Part 1 - Simple Network Management Protocol Lab

Installing the SNMP Manager Server

In this step, we will install the required software to use SNMP Daemon and Utilities. For more information refer to https://packages.ubuntu.com/search?keywords=snmpd

The steps to complete this section are:

- Update software
- Install required software
- Configure the SNMP Manager Server to download MIBs
- Configure the SNMP Agent Server
- Test SNMP
- Configure SNMP on a Cisco device

To install the required files open a terminal window and ssh to the server that will be used to install SNMP.

```
ssh apnic@192.168.30.10
```

NOTE: Type `yes` if asked about wanting to continue connecting

Password = `training`

Update the software repository for Ubuntu

```
sudo apt-get update
```

Password = `training`

Install required software

```
sudo apt-get install -y nano snmpd snmp snmp-mibs-downloader
```

By default the Management Information Base (MIBs) are not downloaded for the SNMP server. To configure the SNMP Manager Server to download the mibs, the `/etc/snmp/snmp.conf` needs to be updated. Add a hash (#) in front of **"mibs :"** to comment it out.

```
cat /etc/snmp/snmp.conf
grep -n "mibs :" /etc/snmp/snmp.conf
sudo sed -i 's/mibs \:/\#mibs \:/' /etc/snmp/snmp.conf
```

In the lab we are using the same server for SNMP Manager Server and SNMP Agent Server. To review the current SNMP Agent Server configuration view the snmpd.conf file with the following command:

```
sudo less /etc/snmp/snmpd.conf
```

NOTE: Press `q` to quit from the snmpd.conf output

First, we need to change the agentAddress directive. Currently, it is set to only allow connections originating from the local computer to port 161. To allow all connections on all interfaces (both IPv4 and IPv6)

```
sudo grep -in "agentaddress " /etc/snmp/snmpd.conf
sudo sed -i 's/127.0.0.1\,\[\:\:1\]/udp\:161\,udp6\:\[\:\:1\]\:161/' /etc/snmp/snmpd.conf
sudo grep -in "agentaddress " /etc/snmp/snmpd.conf
```

The **sed** command will change the text inside a file without having to use vi or another text editor.

To allow 192.168.0.0/16 network to do SNMP queries with community string of **training** add the following line to the "Access Control" section at the end of the file.

```
echo 'rocommunity training 192.168.0.0/16' | sudo tee -a /etc/snmp/snmpd.conf
```

OPTIONAL: Change the SYSTEM INFORMATION section to store details about the location and contact details

```
sudo grep -n "^sysLocation" -A 1 /etc/snmp/snmpd.conf
sudo sed -i 's/^sysLocation.*/sysLocation\tBrisbane\, Australia/' /etc/snmp/snmpd.conf
sudo sed -i 's/^sysContact.*/sysContact\ttraining\@apnic\.net/' /etc/snmp/snmpd.conf
sudo grep -n "^sysLocation" -A 1 /etc/snmp/snmpd.conf
```

View the SNMP Agent configuration file and confirm the above changes have been saved.

```
sudo less /etc/snmp/snmpd.conf
```

NOTE: Press `q` to quit from the snmpd.conf output

For any changes to the configuration file to take effect, force the snmpd service to stop and start or reload the configuration by running the following command(s):

```
sudo systemctl stop snmpd
sudo systemctl status snmpd
```

NOTE: Press `q` to quit from the snmpd status output

Start the service after confirming it is stopped

```
sudo systemctl start snmpd
```

Confirm SNMP is now listening on port 161 (udp) by running the following command:

```
ss -planu
netstat -planu
```

Use snmpwalk command to test SNMP.

```
snmpwalk -v2c -c training 192.168.30.10 | less
```

NOTE: Press `q` to quit from the snmpwalk output

> The snmpwalk command performs a whole series of getnexts automatically, and stops when it returns results that are no longer inside the range of the Object Identifier (OID) that was originally specified. To display all of the information stored on a machine in the system MIB group, for instance, use this command:

```
snmpwalk -v2c -c training 192.168.30.10 system
```

Or to get the system uptime only:

```
snmpwalk -v2c -c training 192.168.30.10 sysUpTime
```

The snmpget command can be used to retrieve data from a remote host given its host name, authentication information and an OID. As a simple example:

```
snmpget -v 2c -c training 192.168.30.10 system.sysUpTime.0
```

Configure SNMP on a Cisco device (R1)

Login Information for routers

Cisco Routers

```
username: apnic
password: training
enable password: labconfig
```

Juniper Routers

```
username: apnic
password: Tr@ining
```

Select IOS-R1 from the Resources tab.

Log into R1 and enter the Privileged EXEC mode.

User = `apnic` Password = `training`

To enter Privileged EXEC mode type the following

```
enable
```

Password = `labconfig`

Configure SNMP on a Cisco device

Configure the router interfaces on IOS-R1 .

> Check the lab topology and the table of IP/ASN assignment at the beginning of the instructions for details.

```
enable
conf t
int gi1
description link to SNMP Manager Server
ip address 192.168.30.1 255.255.255.0
no shutdown
int gi2
description link to R2
ip address 172.16.0.1 255.255.255.252
no shutdown
int gi3
description link to R3
ip address 172.16.0.5 255.255.255.252
```

```
no shutdown
exit
exit
```

To enable SNMP type the following commands:

```
enable
conf t
  access-list 99 permit 192.168.0.0 0.0.255.255
  snmp-server community training ro 99
end
wr
```

This will enable SNMP with community training. Network 192.168.0.0/16 can only do the SNMP query which is defined in access control list 99.

Test connectivity from R1 to the SNMP Manager Server:

```
ping 192.168.30.10
```

Select ubuntu-vm from the Resources tab.

Use snmpwalk command to test SNMP on R1.

```
snmpwalk -v2c -c training 192.168.30.1 | less
```

NOTE: Press `q` to quit from the snmpwalk output

To see how many interfaces there are, try the following snmpwalk command:

```
snmpwalk -v 2c -c training 192.168.30.1 IfName
```

More example commands are as following:

```
snmpwalk -v 2c -c training 192.168.30.1 IfDescr
```

```
snmpwalk -v 2c -c training 192.168.30.1 IfAlias
```

```
snmpwalk -v 2c -c training 192.168.30.1 IfOperStatus
```

```
snmpwalk -v 2c -c training 192.168.30.1 IfAdminStatus
```

Please click the Next button to continue.