SNMP Notifications

Open SDN Controller provides the option to enable SNMP notifications via a RESTCONF request. When enabled, this service mirrors all of the notification messages that are generated by the Monit service and originates an SNMP trap that contains an NMS IP address and community string for each of these messages. Before you proceed, take note of the following points:

- SNMP version 2c is used.
- Traps are originated using SNMPv2-MIB, with a string based on the *Cold Start*, *sysName*, and *0* object identifiers (OID).
- SNMP gets are not currently supported, but may be in a future release.
- At this time, notifications can only be enabled or disabled. They cannot be modified.

This appendix contains the following topics:

Enabling SNMP Notifications

To enable SNMP notifications, you need to make a RESTCONF request using the platform services endpoint. The request's payload text should be structured as follows:

```
                    {
"snmp_nms_ip": "{{SNMP-receiver-IP-address}}"
"snmp_community_string": "{{SNMP-Community-string}}",
"snmp_state": "{{SNMP-state}}"
                    }
```

where:

- `snmp_nms_ip` is the IP address of the SNMP receiver or management station.
- `snmp_community_string` is the community string that that SNMP reads.
- `snmp_state` is the parameter whose value determines whether SNMP notifications are generated.

- To enable notifications, set its value to start.
- To disable notifications, set its value to stop.

An error will occur if you do not enter values for these parameters.

For more information, see Making RESTCONF Requests. When completing the procedure described here, note that you need to select the JSON data format in Step 6.

Key Files

The following table lists the files that are key to the functioning of SNMP notifications and their locations.

Filename	Location	Description
platform_services.log	/var/log	Logs error messages
monit.log	/var/log	Logs notifications generated by the Monit service
monit.log.offset	/var/log	Used for comparison with monit.log when new Monit service notifications are generated
views.py	/opt/cisco/platform/platform-services/app/modules/snmp	Contains REST API information
services.py	/opt/cisco/platform/platform-services/app/modules/snmp	Contains SNMP functions information
snmp-settings.json	/opt/cisco/platform/platform-services/data	Contains SNMP settings information

SNMP Notifications Implementation

When SNMP notifications are enabled, Open SDN Controller inserts an SNMP check into the crontab so that the Monit notifications log (monit.log) is checked for new entries every minute. Open SDN Controller then compares these new entries against the placeholders maintained in an offset file (monit.log.offset). The offset file is moved automatically to the end of the current Monit notifications log to prevent spamming.

When SNMP notifications are disabled, Open SDN Controller removes the SNMP check it inserted previously into the crontab. Until notifications are re-enabled, Open SDN Controller will not report any notifications that have been generated.

Troubleshooting

- Open SDN Controller's implementation of SNMP notifications relies on the Monit, cron, and Ansible services to work properly. If any of these services are not running, this feature may not work.

- To verify that the notification feature is working as expected:

  1. Log in as the user *sdn*.
  2. Run the following command:

     sudo python /opt/cisco/platform/platform-services/main/runcmd.py snmp_notify
  3. Confirm that a trap was sent to the SNMP NMS server.

  If the SNMP NMS server is not receiving messages, do the following:

  1. Check crontab to determine whether the SNMP job is scheduled (indicated by the following text):

     ```
     */1 * * * * python /opt/cisco/platform/platform-services/main/runcmd.py snmp_notify
     ```
  2. If scheduled, see if you can manually run the command listed in the previous step.
  3. If you are able to successfully run the command, check that UDP port 162 is open and that the Monit log file has been updated.
  4. Open the snmp-settings.json file and verify that the correct values are set for the snmp_nms_ip and the snmp_community_string parameters.
  5. Check for error messages in the platform_services.log file.