAC

Mardi 17 janvier 2017

Cloud computing
Travaux Pratiques

Objectif

Dans un premier temps, on utilisera libvirt : une librairie d'accès aux principaux hyperviseurs du marché ; l'API libvirt est écrite en C et est sous licence libre (http://libvirt.org/). Nous allons utiliser le programme `virsh`, une interface en ligne de commande pour la librairie libvirt pour manipuler les machines virtuelles : création, démarrage, arrêt, destruction, modification des ressources, snapshot, recopie et déplacement.

Dans un second temps, nous installerons dans une machine virtuelle, un service de stockage de fichiers en ligne. On profitera de ces dispositifs pour analyser les traces sur le réseau, ce qui nous conduira à augmenter le niveau de sécurité du service. Enfin nous ferons une analyse de traces de serveur.

En début de travaux pratiques, un étudiant utilise un poste de travail et pour la partie de déplacement des machines virtuelles, il faut travailler avec deux postes et donc par groupe de deux étudiants.

Initialisation du système

Au boot de la machine, prendre soin de ré-initialiser le système

```
Installation Linux light: rsync (rapide)
```

puis

```
Demarrer sur le disque
```

Se logguer avec l'utilisateur `tpreseau`, mot de passe `tpreseau`,

Utiliser les paramètres par défault

ouvrir un navigateur (clic droit Applications / Internet / Firefox ESR)

ouvrir un terminal de commande (clic droit sur le bureau et Ouvrir un terminal ici).

Vérifier les possibilités de virtualisation du CPU, la commande :

```
egrep '(vmx|svm)' --color=always /proc/cpuinfo
```

doit afficher les caractères `vmx` ou `svm` en couleur.

Vérifier la configuration BIOS, la commande

```
dmesg | grep -i kvm
```

ne doit rien afficher.

Pour avoir les droits root, exécuter la commande,

```
su
```

le mot de passe est `tpreseau.`

Placer les fichiers nécessaires au TP dans le répertoire /mnt/temp,

```
mkdir /mnt/temp
```

décompresser l'image du disque

```
cd /mnt/temp
gunzip jessie.qcow2.gz
```

pour ne pas perdre de temps, ouvrir un autre terminal, puis

```
su
```

déplacer les scripts et fichiers de configuration dans /root
```
mv /mnt/temp/jessie.xml /mnt/temp/*.sh /root
```
Faire tourner le script
```
bash generic-init.sh
```
répondre OK à la question posée sur la configuration du paquet mdadm
Obtenir de l'aide sur l'interface `virsh` :
```
virsh help|less
```
Obtenir de l'aide sur la commande `start` :
```
virsh help start
```

Le cycle de vie des domaines

Éditer le fichier `jessie.xml` pour lui attribuer une adresse mac en remplaçant les xx par votre numéro attribué par votre enseignant, puis démarrer le domaine jessie qui n'est pas encore enregistré dans la liste des domaines gérés par libvirt et accéder à la console du domaine avec la seconde instruction
```
virsh create jessie.xml ; virt-viewer jessie &
```
Vérifier le démarrage
```
virsh list --all
```
Arrêter le domaine
```
virsh shutdown jessie
```
Vérifier l'arrêt
```
virsh list --all
```
Enregistrer le domaine jessie dans la liste des domaines gérés par libvirt
```
virsh define jessie.xml
```
Vérifier cet enregistrement
```
virsh list --all
```
Supprimer cet enregistrement du domaine jessie
```
virsh undefine jessie
```
Vérifier la suppression
```
virsh list --all
```
Définir à nouveau le domaine jessie
```
virsh define jessie.xml
```
Démarrer le domaine jessie qui est défini (noter la différence avec la commande « virsh create jessie.xml » qui permet de démarrer un domaine qui n'a pas été défini)
```
virsh start jessie
```
Vérifier le démarrage
```
virsh list
```

Vérifications

Accéder à la console de la machine invité
```
virt-viewer jessie &
```
Se logguer en tant `root`, mot de passe `tpreseau` et lancer la commande
```
ip a
```
pour récupérer l'adresse IP du domaine invité.

