

## Exercices SNMP

=====

Remarque : Bon nombre de commandes utilisées dans cet exercice n'ont pas besoin d'être exécutées en tant que root, mais il est prudent de les exécuter toutes en tant que root. Il est donc plus simple de lancer un shell en tant que root et d'entrer toutes les commandes à ce niveau. Vous pouvez lancer un shell de root en entrant la commande ci-après :

```
$ sudo bash
```

### 1. Installation des outils client SNMP :

-----

```
# apt-get install snmp
```

### 2. Essai de SNMP

-----

Pour vérifier que l'installation SNMP est opérationnelle, exécutez la commande `snmpstatus` pour tester :

```
$ snmpstatus -c 'irenala' -v2c IP_ADDRESS
```

### 3. SNMP Walk et OID

-----

Vous allez maintenant utiliser la commande '`snmpwalk`', qui fait partie de la boîte à outils SNMP, sur chacun des équipements testés plus haut afin de lister les tables associées aux OID ci-dessous :

```
.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.31.1.1.1.18
.1.3.6.1.2.1.1.3.0
.1.3.6.1.4.1.2021.9
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

Vous essaieriez avec deux variantes de la commande '`snmpwalk`' :

```
$ snmpwalk -c 'irenala' -v2c IP_ADDRESS OID
```

et

```
$ snmpwalk -On -c 'irenala' -v2c IP_ADDRESS OID
```

... où OID est l'un des trois OID listés ci-dessus : `.1.3.6...`

Remarque : l'option "`-On`" active l'affichage numérique, à savoir : aucune conversion OID <-> MIB de l'objet n'aura lieu.

Pour ces OID :

a) Tous les dispositifs répondent-ils ?

b) Avez-vous remarqué quelque chose d'important à propos de l'OID sur la sortie ?

### 4. Configuration de SNMP sur votre routeur pfSense

-----

Connectez-vous à votre routeur pfSense virtuel, et vérifiez que SNMP y est déjà bien configuré:

```
http://192.168.56.254
```

Login par défaut : "admin", mot de passe "pfsense"

Si ce n'est pas le cas, il faut configurer SNMP.

Maintenant de retour sur votre PC (ouvrez un autre Terminal), effectuez un test en utilisant certains des OID de la section 3 ci-dessus.

```
$ snmpwalk -c 'irenala' -v2c IP_ADDRESS <OID>
```

Que se passe-t-il si vous essayez d'utiliser une chaîne de communauté erronée (en remplaçant par exemple "irenala" par autre chose) ?

## 5. Configuration de snmpd sur votre PC

-----

\* Installez l'agent SNMP:

```
# sudo apt-get install snmpd
```

\* Configuration :

Vous allez sauvegarder le fichier de configuration par défaut, et créer votre version à vous:

```
# cd /etc/snmp/  
# mv snmpd.conf snmpd.conf.dist  
# editor snmpd.conf
```

-- copier ici -----

```
# Listen for connections on all interfaces (both IPv4 *and* IPv6)  
agentAddress udp:161,udp6:[::1]:161  
# Configure Read-Only community and restrict who can connect  
rocommunity irenala <ADRESSE_IP>  
rocommunity irenala 127.0.0.1  
# Information about this host  
sysLocation  
Atelier iRENALA  
sysContact  
sysadm@test.irenala.mg  
# Which OSI layers are active in this host  
# (Application + End-to-End layers)  
sysServices 72  
# Include proprietary diskTable MIB (in addition to hrStorageTable)  
includeAllDisks 10%  
-- copier ici -----
```

Maintenant, sauvegardez et sortez de l'éditeur.

\* Relancez snmpd

```
# service snmpd stop  
# service snmpd start
```

## 6. Vérifiez que snmpd fonctionne :

-----

```
$ snmpstatus -c irenala -v2c localhost
```

Qu'observez-vous ?

## 7. Testez votre voisin

-----

Vérifiez maintenant que vous pouvez exécuter snmpstatus avec le serveur de votre voisin :

```
$ snmpstatus -c irenala -v2c IP_ADDRESS
```

## 8. SNMPwalk - le reste de la MIB-II

-----

Essayez d'exécuter snmpwalk sur des machines que vous n'avez pas encore testés

Notez le type d'informations que vous pouvez obtenir.

```
$ snmpwalk -c irenala -v2c IP_ADDRESS ifDescr  
$ snmpwalk -c irenala -v2c IP_ADDRESS ifTable  
$ snmpwalk -c irenala -v2c IP_ADDRESS ifAlias  
$ snmpwalk -c irenala -v2c IP_ADDRESS ifOperStatus  
$ snmpwalk -c irenala -v2c IP_ADDRESS ifAdminStatus  
$ snmpwalk -c irenala -v2c IP_ADDRESS if
```

Pouvez-vous expliquer la différence entre ifOperStatus et ifAdminStatus ?

Pouvez-vous imaginer un scénario où cela pourrait être utile ?

## 9. Autres choses intéressantes dans les MIB-OID

-----

\* Utilisez les OID du début de cette série d'exercices et examinez :

- a) les processus qui s'exécutent sur le serveur de votre voisin (hrSWRun)
- b) l'espace disque disponible sur le serveur de votre voisin (hrStorage)
- c) les interfaces sur le serveur de votre voisin (ifIndex, IfDescr)

Pouvez-vous utiliser des noms abrégés pour parcourir ces tables OID ?

\* Faites un essai avec la commande "snmptranslate", par exemple :

```
$ snmptranslate .1.3.6.1.4.1.2021.9.1.3.1
```

\* Essayez avec différents OID