

TP 5 Partie 1 : Supervision

Objectifs :

- se familiariser avec les différentes méthodes de surveillance du système d'information
- avoir une première expérience du protocole SNMP

Pré-requis :

- Vérifier la présence du logiciel de virtualisation Oracle VM Virtualbox
- Créer un répertoire de travail dans lequel seront stockés vos documents et les fichiers de vos VM.
- Récupérer le fichier iso d'installation CentOS-8.2.2004-x86_64-boot.iso par le réseau de CentOS 7 sur le site suivant par exemple

http://mirrors.sohu.com/centos/8.2.2004/isos/x86_64/CentOS-8.2.2004-x86_64-boot.iso

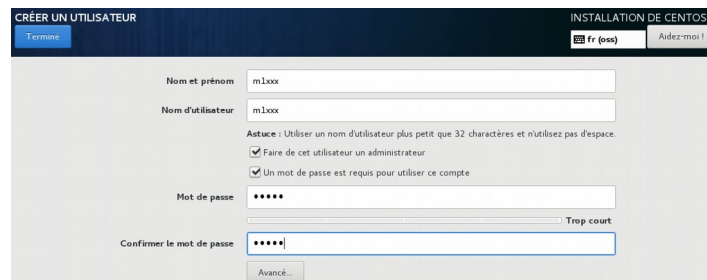
1 Installation et configuration d'un agent SNMP (Centos)

Créer une VM nommée `snmpclient` avec les caractéristiques suivantes :

- VM Linux/RedHat(64-bit)
- Mémoire vive 1024Mo
- 8 Go de disque
- 2 cartes réseau dans les modes suivants: Carte 1 = Bridge Carte 2 =NAT
- le reste par défaut
- Modifier la VM pour ajouter le « Presse papier bidirectionnel » (Général / Avancé)

Lancer l'installation de Centos de votre VM avec comme lecteur de CDROM le fichier CentOS-8.2.2004-x86_64-boot.iso en suivant les instructions suivantes :

- Langue *Français*
- Réseau et nom d'hôte : activer les cartes réseaux et renseigner le nom d'hôte `snmpclient`.
- Source d'installation : renseigner le miroir « Sur le réseau / Miroir le plus proche »
- Destination d'installation : choisir le *disque dur en partitionnement automatique*
- Sélection de logiciel : Installation minimale
- Commencer l'installation
- Mot de passe administrateur (root): `admin2020`
- Nom complet du nouvel utilisateur (cocher la case « faire de cet utilisateur un administrateur ») : `m1xxx`
- Identifiant pour le nouvel utilisateur: `m1xxx`
- Mot de passe pour le nouvel utilisateur: `m1xxx`



- Redémarrer (en enlevant l'image d'installation du centos).

Installation des outils réseaux :

La gestion des paquets est faite sur redhat/centos avec l'utilitaire yum ; la commande **yum whatprovides** suivi d'un nom de programme permet d'afficher le paquet contenant le programme. Rechercher le paquet qui contient les commandes d'administration et de configuration réseau (netstat, ifconfig...)

→ Installer ce paquet

Installation de snmp

Net-snmp est un projet opensource qui fournit une version de snmp très complète, ainsi que de nombreuses ressources (tutoriels, samples) : <http://www.net-snmp.org>

→ Installer le service snmpd et ses dépendances avec la suite net-snmp :

→ Activer le service snmpd :

→ Démarrer le service snmpd

Q1. Reporter dans votre rapport les commandes utilisées

Prise en main de snmp

Snmp est un protocole d'échange de données de configuration des équipements du système d'information (ordinateurs, équipements réseaux, appliances, onduleurs ...).

Les informations de configuration, pour qu'elles soient acceptées par le protocole SNMP, doivent être formatées et structurées selon un format précis : la Management Information Base (MIB). On parle de MIB pour désigner un ensemble d'information SNMP.

Les informations à l'intérieur d'une MIB sont couramment appelées des OIDs.

Chaque constructeur ou éditeur qui souhaite « ouvrir » ses équipements au protocole SNMP va publier sa MIB. Il existe ainsi de nombreuses MIBs, dont vous pouvez voir une liste sur ce site :

<http://www.oidview.com/mibs/detail.html>

Les MIBs sont transcrites dans des fichiers textes ascii, et l'installation de net-snmp amène de nombreuses MIBs lors de l'installation.

Q2. Trouver sur la machine snmpclient le répertoire où sont stockées les MIBs.

Les MIBs respectent les caractéristiques d'une base de données Objet et Hiérarchique.

Q3. Donner de façon succincte les caractéristiques de la modélisation Objet et Hiérarchique des données ?

Parmi les méthodes qui permettent d'interagir avec les MIBs, il existe :

snmpget : lecture d'un OID

snmpwalk : lecture complète d'une MIB

snmpset : écriture d'un OID

Q4. Exécuter la commande suivante et commenter le résultat ainsi que la signification des paramètres :

```
snmpwalk -c public -v1 snmpclient
```

Quel est le résultat ?

Pour ajouter le service snmp à la liste des services autorisés par le pare-feu de snmpclient, utiliser la commande :

```
sudo firewall-cmd --add-service=snmp
```

Vérifier que le service a bien été pris en compte :

```
sudo firewall-cmd --list-all
```

Tester à nouveau la connectivité à l'agent snmp de la vm :

```
snmpwalk -c public -v1 <@IP de snmpclient>
```

Configuration de snmp

La configuration de l'agent snmpd se fait dans le fichier /etc/snmp/snmpd.conf.