Sauvegarde à chaud

Lire le contenu du fichier script php
```
/var/www/html/heure.php
```
sur la machine invitée et faire quelques modifications dans ce fichier afin de le personnaliser, cela nous permettra par la suite d'identifier la machine virtuelle.
Dans un navigateur de la machine hôte, aller à l'adresse
http://ip_inv/heure.php

Pour réaliser une sauvegarde à chaud des domaines, on exécute les trois opérations suivantes :
1) figer le domaine
2) prendre un snapshot (une photo) de la partition support du domaine
3) reprendre l'exécution normale du domaine.
Nous n'avons pas la possibilité ici de montrer le snapshot de la partition, nous ne montrons donc que les étapes 1) et 3), pendant ces deux opérations, conserver un regard sur http://ip_inv/heure.php

Suspendre l'exécution du domaine
```
virsh suspend jessie
```
Reprendre l'exécution du domaine
```
virsh resume jessie
```
On constate que l'horloge système de la machine invité s'est arrêté pendant cette période ; on peut renouveler les opérations suspend et resume pour s'en convaincre.

Modifier les ressources

Dans le domaine jessie, exécuter la commande top afin de visualiser les ressources du domaine
```
top
```

Puis, sur l'hyperviseur, augmenter la mémoire de la façon suivante
```
virsh setmem jessie 1048576
```
Vous devez constater une augmentation immédiate de la ressource Mem, il est aussi possible de diminuer la mémoire, à exécuter avec la plus grande précaution, car si un processus utilise la partie de la mémoire qui disparaît du système, ce processus disparaît !

Augmenter le nombre de CPU :
Arrêter la machine jessie et éditer son fichier de configuration :
```
virsh shutdown jessie
virsh edit jessie
```
Modifier la ligne
```
  <vcpu placement='static'>1</vcpu>
```
en
```
  <vcpu placement='static'>2</vcpu>
```

Redémarrer le domaine pour visualiser l'apparition d'un second CPU, exécuter la commande top, puis appuyer sur la touche 1.

Recopie des machines virtuelles

Une fonctionnalité très appréciée de ces machines virtuelles est de pouvoir se répliquer très facilement. On montre dans ce TP deux modes de recopies.

1) Le clonage d'un domaine, il s'agit d'une recopie de l'image dans l'état, l'outil de création prend soin de ne pas recopier les informations qui doivent être uniques pour un domaine.
2) Le snapshot n'est pas une véritable recopie, il s'agit d'une photo du système à un instant T. Il permet de conserver l'état d'un domaine à un instant T.

Le clonage d'un domaine

Attention, la recopie ne peut pas se faire à chaud
```
virsh shutdown jessie
```
définissez votre adresse mac en remplaçant les xx par votre numéro

```
virt-clone --original=jessie --mac 54:52:00:03:xx:00 --auto-clone
```
Vous venez d'installer une machine complète en un temps record ! Vérifiez que les domaines démarrent bien
```
virsh start jessie
virsh start jessie-clone
```
Pour visualiser les différences des deux domaines, vous pouvez exécuter la séquence de commande suivante :
```
virsh dumpxml jessie > /tmp/jessie.xml
virsh dumpxml jessie-clone > /tmp/jessie-clone.xml
diff /tmp/jessie.xml /tmp/jessie-clone.xml
vi -d /tmp/jessie.xml /tmp/jessie-clone.xml (pour sortir [Echap][:][q][:][q])
```

Snapshot d'un domaine

Commencer par prendre le temps de lire l'article
https://fr.wikipedia.org/wiki/Instantan%C3%A9_%28informatique%29

Sur la machine invitée, écrire un fichier
```
echo "avant snapshot" > journal
```
vérifier l'écriture de ce fichier :
```
cat journal
```

Voir la liste des snapshot d'un domaine
```
virsh snapshot-list jessie
```

Créer un snapshot
```
virsh snapshot-create jessie
```
noter le numéro du snapshot crée

vérifier la présence du snapshot
```
virsh snapshot-list jessie
```

effectuer une modification dans le domaine
```
echo "apres snapshot" >> journal
```
vérifier le contenu du fichier :
```
cat journal
```

revenir au point du snapshot
```
virsh snapshot-revert jessie xxx
```
où xxx est le numéro du snapshot que l'on souhaite restaurer

vérifier dans la VM
```
cat journal
```

supprimer le snapshot
```
virsh snapshot-delete jessie xxx
```
où xxx est le numéro du snapshot que l'on souhaite effacer

