exercises-snmp.md

SNMP exercises

Introduction

Goals

- Install and learn to use the SNMP commands
- Explore and identify standard vs enterprise parts of the MIB tree
- Install vendor specific MIBs and use those with the SNMP commands

Notes

- Commands preceded with “$” imply that you should execute the command as a general user - not as root.
- Commands preceded with “#” imply that you should be working as root.
- Commands with more specific command lines (e.g. “rtrX>” or “mysql>”) imply that you are executing commands on remote equipment, or within another program.

Installing snmp client (manager) tools

Start by installing the net-snmp tools on your individual host. Connect via ssh to hostX.campusY:

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

The second of the two commands downloads the standard IETF and IANA SNMP MIBs which are not included by default.

Note: to find snmp-mibs-downloader, you must enable the “multiverse” source in your APT configuration. This has already been done for you in this workshop.

Now, edit the file `/etc/snmp/snmp.conf` :

```
$ sudo editor /etc/snmp/snmp.conf
```

Change this line:

```
mibs :
```

… so that it looks like:

```
# mibs :
```

(You are “commenting out” the empty mibs statement, which was telling the snmp* tools **not** to automatically load the mibs in the `/usr/share/mibs/` directory).

Save this file and exit.

Now, in your home directory make a `.snmp` directory with file `snmp.conf` inside it, make it readable only by you, and add the credentials to it:

```
$ cd
$ mkdir .snmp
$ chmod 700 .snmp/
$ editor .snmp/snmp.conf
```

Put the following contents in the file:

```
defVersion 3
defSecurityLevel authNoPriv
defSecurityName admin
defAuthPassphrase NetManage
defAuthType SHA
defPrivType AES

# Default community when using SNMP v2c
defCommunity NetManage
```

Creating this configuration file means you won’t have to enter your credentials everytime you use one of the SNMP utilities. Otherwise you would have to add all these values on the command line like this:

(this command will not yet work)

```
snmpstatus -v3 -l authNoPriv -a SHA -u admin -A NetManage
hostX.campusY
```

Configure SNMP on Your Campus Routers and Switches

For this exercise you need to work together as a group. You will be enabling and configuring snmp to run on each of your 4 campus network devices. This includes:

```
* bdr1.campusY
* core1.campusY
* dist1-b1.campusY
* dist1-b2.campusY
```

The commands to enable ssh are the same on each box, so divide the work between your group members.

Now connect to your campus network devices and on each do:

```
$ ssh nmmlab@DEVICE.campusY.ws.nsrc.org

username: nmmlab
password: <CLASS PASSWORD>

DEVICE.campusY> enable
Password: <CLASS PASSWORD>
DEVICE.campusY# configure terminal          (conf t)
```

Now we need to add an Access Control List rule for SNMP access, turn on SNMP, assign a read-only SNMP community string as well as a SNMPv3 group and user and tell the router to maintain SNMP information across reboots. To do this we do:

(Note that “Y” is equal to your campus number)

```
DEVICE.campusY(config)# snmp-server community NetManage ro 99
DEVICE.campusY(config)# snmp-server group ReadGroup v3 auth
access 99
DEVICE.campusY(config)# access-list 99 permit 100.68.Y.128
0.0.0.15
DEVICE.campusY(config)# access-list 99 permit 100.64.0.0
0.0.3.255
DEVICE.campusY(config)# snmp-server user admin ReadGroup v3 auth
sha NetManage
DEVICE.campusY(config)# snmp-server ifindex persist
```

Now let’s exit and save this new configuration to the routers permanent config.

```
DEVICE.campusY(config)# exit
DEVICE.campusY# write memory                    (wr mem)
DEVICE.campusY# exit                            (until you
return to your pc)
```

If you have questions about what the access-list statement is restricting ask your instructors.

