Surveiller l'état du commutateur IP MetroCluster

ONTAP MetroCluster

NetApp
February 13, 2026

Sommaire

Surveiller l’état du commutateur IP MetroCluster

En savoir plus sur la surveillance de l’état des commutateurs dans une configuration IP MetroCluster

Le moniteur d’état des commutateurs Ethernet (CSHM) est chargé de garantir l’intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage.

Remarques importantes pour la configuration de CSHM dans une configuration IP MetroCluster

Cette section présente les étapes générales de configuration de SNMPv3 et de collecte de journaux sur les commutateurs Cisco, Broadcom et NVIDIA SN2100. Vous devez suivre les étapes correspondant à la version du firmware du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le "Hardware Universe" pour vérifier les versions de firmware prises en charge.

Dans une configuration MetroCluster, vous configurez la surveillance de l’état sur les commutateurs de cluster locaux uniquement.

Pour la collecte des journaux avec les commutateurs Broadcom et Cisco, un nouvel utilisateur doit être créé sur le commutateur pour chaque cluster dont la collecte des journaux est activée. Dans une configuration MetroCluster, cela signifie que MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d’un utilisateur distinct sur les commutateurs. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l’utilisateur.

Avant de configurer le CSHM, vous devez désactiver les ISL inutilisés pour éviter toute alerte ISL inutile.

Configurer SNMPv3 pour surveiller la santé des commutateurs IP MetroCluster

Dans les configurations MetroCluster IP, vous pouvez configurer SNMPv3 pour surveiller l’état des commutateurs IP.

Cette procédure montre les étapes génériques de configuration de SNMPv3 sur un commutateur. Certaines versions du micrologiciel du commutateur répertoriées peuvent ne pas être prises en charge dans une configuration IP MetroCluster.

Vous devez suivre les étapes correspondant à la version du micrologiciel du commutateur prise en charge dans une configuration IP MetroCluster. Consultez le "Hardware Universe" pour vérifier les versions de firmware prises en charge.

- SNMPv3 n’est pris en charge que sur ONTAP 9.12.1 et versions ultérieures.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 et les versions ultérieures corrigent ces deux problèmes :
  - "Pour la surveillance de l’état ONTAP des commutateurs Cisco, le trafic SNMPv2 peut toujours être visible après le passage à SNMPv3 pour la surveillance"
  - "Alertes de ventilateur et d’alimentation de commutateur faussement positives en cas de pannes SNMP"

Description de la tâche

Les commandes suivantes sont utilisées pour configurer un nom d’utilisateur SNMPv3 sur les commutateurs **Broadcom**, **Cisco** et **NVIDIA** :

Commutateurs Broadcom

Configurez un nom d'utilisateur SNMPv3 OPÉRATEUR RÉSEAU sur les commutateurs Broadcom BES-53248.

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-
md5|auth-sha] [priv-aes128|priv-des]
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version
SNMPv3 -community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp status
```

```
(sw1)(Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1)(Config)# show snmp user snmp

     Name            Group Name      Auth Priv
                                     Meth Meth    Remote Engine ID
---------------- ------------------ ---- ------
-------------------------
<username>        network-admin      MD5  AES128
8000113d03d8c497710bee
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Après avoir attendu la période d'interrogation CSHM, vérifiez que le numéro de série est renseigné pour le commutateur Ethernet.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: <username>
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA
```

Commutateurs Cisco

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs Cisco 9336C-FX2 :

- Pour **pas d'authentification** :

```
snmp-server user SNMPv3_USER NoAuth
```

- Pour l'authentification **MD5/SHA** :

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
snmp-server user SNMPv3_USER AuthEncrypt  auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp user
```

```
(sw1)(Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1)(Config)# show snmp user

-----------------------------------------------------------------------
---------
                              SNMP USERS
-----------------------------------------------------------------------
---------

User              Auth            Priv(enforce)   Groups
acl_filter
----------------- --------------- --------------- ---------------
-----------
admin             md5             des(no)         network-admin
SNMPv3User        md5             aes-128(no)     network-operator

-----------------------------------------------------------------------
---------
     NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
-----------------------------------------------------------------------
---------

User              Auth                Priv
----------------- ------------------ ------------

(sw1)(Config)#
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: cshm1!
                                 Model Number: N9K-C9336C-FX2
                               Switch Network: cluster-network
                             Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                     Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: N9K-C9336C-FX2
                               Switch Network: cluster-network
                             Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                      Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                       Source Of Switch Version: CDP/ISDP
                                 Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                  RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
```

NVIDIA - CL 5.4.0

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.4.0 :

- Pour **pas d'authentification** :

