Configurazione e risoluzione dei problemi di Nexus Switch con SNMP

Sommario

[Introduzione](#)
[Sfondo](#)
[Componenti usati](#)
[Ripristino degli accessi tramite SNMP](#)
[Configurazione tramite SNMP](#)
[Riferimento](#)

Introduzione

In questo documento viene descritto come risolvere i problemi e configurare uno switch Cisco Nexus con SNMP

Sfondo

La configurazione di uno switch Nexus può essere modificata se è disponibile l'accesso SNMP

È applicabile a tutte le piattaforme Nexus.

Componenti usati

Switch Nexus 5000 con versione 5.1(3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Ripristino degli accessi tramite SNMP

Il dispositivo dispone di un'interfaccia L3 (diversa da Mgmt 0) nel file vrf predefinito

Il server TFTP deve essere accessibile da questo switch tramite il file vrf predefinito e l'autenticazione deve essere disabilitata sul server TFTF

Il dispositivo Nexus deve essere configurato con la community di lettura/scrittura SNMPv2 o l'utente V3

L'autorizzazione AAA deve essere disabilitata

Configurazione switch seguente

La configurazione dello switch contiene un ACL applicato che impedisce l'accesso al dispositivo

```
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
```

Passaggio 1 - Creare un file di configurazione con i comandi per modificare o ripristinare la configurazione corrente dello switch Nexus:

L'esempio che segue mostra il contenuto del file di configurazione per la rimozione di un ACL applicato alla porta Mgmt 0

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

Un altro esempio per ripristinare l'autenticazione locale delle impostazioni AAA sul dispositivo

```
aaa authentication login local
```

2 - Salvare il file con**.config** e inserirla nella directory di avvio o nella directory home dell'applicazione TFTP

3. Eseguire una procedura SNMP per verificare la raggiungibilità e l'accessibilità del dispositivo tramite SNMP

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

Passaggio 4- Eseguire i comandi seguentidal server snmp (quelli evidenziati devono essere sostituiti dai valori effettivi)

Uso di 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
```

Uso di 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
```

Passi di SNMPv3

```
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
```

Cambia configurazione dopo la soluzione alternativa

```
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
```

Èinoltre possibile esaminare i registri di accounting per verificare se il comando è stato eseguito. La modifica della configurazione eseguita dal protocollo SNMP viene visualizzata come utente root -

```
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=
```

Passaggio 5 - Verificare l'accesso al dispositivo tramite ab SSH/Telnet

Configurazione tramite SNMP

File di configurazione come indicato di seguito

switch 3.config:

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

Set di comandi SNMP

```
$ 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
```

Registri di accounting

```
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=

Riferimento

Guida alla configurazione di Nexus Security

Recupero password NXOS