Configurez et dépannez le commutateur de Nexus utilisant le SNMP

Contenu

Introduction

Ce document décrit comment dépanner et configurer un commutateur de Cisco Nexus utilisant le SNMP

Fond

La configuration d'un commutateur de Nexus peut être modifiée si l'accès SNMP est disponible

Il s'applique pour toutes les Plateformes de Nexus.

Composants utilisés

Version 5.1(3) courante de commutateur de Nexus 5000

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Reprise d'Access utilisant le SNMP

Le périphérique a une interface L3 (autre que gestion 0) dans le vrf par défaut

Le serveur TFTP devrait être accessible de ce commutateur par l'intermédiaire du vrf par défaut et d'authentification désactivée sur le serveur TFTF

Le périphérique de Nexus devrait être configuré avec la communauté en lecture/écriture SNMPv2 ou l'utilisateur V3

L'authroization d'AAA doit être désactivé

Config suivant de commutateur

Onctains de config de commutateur qu'un ACL appliqué empêche accéder au périphérique

```
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
```

Étape 1 - Créez un fichier de config avec les commandes de changer ou rouler de retour en configuration en cours de commutateur de Nexus :

L'exemple suivant affiche le contenu du fichier de config pour retirer un ACL appliqué sur les gestion 0 ports

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

Un autre exemple pour remettre à l'état initial les configurations d'AAA à l'authentification locale sur le périphérique

```
aaa authentication login local
```

Étape 2 - Sauvegardez l'extension du fichier with.config et placez-la à l'intérieur du démarrage ou du répertoire home de l'application TFTP

Étape 3 - Exécutez une inspection SNMP au périphérique pour confirmer l'accessibilité et son accessibilité par l'intermédiaire du SNMP

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

Étape 4 - Exécutez le serveur SNMP suivant de commandsfrom (mis en valeur le besoin d'être remplacé par des valeurs réelles)

Utilisant 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
<tftfp_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
```

Utilisant 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
```

Étapes 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
```

Commutez le config après le contournement

```
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
```

Vous pouvez également regarder les journaux de traçabilité pour voir si la commande étaient exécutées. Le changement de configuration fait par SNMP apparaît comme utilisateur de base -

```
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=
```

Étape 5 - Vérifiez l'accès au périphérique en faisant ab SSH/Telnet

Configurez utilisant le SNMP

Fichier de config en tant que ci-dessous

switch3.config :

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

Positionnement de commande 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
```

Journaux de traçabilité

```
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=
```

Référence

Guide de configuration de sécurité de Nexus

Reprise de mot de passe NXOS