SNMP exercises

Goals

* Install and learn to use 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 client (manager) tools

Start by installing the net-snmp tools:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install snmp
$ sudo apt-get install snmp-mibs-downloader
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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

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

~~~~~~~~~~~~~~~~~~~
$ sudo vim /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)

* Install the SNMP agent (daemon)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install snmpd
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

* Configuration.

We will make a backup of the distributed config, and then we will
create our own:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd /etc/snmp
$ sudo mv snmpd.conf snmpd.conf.dist
$ sudo vim snmpd.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Then, copy/paste the following:

~~~~~~
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 bdNOG6 192.168.0.0/16
rocommunity bdNOG6 127.0.0.1

Information about this host
sysLocation   bdNOG6 Linux & Security Workshop
sysContact   sysadm@bdnog.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.

* Restart snmpd

~~~~~~
$ sudo service snmpd restart
~~~~~~

Check that snmpd is working:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ snmpstatus -c bdNOG6 -v 2c localhost
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

What do you observe ?

Test your neighbors

Check now that you can run snmpstatus against your other group members servers:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ snmpstatus -c bdNOG6 -v 2c www.groupxx.com.bd
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

For instance, you should verify against the following hosts:

Note : If DNS is not configured properly use server IP address instead
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
* www.group1.com.bd
* www.group10.com.bd
* www.group15.com.bd
* www.group18.com.bd
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Testing SNMP

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

~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ snmpstatus -c bdNOG6 -v 2c <IP_ADDRESS>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Where <IP_ADDRESS> is : 192.168.1xx.1

What happens if you try using the wrong community string (i.e. change `BdNOG6` to something else ?)

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
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

.1.3.6.1.4.1.9.9.13.1
.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 -c bdNOG6 -v 2c <IP_ADDRESS> <OID>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

and

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ snmpwalk -On -c bdNOG6 -v 2c <IP_ADDRESS> <OID>
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

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

...where `IP_ADDRESS` can be your group's server...

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 ?
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

MRTG LAB

Goals

- Gain experience with MRTG

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.

Exercises

0. Log in to your VM

1. Install MRTG

We will install MRTG and graph input/output data for the network interfaces on our classroom
routers - i.e. how much traffic is flowing across the router.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo apt-get install mrtg
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

When asked whether the file should be owned and readable only by root choose "<No>"

2. Create the /etc/mrtg directory

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo mkdir /etc/mrtg
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

3. SNMP RO Community string: "bdNOG6"

You will need this information later.

4. Find the IP and Name of the Server

You will do this exercises against your server. So, name and IP is

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
name: www.groupxx.com.bd
IP: 192.168.1XX.1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

So, for Group 3 the information would be:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
name: www.group3.com.bd
IP: 192.168.103.1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

You need this information for step 5 (below).

5. Run cfgmaker (the command below all on one line!)

Let's become the root user at this point:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo -s
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

You are now root and your prompt should have a "#" at the end to indicate this.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
mkdir -p /var/www/html/mrtg

/usr/bin/cfgmaker --output=/etc/mrtg/groupx.cfg --global 'workdir:
/var/www/html/mrtg' --global 'options[_]: growright,bits'
bdNOG6@192.168.1xx.1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

View the mrtg configuration file created by cfgmaker, you can make changes and see the results,
if you want (/etc/mrtg/groupx.cfg). For now, however, leave the file as it is.

6. Use indexmaker to create HTML files (all on one line!)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
/usr/bin/indexmaker --output=/var/www/html/mrtg/groupx.html
/etc/mrtg/groupx.cfg
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

7. Run MRTG command. Do this THREE TIMES! Really, *THREE TIMES*

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
LANG=C /usr/bin/mrtg /etc/mrtg/groupx.cfg
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

You will see some WARNING messages. Ignore these and repeat the command. After the third time you
should not see any more warnings.

8. Put the above command in a script

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
echo 'LANG=C /usr/bin/mrtg /etc/mrtg/groupx.cfg' >/etc/mrtg/mrtgscript
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Make the script executable:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
chmod +x /etc/mrtg/mrtgscript
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

9. Edit the crontab and insert the command to be run every 5 minutes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
crontab -e
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

If prompted for what editor to use, pick the one you prefer.

add:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
*/5 * * * * /etc/mrtg/mrtgscript
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

to the bottom of the file. Save the file and exit.

10. Run the mrtg script once manually to make sure we have some initial graphs

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
/etc/mrtg/mrtgscript
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

10. Load the browser through webserver

View the MRTG output in a browers. Point to your PC (pc1 through pc32):

http://www.group1xx.com.bd/mrtg/groupx.html

You will not see any results for a while - up to 10 minutes. At that point your graph should be moving.