R5.02: SNMP - Simple Network Management Protocol

Jean-Marc Pouchoulon

Septembre 2024

Ce document a pour objet de découvrir le protocole SNMP, d'utiliser des clients graphiques et la ligne de commandes afin d'interroger des équipements présents sur l'IUT. Vous apprendrez à interroger un équipement en ligne de commandes avec les outils de la suite net-snmp, à naviguer dans une "mib tree" et à extraire des informations. Vous utiliserez une machine virtuelle sous Debian pour ce TD que vous pourrez ré-utiliser pour les autres TD/TP Supervision.

1 Installation du client SNMP et test sur un serveur containérisé Linux

La communauté public est la communauté en lecture seule et la communauté private est la communauté en lecture-écriture par défaut. Vous travaillerez par défaut avec la version 2c du protocole SNMP.

1. Installez le client SNMP sous Linux dans le container Docker registry.iutbeziers.fr/debianiut:latest

```
docker run -it registry.iutbeziers.fr/debianiut:latest bash
apt-get update
apt-get install snmp snmp-mibs-downloader
```

Remplacez la ligne MIBS: dans /etc/snmp/snmp.conf par

```
mibs +ALL
```

Modifiez /etc/snmp/snmp.conf pour

```
# Pour rendre accessible l'ensemble de l'arbre de la MIB et écouter sur l'IP du container ou de la machine
agentAddress udp:127.agentAddress udp:127.0.0.1,IPadresse_de_la_machine
```

Commentez les lignes suivantes dans /etc/snmp/snmpd.conf:

```
# Read-only access to everyone to the systemonly view
#rocommunity  public default -V systemonly
#rocommunity6 public default -V systemonly
```

Rajoutez

```
view all included .1
rocommunity public default -V all
rocommunity public localhost -V all
rocommunity public 172.17.0.2 -V all
```

Redémarrer le service snmpd (service snmpd restart)

Remplacez la mib qui génère une erreur (dangereux ne pas faire en prod) :

```
wget http://pastebin.com/raw.php?i=p3QyuXzZ -O /usr/share/snmp/mibs/ietf/SNMPv2-PDU
```

2 Interrogation d'un serveur Linux via SNMP

1. Lancez un container serveur SNMP via la commande suivante:

```
docker run --rm -p 161:161/udp  -p 162:162/udp -d \
   --hostname snmpserver -it  registry.iutbeziers.fr/snmpiut:latest
```

2. Interrogez ce container serveur SNMP (communauté publicbeziers)afin de retrouver les informations concernant les performances du serveur au travers de la MIB UCD-SNMP-MIB et HOST-RESOURCES-MIB. Inspirez vous de documentation fedora Vous retrouverez les informations suivantes concernant le serveur:
   - La mémoire totale de la machine.
   - L'uptime de la machine
   - Le nombre de process de la machine
   - L'espace de stockage utilisée sur la machine
   - La taille d'une unité d'allocation de stockage

   Utilisez snmptable afin de récupérez:
   - la table des interfaces réseaux.
   - la table des partitions.
   - la table des loadaverage
   - la table des IO.

3 Installation d'un serveur SNMP sous Linux

1. Installez le serveur SNMP sous DEBIAN

```
deb http://debian.iutbeziers.fr/debian/ bookworm contrib non-free
apt-get update
apt-get install snmp snmpd snmp-mibs-downloader libsnmp-dev

#Remplace la ligne dans /etc/snmp/snmp.conf par:
mibs +ALL

# Remplacer la mib qui génère une erreur (ne pas faire en prod) :
\begin{bashcode}
wget http://pastebin.com/raw.php?i=p3QyuXzZ -O /usr/share/snmp/mibs/ietf/SNMPv2-PDU
\end{bashcode}
```

2. Configurez et testez les traps SNMP.

   Vous devez installer le paquet snmptrapd

   ```
   apt-get install snmptrapd
   ```

   Sous /usr/bin installez ce petit shell affiche.sh:

   ```
   #!/bin/bash
   echo    "$(date)\n" >> /tmp/montrap
   ```

Configurez /etc/snmp/snmptrapd.conf avec les commandes suivantes:

```
authCommunity   log,execute,net public
traphandle default /bin/bash   /usr/bin/affiche.sh
```

Générez un trap à l'aide de snmptrap :