Dans ce fichier, vous allez modifier la ligne suivantes :

```
com2sec notConfigUser default public
```

pour

```
com2sec notConfigUser default mlxxx
```

De manière à ce que l'agent SNMP sur la machine snmpclient puisse accéder à l'ensemble des métriques « système », il faut modifier la partie qui concerne la view : changer les deux lignes pour donner accès à votre communauté à l'arbre des OID à partir de 1.3.6.1.2.1 :

```
view systemview included .1.3.6.1.2.1
#view systemview included .1.3.6.1.2.1.25.1.1
```

Redémarrer le service snmpd

```
sudo systemctl restart snmpd
```

Exécuter à nouveau la commande snmpwalk vue précédemment.

Q5. Que se passe-t-il ? Pourquoi et que faut-il modifier dans la commande pour qu'elle fonctionne à nouveau ? Quel est le rôle de la communauté ?

2 Création de la seconde VM (super-serveur)

Pour créer la VM qui hébergera le serveur de supervision, cloner la vm snmpclient (clone intégral).

Modifier la configuration réseau pour ne laisser que la carte en mode NAT.

Q6. Que faut-il configurer pour que le serveur web et ssh de super-serveur soient accessibles depuis le PC hôte et/ou la VM snmpclient ?

Configurez la redirections suivantes :

PC hôte port 5580 vers la VM port 80

PC hôte port 5522 vers la VM port 22

Changer le hostname de cette machine (commande `hostnamectl`) avec la valeur : super-serveur :

```
hostnamectl set-hostname super-serveur
```

Déconnecter vous et reconnecter vous pour vérifier que le prompt vous indique le nouveau nom du serveur :

```
[mlxxx@super-serveur ~]$
```

3 Nagios XI

Installation de Nagios sur super-serveur

Nagios est une solution de supervision dont le noyau (Core) est open source ; nous allons installer la version Nagios XI qui est en licence Nagios mais dispose d'une période d'essai de 60 jours.

Créer un utilisateur qui sera propriétaire de l'installation de Nagios XI :

```
sudo adduser nagiosuser
sudo passwd nagiosuser
```

Mettre nagios2019 en mot de passe

```
sudo gpasswd -a nagiosuser wheel
```

Cette dernière commande permet d'autoriser nagiosuser à exécuter des programmes en root.

Connectez vous en nagiosuser et exécuter les commandes suivantes :

```
sudo yum install wget
cd /tmp
wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
tar xzf xi-latest.tar.gz
cd nagiosxi
sudo ./fullinstall
```

Répondre Y à la question « Do you want to continue ? ». L'installation est assez longue et peut durer 10 à 15 minutes.

Une fois l'installation terminée, ouvrez sur votre PC hôte un navigateur à l'adresse :

<http://localhost:5580/nagiosxi>

Et finalisez l'installation en spécifiant :

- mot de passe nagiosadmin : nagiosadmin
- décocher la case « Send this account email notifications »
- laisser les autres champs par défaut et cliquer sur Finalize

Connectez vous ensuite à nagios xi avec l'utilisateur nagiosadmin/nagiosadmin.

Prise en main de Nagios XI

Nagios XI est un outil de supervision qui donne l'état des systèmes (hosts) et des services qu'il connaît.

Naviguer dans le menu Details > Host status.

Q7. Quel est le host que connaît votre serveur Nagios XI ?

Idem pour les services (menu Service Status).

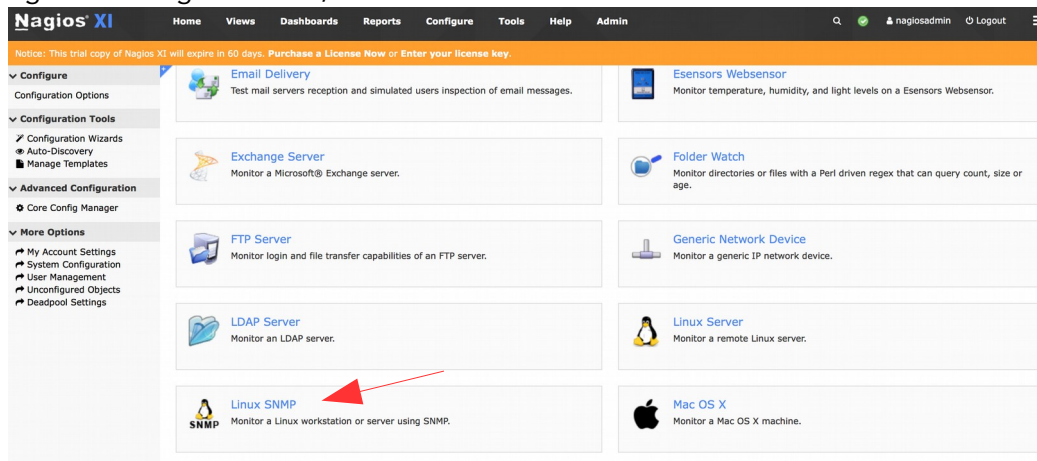
Prenez le temps de naviguer dans ces deux menus :

- voir notamment comment est déterminé l'état des services, à quelle fréquence, combien de tentatives sont possibles, etc...
- regarder les possibilités des graphes de performance

Q8. Arrêter le service sshd sur le super-serveur, et vérifier que le changement est bien détecté par Nagios XI.

Ajout du snmpclient dans Nagios XI

Menu Configure > Configure Wizard, et choisir Linux SNMP



Renseigner l'IP (bridge) de la VM snmpclient et la communauté m1xxx.

Sélectionner la surveillance du service sshd dans l'écran suivant et laisser les autres paramètres par défaut.

Cliquer ensuite sur Finish.

Retrouver l'état de la VM snmpclient sur les pages Host Status et Service Status.

A LA FIN DE CETTE PARTIE CONSERVEZ VOS VMS QUI VOUS SERVIRONT EN PARTIE 2