Testing SNMP

To check that your SNMP installation works, run the snmpstatus command on each of the following devices from your host:

```
$ snmpstatus <IP_ADDRESS>
```

Where is each of the following:

```
* Campus border router:              100.68.Y.1
* Campus core switch:                100.68.Y.2
* Building 1 distribution switch:    172.2Y.10.2
* Building 2 distribution switch:    172.2Y.20.2
```

Note that you just used SNMPv3. Not all devices that implement SNMP support v3. Try again, adding “-v2c” as a parameter. Notice that the command automatically uses the community string in the snmp.conf file instead of the v3 user credentials. Try “-v1”. That is try:

```
$ snmpstatus -v2c <IP_ADDRESS>
```

and

```
$ snmpstatus -v1 <IP_ADDRESS>
```

What happens if you try using the wrong community string (i.e. change `NetManage` to something else) using the options “-v2c -c NetWrong”?

```
$ snmpstatus -v2c -c NetWrong <IP_ADDRESS>
```

SNMP Walk and OIDs

Now, you are going to use the `snmpwalk` command, part of the SNMP toolkit, to list the tables associated with the OIDs listed below, on each piece of equipment you tried above:

```
.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.31.1.1.1.18
.1.3.6.1.4.1.9.9.92.1
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

You will try this with two forms of the `snmpwalk` command:

```
$ snmpwalk <IP_ADDRESS> <OID>
```

and

```
$ snmpwalk -On <IP_ADDRESS> <OID>
```

… where `OID` is one of the OIDs listed above: .1.3.6…

…where `IP_ADDRESS` can be your group's router…

Note: the `-On` option turns on numerical output, i.e.: no translation of the OID <-> MIB object takes place.

For these OIDs:

a. Do all the devices answer?
b. Do you notice anything important about the OID on the output?

Configuration of snmpd (server/agent) on your host (hostX.campusY.ws.nsrc.org)

For this exercise your group needs to verify that the snmpd service is running and responding to queries for all machines in your group. First enable snmpd on your machine, then test if your machine is responding, then check each machine of your other group members.

- Install the SNMP agent (daemon) on your host

```
$ sudo apt install snmpd
$ sudo apt install libsnmp-dev
```

- Configuration

We will make a backup of the distributed config, and then we will create our own (be sure you mv "snmpd.conf" and *not* "snmp.conf"):

```
$ cd /etc/snmp
$ sudo mv snmpd.conf snmpd.conf.dist
$ sudo editor snmpd.conf
```

Then, copy/paste the following (change hostX.campusY to your own host and campus number) and replace "Y" with your campus number:

```
#  Listen for connections on all interfaces (both IPv4 *and*
IPv6)
agentAddress udp:161,udp6:161
```

```
# For SNMPv2: Configure Read-Only community and restrict who can
connect
rocommunity NetManage 100.64.0.0/22
rocommunity NetManage 100.68.Y.128/28
rocommunity NetManage 127.0.0.1
rocommunity6 NetManage 2001:db8:Y:1::/64
rocommunity6 NetManage ::1

# Information about this host
sysLocation    NSRC Network Management Workshop
sysContact     sysadm@hostX.campusY.ws.nsrc.org

# Which OSI layers are active in this host
# (Application + End-to-End layers)
sysServices    72

# Include proprietary dskTable MIB (in addition to
hrStorageTable)
includeAllDisks  10%
```

Now save and exit from the editor.

Now we will add the same SNMPv3 user to your PC. We need to stop snmpd before adding the user, and restart it to read the above changes as well as the new user:

```
$ sudo systemctl stop snmpd
$ sudo net-snmp-create-v3-user -ro -A NetManage -a SHA -x AES
admin
$ sudo systemctl start snmpd
```

Check that there are no errors in the config file:

```
$ sudo journalctl -eu snmpd
```

Check that snmpd is working:

Make an SNMP query to the agent which should now be running on your own host.

```
$ snmpstatus localhost
```

What do you observe? If you see an error or get no response, ask for help.

Test your neighbors

Check now that you can run snmpstatus against your other group members host.