Modifiez /etc/default/snmptrapd afin d'activer trapd, redémarrer snmptrapd et vérifiez que /tmp/-montrap s'incrémente.

```
"snmptrap -v 2c -c public localhost "" UCD-SNMP-MIB::ucdStart"
```

Afin d'avoir accès à l'ensemble de l'arbre de la MIB remplacez les lignes suivantes de votre fichier /etc/snmp/snmpd.conf.

```
#  Default access to basic system info
#rocommunity public  default    -V systemonly
rocommunity publicbeziers
```

3. Monitorez à l'aide de SNMP le nombre de process Apache sur votre serveur.

   Installez et démarrer apache sur votre machine. Pour mettre en charge apache installez la commande ab (apache bench) et lancer 100 clients et 10000 requêtes :

   ```
   ab -c 100 -n 100000 http://localhost/
   ```

   Configurez snmpd.conf pour tester l'interrogation du nombre de process apache lancé. (déclarer un minimum et un maximum de process avec l'instruction "proc nom_du_processus max_process min_process") Visualisez avec la commande suivante si une alerte est positionné dans la mib.

   ```
   snmpwalk localhost -v2c -c public  UCD-SNMP-MIB::prTable
   ```

   Créez le shell nbprocess.sh ci-dessous qui renvoie le nombre de processus sur la machine

   ```
   # !/bin/bash
   ps -ef|wc -l
   ```

   Le programme doit être exécuté avec le bit setuid positionné pour avoir l'ensemble des process de la machine. Rajoutez dans snmpd.conf

   ```
   exec nbprocess /bin/sh /usr/bin/nbprocess.sh
   ```

   Interrogez snmp pour savoir le nombre de process qui tournent sur la machine.

4 Configurer SNMP sur les switchs CISCO

Vous pouvez au choix utiliser un switch 2960 ou un mini switch SG-250.

1. Configurez le switch cisco comme serveur SNMP avec une communauté RW *privatebeziers* et une communauté RO *publicbeziers* . Vous pouvez vous inspirer de `http://wiki.monitoring-fr.org/supervision/snmp-install`

   Exemple pour le 2960:

   ```
   enable
   conf t
   snmp-server community COMMUNAUTE_RESEAU ro 1
   snmp-server host @IP_SERVEUR_SUPERVISION COMMUNAUTE_RESEAU

   snmp-server community COMMUNAUTE_RESEAU RO 1
   snmp-server trap-source Vlan1
   snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
   ```

```
snmp-server enable traps tty
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps rf
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host @IP_SERVEUR_SUPERVISION COMMUNAUTE_RESEAU
```

Pour le SG-250 utilisez l'interface graphique du switch.

5 Installation d'un Browser de MIB

1. Pré-requis:

   Installez sur une VM le browser de mib de la société "ireasonning" en version pro depuis `http://ireasoning.com/downloadmibbrowserpro.shtml` ou installez et utilisez qtmib.
2. Installer les mibs Cisco:

   ```
   sudo apt-get install snmp-mibs-downloader
   ```

   ```
   sudo cp /usr/share/doc/snmp-mibs-downloader/examples/cisco*
   ```

   /etc/snmp-mibs-downloader/"

   ```
   cd /etc/snmp-mibs-downloader && sudo gzip -d ciscolist.gz
   ```

   ```
   # Modifiez
   ```

   /etc/snmp-mibs-downloader/snmp-mibs-downloader:"

   ```
   BASEDIR=/var/lib/mibs
   ```

   ```
   AUTOLOAD=
   ```

   rfc ianarfc iana cisco"

   ```
   # Modifiez /etc/snmp-mibs-downloader/ciscolist en supprimant les mib suivantes:
   ```

   ```
   CISCO-802-TAP-MIB
   ```

   ```
   CISCO-IP-TAP-CAPABILITY
   ```

   ```
   CISCO-IP-TAP-MIB
   ```

   ```
   CISCO-SYS-INFO-LOG-MIB
   ```

   ```
   CISCO-TAP2-CAPABILITY
   ```

   ```
   CISCO-TAP2-MIB
   ```

   ```
   CISCO-TAP-MIB
   ```

   ```
   CISCO-USER-CONNECTION-TAP-MIB
   ```

   ```
   # Download des MIBS
   ```

   ```
   sudo download-mibs
   ```

3. Retrouvez les informations que vous avez vu obtenu avec la ligne de commande dans le mib browser.
4. Visualiser la branche entreprise de la mib. Chargez les mibs Cisco précédemment installées sour /var/lib/mibs/cisco en modifiant le fichier /etc/snmp/snmp.conf

   Méthode alternative si le ftp Cisco ne répond pas: Clonez le dépôt git suivant `https://github.com/cisco/cisco-mibs.git` Chargez les mibs Cisco (directory V1,V2) dans le browser de mib et dans /usr/share/mibs/cisco.
5. Utilisez le browser pour parcourir votre switch Cisco.
6. Faites de même avec un routeur Cisco (physique ou gns3).

