Konfiguration und Fehlerbehebung für Nexus Switch mithilfe von SNMP

Inhalt

Einführung

Dieses Dokument beschreibt die Fehlerbehebung und Konfiguration eines Cisco Nexus Switches mithilfe von SNMP.

Hintergrund

Die Konfiguration eines Nexus-Switches kann geändert werden, wenn SNMP-Zugriff verfügbar ist.

Sie gilt für alle Nexus-Plattformen.

Verwendete Komponenten

Nexus 5000-Switch mit Version 5.1(3)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Wiederherstellung mit SNMP

Gerät hat eine L3-Schnittstelle (außer Mgmt 0) im Standard-VRF

Der Zugriff auf den TFTP-Server sollte von diesem Switch aus über Standard-VRF möglich sein. Die Authentifizierung auf dem TFTF-Server ist deaktiviert.

Das Nexus-Gerät muss mit der SNMPv2-Lese-Community oder dem V3-Benutzer konfiguriert werden.

Die AAA-Autorisierung muss deaktiviert werden.

Folgende Switch-Konfiguration

Die Switch-Konfiguration enthält eine angewendete ACL, die den Zugriff auf das Gerät verhindert.

```
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 address10.22.65.39/25
```

Schritt 1 - Erstellen Sie eine Konfigurationsdatei mit den Befehlen, die in der aktuellen Konfiguration des Nexus-Switches geändert oder zurückgesetzt werden sollen:

Das folgende Beispiel zeigt den Inhalt der Konfigurationsdatei zum Entfernen einer auf dem Mgmt 0-Port angewendeten ACL.

```
interface mgmt0
no ip access-group filter_internal_snmp_i in
```

Ein weiteres Beispiel für das Zurücksetzen der AAA-Einstellungen auf die lokale Authentifizierung auf dem Gerät

```
aaa authentication login local
```

Schritt 2: Speichern der Datei mit**.config**-Erweiterung und Platzierung im Boot- oder Home-Verzeichnis der TFTP-Anwendung

Schritt 3 - Führen Sie einen SNMP-Spaziergang zum Gerät durch, um die Erreichbarkeit und den Zugriff über SNMP zu bestätigen.

```
$ ./snmpwalk  -v2c -c 1.3.6.1.4.1.9.9.96.1.1.1.1.10.222
```

Schritt 4 - Führen Sie die folgenden Befehle ausvom snmp-server (die markierten müssen durch tatsächliche Werte ersetzt werden)

Verwenden von SNMP v2

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

Verwenden von SNMPv3

```
snmpset -v3 -l authNoPriv -u -a MD5 -A .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 -a MD5 -A .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 .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:
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-Schritte

```
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-Konfiguration nach der Problemumgehung

```
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
```

Sie können sich auch die Accounting-Protokolle ansehen, um festzustellen, ob der Befehl ausgeführt wurde. Konfigurationsänderung durch SNMP wird als Root-Benutzer angezeigt -

```
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=
```

Schritt 5 - Überprüfen Sie den Zugriff auf das Gerät mithilfe von SSH/Telnet.

Konfigurieren mithilfe von SNMP

Konfigurationsdatei wie unten

switch3.config:

```
vrf context management
ip route 0.0.0.0/0 10.128.164.1
end
```

SNMP-Befehlssatz

```
$ 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-Protokolle

```
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=

Referenz

Nexus-Sicherheitskonfigurationsleitfaden

NXOS-Kennwortwiederherstellung