TP1 :

Préparation de l'environnement à superviser

Khalid Ôchi

L'objectif de ce premier TP est de mettre en place les outils nécessaires à la supervision, et de vous familiariser avec les commandes de base de SNMP.

A la fin du TP, vous devez avoir effectué :

1. La mise en place du serveur (DNS) pour la résolution des noms d'Hôtes internes.
2. L'installation du serveur SNMP (snmpd/Agent) sur la machine.
3. L'installation du moniteur (Client) sur la même machine
4. Effectuer les opérations de supervision de base (telles que **snmpwalk**, ***snmpget et snmptranslate***).
5. Visualisation des différentes composantes de la MIB-II par l'interface GUI.

Prérequis logiciels:

1. Linux (machine virtuelle ou physique) Debian.

Introduction

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux. SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications: les bases de données, les serveurs, les logiciels, etc.

L'environnement de gestion SNMP est constitué de plusieurs composantes : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole. Les différentes composantes du protocole SNMP sont les suivantes:

Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer. Cela va d'une station de travail à un concentrateur, un routeur, un pont, etc. Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision. Les agents sont

des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion comme par exemple le nombre de paquets en reçus ou transmis.

- La station de supervision (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.
- La MIB (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.
- Le protocole, qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

1. Installation du Serveur de noms (DNS) :

Il convient plus d'utiliser des noms de machines plutôt que des adresses IP, le serveur DNS se chargera de cette correspondance.

Le service DNS sous GNU/Linux est représenté par le Daemon BIND9. Pour l'installer, on tape :

La configuration se fait principalement en trois étapes :

- La déclaration de la zone et de la zone inverse.

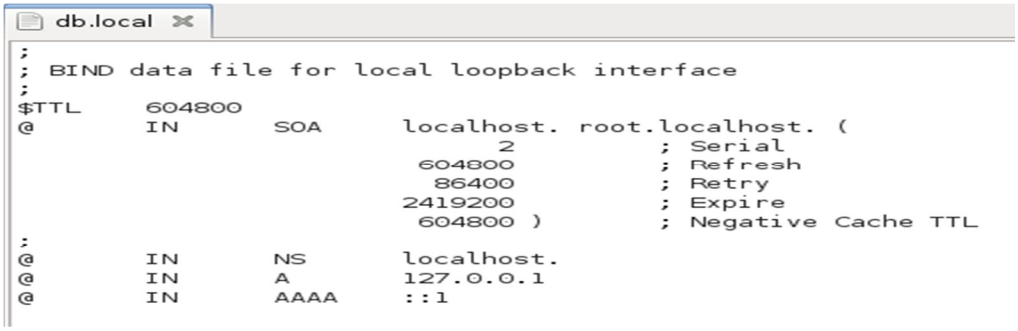
```
root@ensias-pc:~# apt-get install bind9
```

- Définition de la zone.
- Définition de la zone inverse.

Commençons par la déclaration des zones, et éditons le fichier /etc/bind/named.conf.local :

```
zone "rsensias.ma" {
        type master;
        file "/etc/bind/db.rsensias.ma";
};
zone "0.1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.rsensias.inv";
};
```

Commençons tout d'abord par visualiser le contenu du fichier : /etc/bind/db.local :



Il s'agit de la définition de zone locale, on se basera sur cette définition pour créer le domaine **rsensias.ma.**

Enregistrez une copie du fichier sous le nom indiqué dans la section : file du fichier named.conf.local, et modifiez-le pour renseigner l'adresse de l'interface ETH0, le nom FQDN de la machine, et les serveurs de la salle, de la façon suivante :

Nom_de_la_machine1	IN	A	Adresse_IP
Nom_de_la_machine2	IN	A	Adresse_IP

De la même façon, créez le fichier de résolution inverse.