```
$ snmpstatus host[1..6].campusY.ws.nsrc.org
```

For instance, in group 5, you should verify against:

```
* host1.campus5.ws.nsrc.org
* host2.campus5.ws.nsrc.org
* host3.campus5.ws.nsrc.org
* host4.campus5.ws.nsrc.org
* host5.campus5.ws.nsrc.org
* host6.campus5.ws.nsrc.org
```

and, so on.

Configuration of snmpd on your srv1.campusY.ws.nsrc.org server

Be sure that you install the snmp daemon (agent) on your campus server at this time. Select someone from your group to do this. Otherwise, it will be configured later as well.

At a minimum you need to complete sections 3 and 7 to 7.1.

Adding MIBs

Remember when you ran:

```
$ snmpwalk 100.68.Y.1 .1.3.6.1.4.1.9.9.92.1
```

If you noticed, the SNMP client (snmpwalk) couldn't interpret all the OIDs coming back from the Agent:

```
SNMPv2-SMI::enterprises.9.9.92.1.1.1.1.1 = STRING: "Cisco"
SNMPv2-SMI::enterprises.9.9.92.1.1.1.2.1 = STRING:
"92D8PBYYIWNV8D4765QH3"
SNMPv2-SMI::enterprises.9.9.92.1.1.1.3.1 = STRING: "IOSv"
SNMPv2-SMI::enterprises.9.9.92.1.1.1.4.1 = STRING: "1.0"
```

What is `9.9.92.1.1.1.4.1` ?

To be able to interpret this information, we need to download extra MIBs - and tell the snmp tools where to find them.

To see which directories the Linux net-snmp package looks in by default for MIB files, run this command:

```
$ net-snmp-config --default-mibdirs
/home/sysadm/.snmp/mibs:/usr/share/snmp/mibs:/usr/share/snmp/mib
s/iana:/usr/share/snmp/mibs/ietf
```

So we can either put them in one of those directories, or create a new directory for them. We'll choose a new directory, `/usr/share/snmp/mibs/cisco` , to keep them separate.

The MIBs we'll use are the following, but don't download them yet!

CISCO MIBS

```
ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
ftp://ftp.cisco.com/pub/mibs/v2/CISCO-ENTITY-ASSET-MIB.my
```

To make it quicker, we have a local mirror on `http://www.ws.nsrc.org/downloads/mibs/`

Download them now as follows:

```
$ cd /usr/share/snmp/mibs
$ sudo mkdir cisco
$ cd cisco

$ sudo wget http://www.ws.nsrc.org/downloads/mibs/CISCO-SMI.my
$ sudo wget http://www.ws.nsrc.org/downloads/mibs/CISCO-ENTITY-
ASSET-MIB.my
```

Now we need to tell the snmp tools that we have the cisco MIBS it should load. So edit the file `/etc/snmp/snmp.conf` (as root), and add the following two settings:

```
mibs +CISCO-SMI:CISCO-ENTITY-ASSET-MIB
mibdirs +/usr/share/snmp/mibs/cisco
```

Save the file, quit.

Now, try again (the example uses bdr1.campusY.ws.nsrc.org below. You can do this whichever network device you are configuring):

```
$ snmpwalk 100.68.Y.1 .1.3.6.1.4.1.9.9.92.1
```

What do you notice ?

SNMPwalk - the rest of MIB-II

Try and run snmpwalk on any hosts (routers, switches, machines) you have not tried yet, in the 100.68 address range.

Note the kind of information you can obtain.

(For your building distribution switches use 172.2Y.10.2 and 172.2Y.20.2)

```
$ snmpwalk 100.68.Y.1 ifDescr
$ snmpwalk 100.68.Y.1 ifAlias
$ snmpwalk 100.68.Y.1 ifTable | less
$ snmpwalk 100.68.Y.1 ifXTable | less
$ snmpwalk 100.68.Y.1 ifOperStatus
$ snmpwalk 100.68.Y.1 ifAdminStatus
```

(Remember that with `less` you press space for next page, `b` to go back to previous page, and `q` to quit)

Can you see what's different between `ifTable` and `ifXTable` ?

What do you think might be the difference between `ifOperStatus` and `ifAdminStatus` ? Can you imagine a scenario where this could be useful ?

More MIB-OID fun

- Use SNMP to examine:

a. the running processes on your neighbor's host (hrSWRun)
b. the amount of free diskspace on your neighbor's host (hrStorage)
c. the interfaces on your neighbor's host (ifIndex, ifDescr)

Can you use short names to walk these OID tables ?

- Experiment with the "snmptranslate" command, example:

```
$ snmptranslate .1.3.6.1.4.1.9.9.92.1
```

- Try with various OIDs