Configuring SNMP

SNMP Config on devices

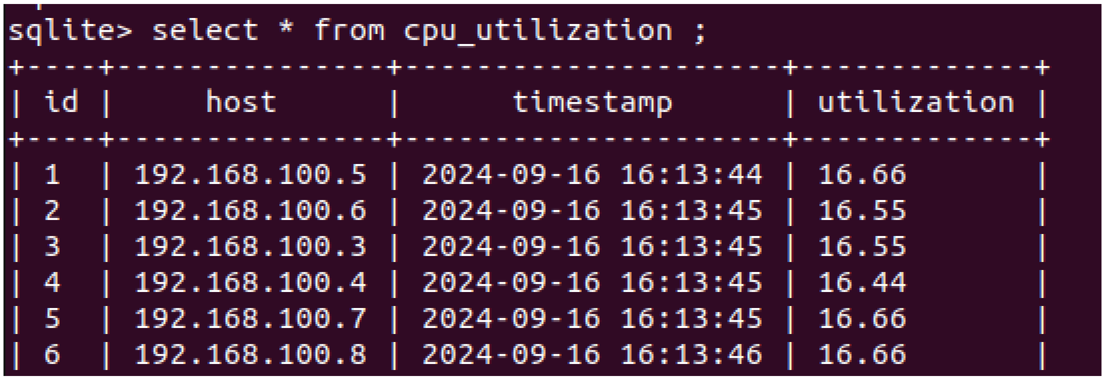
```
snmp-server local-interface Ethernet2.100
snmp-server community private rw
snmp-server community public ro
snmp-server host 192.168.100.2 version 2c public
snmp-server enable traps snmp link-down
snmp-server enable traps snmp link-up
```

Polling CPU Utilization from the devices

I have a monitor_cpu.sh script that polls in **1.3.6.1.2.1.25.3.3.1.2** OID from all the hosts to get the CPU utilization %. It then extracts the CPU % and stores it in an SQL database (**logs.db**) with **cpu_utilization** table. I have a **monitor_cpu.service** that runs this script:

```
student@csci5840-vm1-snir8112:/var/log/netman$ cat
/etc/systemd/system/monitor_cpu.service
[Unit]
Description=CPU Utilization Monitoring Service

[Service]
ExecStart=/usr/local/bin/monitor_cpu.sh
Restart=always
User=root
Group=root

[Install]
WantedBy=multi-user.target
```

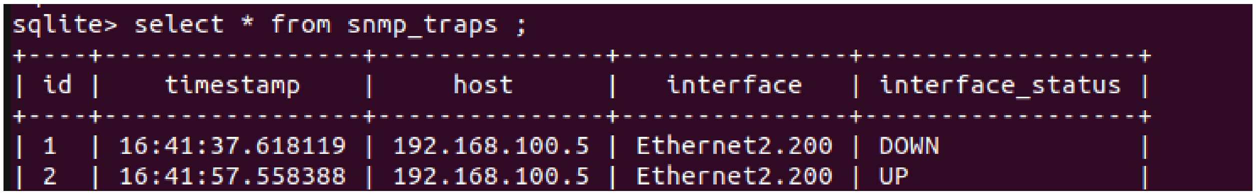
After this, I ran a `systemctl enable monitor_cpu` and `systemctl start monitor_cpu` to bring this service up.



```
sqlite> select * from cpu_utilization ;
+----+---------------+---------------------+-------------+
| id |     host      |      timestamp      | utilization |
+----+---------------+---------------------+-------------+
| 1  | 192.168.100.5 | 2024-09-16 16:13:44 | 16.66       |
| 2  | 192.168.100.6 | 2024-09-16 16:13:45 | 16.55       |
| 3  | 192.168.100.3 | 2024-09-16 16:13:45 | 16.55       |
| 4  | 192.168.100.4 | 2024-09-16 16:13:45 | 16.44       |
| 5  | 192.168.100.7 | 2024-09-16 16:13:45 | 16.66       |
| 6  | 192.168.100.8 | 2024-09-16 16:13:46 | 16.66       |
```

SNMP Traps

I have another service called snmptrap that runs the **capture_snmp_traps.sh** script. The script listens on port 162 for any traps sent by the devices. The devices only send traps for any link changes. Once a trap is received, it stores this trap to **logs.db** database under **snmp_traps** table.



```
sqlite> select * from snmp_traps ;
+----+-----------------+---------------+---------------+------------------+
| id |    timestamp    |     host      |   interface   | interface_status |
+----+-----------------+---------------+---------------+------------------+
| 1  | 16:41:37.618119 | 192.168.100.5 | Ethernet2.200 | DOWN             |
| 2  | 16:41:57.558388 | 192.168.100.5 | Ethernet2.200 | UP               |
```

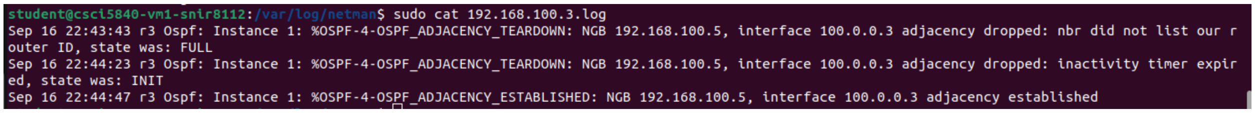
Syslog

For syslog, on the devices, I have enabled logging to the NMAS server:

```
logging trap debugging
logging host 192.168.100.2
```

