

Configure and troubleshoot Nexus Switch using SNMP

Contents

[Introduction](#)

[Background](#)

[Components used](#)

[Access recovery using SNMP](#)

[Configure using SNMP](#)

[Reference](#)

Introduction

This document describes how to troubleshoot and configure a Cisco Nexus Switch using SNMP

Background

Configuration of a Nexus switch can be modified if SNMP access is available

It is applicable for all Nexus platforms.

Components used

Nexus 5000 switch running version 5.1(3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Access recovery using SNMP

Device has a L3 interface (other than Mgmt 0) in default vrf

TFTP server should be accessible from this switch via default vrf and authentication disabled on TFTP server

Nexus device should be configured with SNMPv2 read-write community or V3 user

AAA authorization must be disabled

Following switch config

Switch config contains an ACL applied prevents accessing the device

```
N5K(config)# sh run int mgmt0
version 5.1(3)N2(1)
interface mgmt0
description "Testing with snmpv3"
ip access-group filter_internal_snmp_i in
vrf member management
ip address 10.22.65.39/25
```

Step 1 - Create a config file with the commands to change or roll back in the running config of Nexus switch:

Following example shows content of the config file for removing an ACL applied on the Mgmt 0 port

```
interface mgmt0
no ip access-group filter_internal_snmp_i in
Another example to reset the AAA settings to local authentication on the device
```

```
aaa authentication login local
```

Step 2 - Save the file with **.config** extension and place it inside the boot or home directory of the TFTP application

Step 3 - Perform an SNMP walk to the device to confirm reachability and its accessibility via SNMP

```
$ ./snmpwalk -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.10.222
```

Step 4 - Run the following commands from snmp-server (the highlighted ones need to be replaced by actual values)

Using snmp v2

```
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 i 5
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.2.222 i 1
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.3.222 i 1
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.4.222 i 4
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.5.222 a
<tftp_server>
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.6.222 s
<switch.config>
$ snmpset -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 i 1
$ ./snmpwalk -v2c -c <SNMPv2 RW communitiy><switch_ip> 1.3.6.1.4.1.9.9.96.1.1.1.1.10.222
```

Using SNMPv3

```
snmpset -v3 -l authNoPriv -u <SNMPv3 USER> -a MD5 -A <PASSWORD> <SWITCH_IP>
.1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer 6 ( to destroy any previous row )
snmpset -v3 -l authNoPriv -u <SNMPv3 USER> -a MD5 -A <PASSWORD> <SWITCH_IP>
.1.3.6.1.4.1.9.9.96.1.1.1.1.2.222 integer 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.3.222 integer 1
.1.3.6.1.4.1.9.9.96.1.1.1.1.4.222 integer 4 .1.3.6.1.4.1.9.9.96.1.1.1.1.5.222 a <TFTP_SERVER>
.1.3.6.1.4.1.9.9.96.1.1.1.1.6.222 s "switch.config" .1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.2.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.3.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.4.222 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.5.222 = IPAddress: <TFTP_SERVER>
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.6.222 = STRING: "switch.config"
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.14.222 = INTEGER: 4
```

SNMPv3 steps

```
snmpset -v3 -l authNoPriv -u admin -a MD5 -A ***** 10.22.65.39
.1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer 6 ( to destroy any previous row )
snmpset -v3 -l authNoPriv -u admin -a MD5 -A ***** 10.22.65.39
.1.3.6.1.4.1.9.9.96.1.1.1.1.2.222 integer 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.3.222 integer 1
.1.3.6.1.4.1.9.9.96.1.1.1.1.4.222 integer 4 .1.3.6.1.4.1.9.9.96.1.1.1.1.5.222 a 172.18.108.26
.1.3.6.1.4.1.9.9.96.1.1.1.1.6.222 s "switch.config" .1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer 4
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.2.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.3.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.4.222 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.5.222 = IPAddress: 172.16.1.1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.6.222 = STRING: "switch.config"
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.14.222 = INTEGER: 4
```

Switch config after the workaround

```
N5K-1(config)# sh run int mgmt0
version 5.1(3)N2(1)
interface mgmt0
description "Testing with snmpv3"
vrf member management
ip address 10.22.65.39/25
```

You can also look at the accounting logs to see if the command were executed. Config change done by SNMP appears as Root user -

```
N5K-1(config)# sh accounting log
Mon Aug  6 17:07:37 2018:type=start:id=vsh.5777:user=root:cmd
Mon Aug  6 17:07:37 2018:type=update:id=vsh.5777:user=root:cmd=configure terminal ; interface
mgmt0 (SUCCESS)
Mon Aug  6 17:07:37 2018:type=update:id=vsh.5777:user=root:cmd=configure terminal ; interface
mgmt0 ; no ip access-group filter_internal_snmp_i in (SUCCESS)
Mon Aug  6 17:07:37 2018:type=stop:id=vsh.5777:user=root:cmd=
```

Step 5 - Verify the access to the device by doing ab SSH/Telnet

Configure using SNMP

Config file as below

switch3.config:

```
vrf context management
ip route 0.0.0.0/0 10.128.164.1
end
SNMP command set
```

```
$ snmpset -v2c -c TEST 10.10.10.1 1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer 6 ( to clear any
previous line)
```

```
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.14.222 = INTEGER: 6
$ snmpset -v2c -c TEST 10.10.10.1 .1.3.6.1.4.1.9.9.96.1.1.1.1.2.222 integer 1
.1.3.6.1.4.1.9.9.96.1.1.1.1.3.222 integer 1 .1.3.6.1.4.1.9.9.96.1.1.1.1.4.222 integer 4
.1.3.6.1.4.1.9.9.96.1.1.1.1.5.222 a 172.18.108.26 .1.3.6.1.4.1.9.9.96.1.1.1.1.6.222 s
"switch3.config" .1.3.6.1.4.1.9.9.96.1.1.1.1.14.222 integer 4
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.2.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.3.222 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.4.222 = INTEGER: 4
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.5.222 = IPAddress: 172.18.108.26
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.6.222 = STRING: "switch3.config"
SNMPv2-SMI::enterprises.9.9.96.1.1.1.1.14.222 = INTEGER: 4
```

Accounting logs

```
Mon Sep  3 15:15:35 2018:type=update:id=snmp_62528_10.82.250.52:user=TEST:cmd=copy
tftp://172.18.108.26:69switch3.config running-config vrf management (SUCCESS)
Mon Sep  3 15:15:35 2018:type=start:id=vsh.12593:user=root:cmd=
Mon Sep  3 15:15:35 2018:type=update:id=vsh.12593:user=root:cmd=configure terminal ; vrf context
management (SUCCESS)
Mon Sep  3 15:15:35 2018:type=update:id=vsh.12593:user=root:cmd=configure terminal ; vrf context
management ; ip route 0.0.0.0/0 10.128.164.1 (SUCCESS)
Mon Sep  3 15:15:35 2018:type=stop:id=vsh.12593:user=root:cmd=
```

Reference

[Nexus Security configuration guide](#)

[NXOS password recovery](#)