Testez ensuite la configuration en utilisant la commande **nslookup mon_domaine.**

2. Installation de l'agent (SNMPD) et du superviseur(SNMP)

Pour pouvoir obtenir les paquets nécessaires, il est nécessaire d'ajouter des sources d'installation externes :

- Les MIB ne sont plus disponibles nativement sur les nouvelles distributions de linux.
- Nous utiliserons un browser de MIB qui n'est désormais plus disponible sur Squeeze (mbrowse).

Pour ces raisons, nous ajouterons ces lignes dans le fichier de configuration /etc/apt/sources.list.

```
deb http://ftp.fr.debian.or/debian squeeze main non-free

deb http://ftp.de.debian.org/debian lenny main

deb http://security.debian.org/ squeeze/update main contrib

deb-src http://security.debian.org/ squeeze/update main contrib
```

Il faut installer les paquets : **snmpd, snmp, mbrowse, Scli, snmp-mib-downloader.**

1) Configurer le fichier /etc/snmp/snmpd.conf

La première chose à faire étant d'indiquer le nom de communauté. Il s'agit d'un type d'authentification SNMP – pour les versions 1 et 2c - définissant un type accès qui peut être en lecture seule (RO) ou encore en Lecture/Ecriture (RW).

L'accès en écriture permet de modifier des paramètres au niveau de la machine supervisée, sans avoir recours à sa console. Un avantage certain, qui tourenra mal si la cible n'est pas protégée correctement.

Les noms de communautés par défaut sont public (RO) et private (RW) qu'il faut évidemment éviter … ensuite, on pourrait définir d'autres attributs comme le contact de l'administrateur ou encore la localisation. Voici un exemple :

```
rocommunity  test
rwcommunity  test2
syslocation  kitchen
syscontact  "root"
```

2. Créez la communauté **rsensiasrw** pour l'accès en écriture et **rsensiasro** pour l'accès en lecture seule.
3. Personnaliser les autres attributs selon votre choix.

Il faut définir ensuite quels données seront accessibles par les communautés ci-dessus.

4. Allez à la section **ACESS CONTROL** . et déclarez une vue « **TOUT** » pour l'accès à toute l'arborescence, après ces lignes.

```
###############################################################################
#
#  ACCESS CONTROL
#

                                                #  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1
```

5. Ensuite affecter cette vue à la communauté **rsensiasrw**, et la vue **systemonly** à **rsensiasro** **.**
6. Allez ensuite à la section concernant l'agent, et modifiez les paramètres pour que votre machines soit accessible seulement depuis votre réseau local.
7. Explorez le reste du fichier de configuration et notez les sections **SYSTEM INFORMATION** et **ACTIVE MONITORING** . Fermez le fichier et redémarrez le serveur.

2) Consultation de la MIB

1. Commencez par tapper la commande : **snmpwalk -c « communauté » -v 1 localhost.**Observez le résultat de la commande en changeant le nom de communauté.
2. Maintenant, tappez la commande **snmpwalk -c « communauté » -v 1 localhost sysContact.**

Remarquez l'arborescence à laquelle appartient **sysContact**, ainsi que sa valeur, et son type.

3. Tappez maintenant la commande **snmpget** avec les même paramètres décris en haut.

Refaites le même test , cette fois, en renseignant toute l'arborescence de **sysContact**.

4. Quelle conclusion pouvez vous faire à propos de **snmpget** et **snmpwalk,** et quel est le rôle du zero à la fin pour **snmpget** ?
5. Maintenant, tappez la commande **snmptranslate –On « arborescence ».**

Essayer à nouveau **snmpget** avec l'OID que vous venez de récupérer.

6. Déduisez le rôle de **snmptranslate** et l'importance de la MIB dans snmp.
7. Dans une console, tappez la commande **mbrowse.** Amusez-vous à découvrir les MB qu'on a installées. Faites des GETs en changeant les adresses IP en ceux des voisins.
8. Tappez dans une console **scli** et faites des manipulations de votre choix pour récupérer des informations sur votre machine supervisée.