6 Configurez SNMP V3 sur votre serveur LINUX

1. Configurez un utilisateur SNMP sur votre serveur SNMP Linux et interrogez le:

```
net-snmp-config --create-snmpv3-user  -a SHA -A ceciestunlongmotdepasse1 \
 -x AES -X ceciestunlongmotdepasse2 securev3user

#Lancer un snmpwalk en version 3:
snmpwalk -v 3 -u securev3user -l authPriv -a SHA -A ceciestunlongmotdepasse1  \
-x AES -X ceciestunlongmotdepasse2 localhost
```

   Expliquer Utilisez tcpdump ou wireshark ou snmpget -d et analysez ce que veut dire authnopriv. Pourquoi y a t il deux mots de passes ?

7 Interrogation de serveurs windows via SNMP

Il vous faudra un serveur Windows... Utiliser votre propre serveur Windows. SNMP est activable dès la version 10 de Windows. L'adresse 10.6.0.1 vous permettra peut être de faire vous interrogation sur un serveur.

1. Interrogation de base d'un des serveurs 10.6.0 via snmp.
   a) Dumper l'ensemble des informations du serveur distant via un snmpwalk.
   b) Retrouver le système d'exploitation de la machine via un snmpget.
   c) Retrouvez l'uptime de la machine via un snmpget.
   d) Afficher l'arbre system de la mib à l'aide de la commande :

      ```
      snmptranslate -On -Tp SNMPv2-MIB::system
      ```
   e) Traduisez en oid SNMPv2-MIB::system et réciproquement.
   f) Retrouvez à l'aide de snmpnetstat la liste des connections TCP et UDP du serveur distant.
   g) A quoi sert la commande snmpgetnext ? Utilisez la pour retrouvez SNMPv2-MIB::sysContact.0

8 Utilisez SNMP afin de sauvegarder la configuration et rebooter votre switch CISCO 2960 à distance

1. Rebooter votre switch cisco via snmp

   Un matériel Cisco se "reboote" via SNMP. Pour cela il faut écrire dans la configuration:

   ```
   snmp-server system-shutdown
   ```

   et envoyer l'ordre de reboot via le set suivant:

   ```
   snmpset -v2c -c private 192.168.1.60 CISCO-SMI::local.9.9.0 i 2
   ```

   a) Utilisez `http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en` afin de retrouvez la MIB qui permet de réaliser ce reboot.
   b) Utilisez

```
snmptranslate -On -Td CISCO-SMI::local.9.9
```

que signifie le message ?

c) Installez la mib nécessaire pour la visualisation des différents FLAGS de reboot.

2. Sauvegardez votre switch Cisco par SNMP. Cisco permet de positionner dans une table SNMP les informations nécessaires à la sauvegarde des serveurs Vous devez d'abord configurer un serveur TFTP sur votre machine LINUX. Je vous propose d'utiliser tftpd-hpa.

```
apt-get install tftpd-hpa
# Modifiez /etc/default/tftpd-hpa

RUN_DAEMON="yes"
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure --create"
```

N'oubliez pas les permissions sur le fichier (666) Tester votre serveur tftp d'abord depuis le switch via un write net pour vous assurer que tout fonctionne bien. Vous pouvez vous inspirez de l'article suivant `http://www.ciscozine.com/how-to-save-configurations-using-snmp/`

```
snmpset -v2c -c private 192.168.1.60 \
ccCopyProtocol.25 i tftp \
ccCopySourceFileType.25 i runningConfig \
ccCopyDestFileType.25 i networkFile \
ccCopyServerAddress.25 a 192.168.1.50 \
ccCopyFileName.25 s sw01-confg
snmpset -v2c -c private 192.168.1.60  ccCopyEntryRowStatus.25 i active
snmpset -v2c -c private 192.168.1.60  ccCopyEntryRowStatus.25 i destroy
```