1. I configured a config file under **/etc/rsyslog.d** which mentions that if any critical errors are received by a device, store it in a ***<ip_address>.log*** file under ***/var/log/netman***.

```
student@csci5840-vm1-snir8112:/etc/rsyslog.d$ cat netman.conf
# Direct logs from specific IP addresses to files in /var/log/netman
if $fromhost-ip == '192.168.100.5' then /var/log/netman/192.168.100.5.log
if $fromhost-ip == '192.168.100.6' then /var/log/netman/192.168.100.6.log
if $fromhost-ip == '192.168.100.3' then /var/log/netman/192.168.100.3.log
if $fromhost-ip == '192.168.100.4' then /var/log/netman/192.168.100.4.log
if $fromhost-ip == '192.168.100.7' then /var/log/netman/192.168.100.7.log
if $fromhost-ip == '192.168.100.8' then /var/log/netman/192.168.100.8.log

# Stop further processing of the log messages to prevent duplication
& stop
```



```
student@csci5840-vm1-snir8112:/var/log/netman$ sudo cat 192.168.100.3.log
Sep 16 22:43:43 r3 Ospf: Instance 1: %OSPF-4-OSPF_ADJACENCY_TEARDOWN: NGB 192.168.100.5, interface 100.0.0.3 adjacency dropped: nbr did not list our r
outer ID, state was: FULL
Sep 16 22:44:23 r3 Ospf: Instance 1: %OSPF-4-OSPF_ADJACENCY_TEARDOWN: NGB 192.168.100.5, interface 100.0.0.3 adjacency dropped: inactivity timer expir
ed, state was: INIT
Sep 16 22:44:47 r3 Ospf: Instance 1: %OSPF-4-OSPF_ADJACENCY_ESTABLISHED: NGB 192.168.100.5, interface 100.0.0.3 adjacency established
```

Netconf/GRPC config

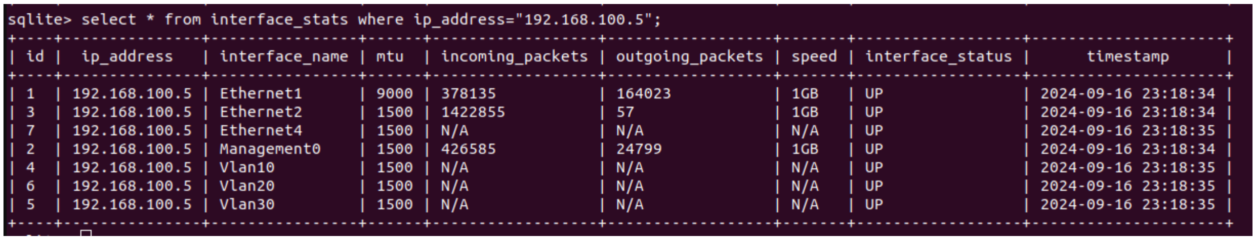
```
management api netconf
  transport ssh default

management api gnmi
  transport grpc default
        port 57400
```

Streaming interface statistics

I have a python script called **interface_stats.py** that polls in information every 1 second for every device for the following information:

a. Interface name
b. MTU
c. Speed
d. In packets
e. Out packets
f. Timestamp

And stores this information in logs.db database under **interface_stats** table.



```
sqlite> select * from interface_stats where ip_address="192.168.100.5";
+----+---------------+----------------+------+------------------+------------------+-------+------------------+---------------------+
| id |  ip_address   | interface_name | mtu  | incoming_packets | outgoing_packets | speed | interface_status |      timestamp      |
+----+---------------+----------------+------+------------------+------------------+-------+------------------+---------------------+
| 1  | 192.168.100.5 | Ethernet1      | 9000 | 378135           | 164023           | 1GB   | UP               | 2024-09-16 23:18:34 |
| 3  | 192.168.100.5 | Ethernet2      | 1500 | 1422855          | 57               | 1GB   | UP               | 2024-09-16 23:18:34 |
| 7  | 192.168.100.5 | Ethernet4      | 1500 | N/A              | N/A              | N/A   | UP               | 2024-09-16 23:18:35 |
| 2  | 192.168.100.5 | Management0    | 1500 | 426585           | 24799            | 1GB   | UP               | 2024-09-16 23:18:34 |
| 4  | 192.168.100.5 | Vlan10         | 1500 | N/A              | N/A              | N/A   | UP               | 2024-09-16 23:18:35 |
| 6  | 192.168.100.5 | Vlan20         | 1500 | N/A              | N/A              | N/A   | UP               | 2024-09-16 23:18:35 |
| 5  | 192.168.100.5 | Vlan30         | 1500 | N/A              | N/A              | N/A   | UP               | 2024-09-16 23:18:35 |
+----+---------------+----------------+------+------------------+------------------+-------+------------------+---------------------+
```