SNMP exercises, Part II

Contents

1 Introduction

1.1 Goals

- Learn How to setup SNMPv3

1.2 Note

- SHA authentication and DES/AES encryption support is only available if you have OpenSSL installed.
- Encryption support now *is* enabled in the binary releases downloadable from the net-snmp web site.
- This description assumes you're using the software compiled from source, and so installed using the default prefix location (/usr/local).
- If you're working with a vendor-provided system, or have configured things with a different prefix, you'll need to adjust locations accordingly.

1.3 # CREATING THE FIRST USER:

First, you need to create a new snmpv3 user and give them rights to do things:

```
net-snmp-config --create-snmpv3-user -a "my_password" myuser
```

WARNING: SNMPv3 pass phrases must be at least 8 characters long!

The above line creates the user "myuser" with a password of "my_password" (and uses MD5 and DES for protection). (Note that encryption support isn't enabled in the binary releases downloadable from the net-snmp web site.) net-snmp-config will also add a line to your snmpd.conf file to let that user have read/write access to your agent. You may want to change this in your snmpd.conf file (see the snmpd.conf manual page). Run net-snmp-config –help for more information about it.

Start the agent and test your setup:

```
/usr/local/sbin/snmpd
   [...wait a few seconds...  It will run in the background and
    return you to your shell immediately.]

snmpget -v 3 -u myuser -l authNoPriv -a MD5 -A my_password localhost sysUpTime.0
   [ this should return information about how long your agent has been up]

snmpget -v 3 -u myuser -l authPriv   -a MD5 -A my_password
                                     -x DES -X my_password localhost sysUpTime.0
   [ this should return similar information, but encrypts the transmission ]
```

1.4 # CREATING A SECOND USER:

Start the agent (if you didn't do so above).

You can create as many users as you like using the above method, but this details another way of doing it while the agent is running by modifying the user database using the snmp protocol itself:

Now, lets create a second user using the first user (just for fun) for both authentication purposes and as a template (or "cloning source"):

```
snmpusm -v 3 -u myuser -l authNoPriv -a MD5 -A my_password localhost create wes myuser
```

The above should have created the user "wes" with the same password as the "myuser" user. So then, you need to change his password using:

```
snmpusm -v 3 -u wes -l authNoPriv -a MD5 -A my_password localhost passwd my_password new_pas
```

See, wasn't that easy? You can now create users. Wheeee....

But, you'll have to add a configuration line that allows them access to do things. Do this with another "rwuser" line in your /usr/local/share/snmp/snmpd.conf file (you'll need to stop and start the agent again, or send the agent a SIGHUP signal):

```
rwuser wes
```

Or, optional use the "rouser" token instead of the "rwuser" token to only grant them read-only access.

Now, test your new user:

```
snmpget -v 3 -u wes -l authNoPriv -a MD5 -A new_passphrase localhost sysUpTime.0
```

1.5 # FURTHER STUDIES:

1.6 Tired of all those command line authentication options?

put something like this in your $HOME/.snmp/snmp.conf file (make it readable only by you!!!):

```
defSecurityName wes
defContext ""
defAuthType MD5
defSecurityLevel authNoPriv
defAuthPassphrase new_passphrase
defVersion 3
```

And this is in place the last of the above example lines boils down to:

```
snmpget localhost sysUpTime.0
```