Vérifier la disparition du snapshot
```
virsh snapshot-list jessie
```

Travailler sur le disque virtuel

Travailler sur un disque dont le système est éteint
```
virsh shutdown jessie
```
Préparer le point de montage
```
mkdir /mnt/test
```
Vérifier que le répertoire est bien vide
```
ls /mnt/test
```
Monter le disque

```
guestmount -d jessie -i /mnt/test
```
Vérifier que le disque est bien monté
```
ls /mnt/test
cat /mnt/test/root/journal
```
Démonter le disque
```
guestunmount /mnt/test
```

Migration de domaine

Il faut maintenant travailler avec deux postes et donc à deux étudiants, soient les postes A et B. L'objectif de cet exercice est de montrer qu'un domaine peut être migré d'une machine hôte vers une autre machine hôte sans arrêt du domaine. Cet exercice illustre les propos d'Eben Moglen : « Cloud means servers have gained freedom. Freedom to move. Freedom to dance; to combine and to separate, re-aggregate, and do all sorts of tricks.» lors d'une conférence donnée à l'Internet Society en 2010. Ici, l'image du domaine réside sur la machine A. Au début de l'exercice, le domaine est exécuté sur la machine A et nous montrons que tout en résidant sur la machine A son exécution peut se déplacer sur la machine B.

Situation initiale :

Sur la machine A

Le domaine jessie est défini est il est en cours d'exécution, vérifier avec
```
virsh list
```

Sur la machine B

Le domaine jessie n'est pas défini, exécuter
```
virsh shutdown jessie
virsh undefine jessie
```
Afin de préparer l'espace d'accueil, le fichier
```
/mnt/temp/jessie.qcow2
```
doit bien être présent.

Maintenant les deux machines sont prêtes pour la migration du domaine, pendant l'opération observez bien la continuité d'exécution du domaine http://ip_inv/heure.php

Sur la machine A, exécuter la commande
```
virsh migrate --live  --persistent --copy-storage-all --verbose --xml jessie.xml
jessie qemu+ssh://ip_de_B/system
```
rentrer le mot de passe tpreseau

La migration devrait durer 15 à 20 minutes ; sur les machines A et B, vérifier la liste des domaines
```
virsh list --all
```
Pendant ce temps, vous pouvez prendre une pause.

Installation de NextCloud

NextCloud est un logiciel libre de service de stockage et de partage de fichiers en ligne qui possède des clients intégrés pour les principaux systèmes d'exploitation windows, mac et linux et pour les mobiles android et ios ; on peut comparer son périmètre fonctionnel à Dropbox. Il existe d'autres logiciels libres sur ce sujet : sparkleshare, seafile, cozycloud et pydio.

Le script install_nextcloud.sh que vous devez relire pour comprendre ce qu'il fait va installer l'application NextCloud.
```
su
bash install_nextcloud.sh
```

Dans l'interface web, créer le compte administrateur, par exemple :
utilisateur = admin , mot de passe = tpreseau

puis renseigner les champs relatifs à la base de données en prenant soin de les faire correspondre aux paramètres du script install_nextcloud.sh

La création des comptes utilisateurs se fait dans le menu admin (en haut à droite de l'écran) et dans la partie Utilisateurs ; créer un compte toto et un autre titi, sortir de la session admin, rentrer avec la session toto, uploader un document, le partager avec titi, sortir de la session, rentrer avec titi et vérifier que le document uploadé est bien disponible, puis sortir de l'application.

Le site protège son accès par mot de passe sans chiffrement, c'est comme fermer une porte sans la fermer à clé, n'importe qui peut rentrer sans casser la serrure. Pour le montrer, il suffit de se placer sur une machine qui se trouve sur le chemin réseau de la requête (en l'occurrence la machine hôte ou la machine invité) et observer le flux :

avec la commande sur la machine invité :

```
tcpdump -i eth0 port 80 -A | grep -i password=
```

et sur la machine hôte avec la commande :

```
tcpdump -i br0 port 80 -A | grep -i password=
```

si la commande tcpdump n'est pas installée, vous pouvez l'installer avec la commande

```
apt-get install tcpdump
```

À la suite de cette observation, la nécessité de chiffrer le flux réseau devient évidente. Il faut dans un premier temps installer le module SSL du serveur Apache, le paramétrer et installer un certificat. Comme il n'est pas possible de réaliser un certificat chez un tiers de confiance dans le cadre de notre TP, nous nous contenterons donc d'un certificat auto-signé. Dans un second temps, il faut aller dans l'interface d'administration de NextCloud pour cocher la case « Forcer HTTPS ».

