

FOSSIER Dimitri
GELUS Jean-Philippe
GRATTA Florent
SOUBEYRAND Rémi
THEVENON Julien

TP sur SNMP

1. Installation / configuration

Dans cette première partie, allez sur le site de **net-snmp** (<http://net-snmp.sourceforge.net>). Ce site servira de référence pour la syntaxe des commandes. Vous avez soit la possibilité d'installer **net-snmp** à partir des sources, soit à partir des packages debian.

Pour ce TP, on se servira des packages debian. Vérifiez si **net-snmp** est installé sur les images Linux, et si ce n'est pas le cas, installez le (packages **snmp** et **snmpd**).

Rechercher les fichiers de configuration. Où se trouve le fichier **snmpd.conf** ? et les fichiers des MIBs ?

On va maintenant s'intéresser aux commandes classiques de **net-snmp**, pour interroger sa propre machine.

Vous penserez à utiliser les commandes **tcpdump**, **netstat** et **ethereal** pour vérifier les manipulations suivantes :

- a) La commande **snmptranslate** permet d'établir la correspondance entre l'OID et le nom du nœud concerné. Quel est l'OID de **sysContact** ?
- b) Affichez l'arbre de la hiérarchie **System**.
- c) Récupérez, sur une autre machine que la votre, la description de la machine grâce à la commande **snmpget**
- d) A l'aide de la commande **snmpset**, modifiez le nom de la personne chargée « administrativement » de s'occuper de la machine. Attention, pensez à analyser la bonne MIB ou utilisez les commandes précédentes pour connaître le champ qui doit être modifié. De la même manière, modifiez le paramètre **sysUpTime** de la machine...
- e) Observez le nombre de trames nécessaires pour transmettre plusieurs OID
- f) A l'aide de la commande **snmp** correspondant à **GET-NEXT**, récupérez la situation géographique de la machine.

Les commandes vu précédemment permettent de faire des requêtes simples à notre agent SNMP. Mais grâce à la commande **getnext** on a accès à la valeur de la MIB localisée juste après celle qui a été demandée, cela permet de parcourir l'arbre de la MIB à coup de **getnext**.

Créez un script shell qui permet de parcourir la MIB en utilisant cette méthode.

Comparez le résultat de votre script avec la commande :

```
snmpwalk localhost public | more
```

Vous l'avez peut-être remarqué avec la commande **snmpwalk** précédemment, on n'accède pas par défaut à autre chose qu'au groupe **system** : cela provient de la configuration de **snmpd**.

Vous allez donc éditer le fichier de configuration de **net-snmp** pour autoriser l'accès à tout le sous-arbre **.iso.org.dod.internet.mgmt.mib-2**

Vérifiez que votre modification fonctionne.

Sur une machine distante, ouvrez une connexion SSH, ainsi qu'une connexion FTP en localhost. A la base de la table **tcpConnTable**, récupérez l'état des connexions ainsi que les ports utilisés pour les connexions TCP.

2. Génération de traps

Générez des traps à destination de votre machine locale.

Vérifiez qu'elles sont bien interceptées à l'aide de l'écouteur de traps.

Envoyez ensuite des traps à une machine distante puis réalisez un script afin d'automatiser cette tâche.

3. Commandes supplémentaires

Vous pouvez expérimenter les commandes comme **snmptable**, **snmpget**, **snmpset**,... sur la machine **test.net-snmp.org** (voir le site **net-snmp.sourceforge.net** pour avoir des informations) ou sur une machine de la salle de TP.

4. Activation du protocole sur les routeurs, l'imprimante et les switches

A l'aide du manuel d'utilisation des routeurs Cisco, configurez le routeur de votre poste pour qu'il soit accessible par le réseau. Activez le serveur SNMP.

Interrogez ensuite le serveur pour vérifier que le serveur SNMP fonctionne.

Profitez en pour récupérer les informations du routeur (Nom, localisation ...)

.

N.B. : les routeurs ne possèdent pas d'image au démarrage. Par conséquent, lors de la procédure d'initialisation, ne pas valider l'option **snmp** par défaut. Ceci doit être configuré manuellement.

Observez la manière dont on active l'agent SNMP de l'imprimante.

Vérifiez que les traps de l'imprimante sont activées et configurez la pour les recevoir sur votre machine.

Configurez ensuite le routeur pour générer des traps d'avertissement en cas de changement d'état des liens

ATTENTION :

- NE SUPPRIMEZ PAS LES LIGNES DES AUTRES BINOMES
- VERIFIEZ QUE LE NUMERO DE PORT SUR LEQUEL L'IMPRIMANTE ENVERRA LA TRAP EST BIEN CELUI ECOUTE PAR LE HANDLER

N.B. : adresse IP de l'imprimante : 192.168.130.220

Une fois que les traps sont configurées sur l'imprimante pour tous les groupes, déclenchez en une en provoquant un bouchage papier ou en plaçant un nombre de feuilles insuffisant pour une impression.

5. MIB

- Utilisation de **tkmib** :

Cet utilitaire permet de visualiser directement la MIB et obtenir les OID.
Utilisez le sur le routeur de votre poste.

- Cohérence de la MIB et **netstat**

A l'aide de commandes de base comme le **ping**, modifiez le nombre de paquets ICMP transmis et reçus. Vérifiez que le nombre donné à l'aide de l'outil **netstat** est cohérent par rapport à celui donné à base des commandes SNMP.

Vous effectuerez la même démarche concernant le contenu de la table de routage au niveau de la machine agent. Pour cela, vous rajouterez à la table de routage l'entrée suivante :

Adresse IP : adresse de votre choix

Gateway : adresse de votre choix

Interface : eth0

Observez les modifications dans la MIB grâce à tkmib.

Questions subsidiaires

Programmez un script qui effectue le **traceroute** à l'aide des commandes SNMP, de préférence en shell script.

Interrogez l'agent SNMP du switch