Le script install_ssl-nextcloud.sh vous permettra de réaliser cette installation. Comme l'opération de création du certificat auto-signé génère un ensemble de questions et réponses, il est préférable de copier le script install_ssl-nextcloud.sh sur la machine invité et d'exécuter le script en local :

depuis la machin hôte :

```
scp install_ssh-nextcloud.sh root@ip_inv:
```

depuis la machine invité :

```
bash install_ssh-nextcloud.sh
```

À la suite de cette installation, vérifier que le chiffrement est bien opérationnel :

```
tcpdump -i eth0 port 80 or port 443 -A | grep -i password=
```

Utiliser SSH

Vous pouvez commencer par lire l'article https://fr.wikipedia.org/wiki/Secure_Shell
L'exercice consiste à utiliser SSH avec authentification par clé.
Nous allons permettre à l'utilisateur tpreseau de la machine A de se connecter en ssh sur le compte tpreseau de la machine B sans avoir à rentrer de mot de passe.
Il faut créer un couple de clé privé, clé public sur la machine A :

```
tpreseau@A:~$ ssh-keygen
```

- le choix proposé d'emplacement de la clé peut être validé, appuyer sur entrée pour le valider
- la passphrase peut être vide, appuyer sur entrée
- pour confirmer, appuyer à nouveau sur entrée

Il faut envoyer la clé publique de tpreseau de la machine A dans le compte tpreseau de la machine B :

Depuis le compte tpreseau de la machine A, réaliser une première connexion ssh
```
tpreseau@A:~$ ssh ip_B
```
afin de stocker une empreinte (le fingerprint) de la machine B sur la machine A. Cette empreinte permet de se protéger d'une usurpation d'identité de la machine B. Il s'agit d'une ligne stockée dans le fichier kown_hosts que vous pouvez vérifier :
```
tpreseau@B:~$ cat /home/tpreseau/.ssh/known_hosts
```

Nous allons maintenant recopier la clé publique de tpreseau sur la machine B, la clé se placera dans un fichier authorized_keys. Vérifions que le fichier est non existant :
```
tpreseau@B:~$ cat /home/tpreseau/.ssh/authorized_keys
```

copier la clé publique de tpreseau de la machine A dans le compte tpreseau de la machine B :
```
tpreseau@A:~$ ssh-copy-id ip_B
```

Maintenant, vérifier le contenu du fichier :
```
tpreseau@B:~$ cat /home/tpreseau/.ssh/authorized_keys
```

Vous pouvez maintenant vérifier que la commande
```
tpreseau@A:~$ ssh ip_B
```
ne demande pas de mot de passe.

Analyse des traces

Donner la liste des adresses IP qui ont vu la page truc.html
```
grep truc.html access.log
grep truc.html access.log | cut -d" " -f1
grep truc.html access.log | cut -d" " -f1 | sort
grep truc.html access.log | cut -d" " -f1 | sort | uniq -c
grep truc.html access.log | cut -d" " -f1 | sort | uniq -c | sort -rn
```

utiliser man grep, man cut, man sort, man uniq pour bien comprendre chacune des étapes

Obtenir la liste des adresses IP qui se sont connectées le 8 février entre 7h et 7h15 et le nombre de fois où chacune d'elle s'est connectée. Avec la suite des commandes suivantes, expliquer comment on arrive au résultat.
```
grep "08/Feb/2014:07:0" access.log
grep "08/Feb/2014:07:1[0-5]" access.log
grep "08/Feb/2014:07:0\|08/Feb/2014:07:1[0-5]" access.log
grep "08/Feb/2014:07:0\|08/Feb/2014:07:1[0-5]" access.log | cut -d" " -f1 |sort
|uniq -c
```

Obtenir la liste des adresses ip qui se sont connectées le 9 février entre 7h05 et 7h15 et qui ont vu la page bidule.html et le nombre de fois où ces deux conditions se sont produites.

Donner tous les jours où l'adresse IP 192.168.11.53 s'est connecté. Utiliser la commande man sed
```
grep 192.168.11.53 access.log
grep 192.168.11.53 access.log| sed -e 's/.*\[//'
grep 192.168.11.53 access.log| sed -e 's/.*\[//' -e 's/:.*//'
grep 192.168.11.53 access.log| sed -e 's/.*\[//' -e 's/:.*//'|uniq -c
```