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     4318
Version 1 and 2c Community String  Configured
Version 3 Usernames                Not Configured
---------------------------------  ----------------
cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf        2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf   2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
 # Auto-generated config file: do not edit. #
 agentaddress udp:@mgmt:161
 agentxperms 777 777 snmp snmp
 agentxsocket /var/agentx/master
 createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
 ifmib_max_num_ifaces 500
 iquerysecname _snmptrapusernameX
 master agentx
 monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```
 pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
 pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! default


net add/del commands since the last "net commit"

User        Timestamp                   Command
----------  --------------------------
------------------------------------------------------------------------
-----
SNMPv3User  2020-08-11 00:13:51.826987  net add snmp-server username
SNMPv3User auth-md5 <password> encrypt-aes <password>

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     24253
Version 1 and 2c Community String  Configured
Version 3 Usernames                Configured     <---- Configured
here
---------------------------------  ----------------
cumulus@sw1:~$
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv3
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
          Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

NVIDIA - CL 5.11.0

Configurez un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.11.0 :

- Pour **pas d'authentification** :

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Pour l'authentification **MD5/SHA** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Pour l'authentification **MD5/SHA avec cryptage AES/DES** :

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP :

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM :

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server
                     applied
-------------------  ----------------------------------------
[username]           SNMPv3_USER
[username]           limiteduser1
[username]           testuserauth
[username]           testuserauthaes
[username]           testusernoauth
trap-link-up
  check-frequency    60
trap-link-down
  check-frequency    60
[listening-address]  all
[readonly-community] $nvsec$94d69b56e921aec1790844eb53e772bf
state                enabled
cumulus@sw1:~$
```

2. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv3
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Configurer la collecte de journaux sur un commutateur IP MetroCluster

Dans une configuration IP MetroCluster, vous pouvez configurer la collecte de journaux pour collecter les journaux de commutation à des fins de débogage.

> Sur les commutateurs Broadcom et Cisco, un nouvel utilisateur est requis pour chaque cluster avec collecte de journaux. Par exemple, MetroCluster 1, MetroCluster 2, MetroCluster 3 et MetroCluster 4 nécessitent tous la configuration d'un utilisateur distinct sur les commutateurs. L'utilisation de plusieurs clés SSH pour un même utilisateur n'est pas prise en charge.

Description de la tâche

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage. Cette procédure vous guide tout au long du processus de configuration de la collecte, de demande de journaux **support** détaillés et d'activation d'une collecte horaire de données **périodiques** collectées par AutoSupport.

REMARQUE : si vous activez le mode FIPS, vous devez effectuer les opérations suivantes :

1. Régénérer les clés SSH sur le commutateur en suivant les instructions du fournisseur.
2. Régénérer les clés SSH dans ONTAP à l'aide de `debug system regenerate-systemshell-key-pair`
3. Réexécutez la routine de configuration de la collecte des journaux à l'aide de la `system switch ethernet log setup-password` commande

Avant de commencer

- L'utilisateur doit avoir accès aux commandes du commutateur `show` . S'ils ne sont pas disponibles, créez un nouvel utilisateur et accordez les autorisations nécessaires à l'utilisateur.
- La surveillance de l'état du commutateur doit être activée pour le commutateur. Vérifiez cela en vous assurant que `Is Monitored:` le champ est défini sur **true** dans la sortie du `system switch ethernet show` commande.
- Pour la collecte de journaux avec les commutateurs Broadcom et Cisco :
  - L'utilisateur local doit disposer de privilèges d'administrateur réseau.
  - Un nouvel utilisateur doit être créé sur le commutateur pour chaque configuration de cluster avec la collecte des journaux activée. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour le même utilisateur. Toute configuration de collecte de journaux supplémentaire effectuée remplace toute clé SSH préexistante pour l'utilisateur.
- Pour la prise en charge de la collecte de journaux avec les commutateurs NVIDIA, *user* pour la collecte de journaux doit être autorisé à exécuter la `cl-support` commande sans avoir à fournir de mot de passe. Pour autoriser cette utilisation, lancer la commande :

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus
```

Étapes

ONTAP 9.15.1 et versions ultérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

   REMARQUE : Si vous répondez **y** à l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessaires comme indiqué dans Avant de commencer .

   ```
   system switch ethernet log setup-password
   ```

   ```
   cluster1::*> system switch ethernet log setup-password
   Enter the switch name: <return>
   The switch name entered is not recognized.
   Choose from the following list:
   cs1
   cs2

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs1
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs2

   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>
   ```

   Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Activer la collecte périodique des journaux :

   ```
   system switch ethernet log modify -device <switch-name> -periodic
   -enabled true
   ```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs1: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs2: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       true        scheduled
never-run
cs2                                       true        scheduled
never-run
2 entries were displayed.
```

2. Demander la collecte du journal de support :

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1

cs1: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> system switch ethernet log collect-support-log -device
cs2

cs2: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> *system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       false       halted
initiated
cs2                                       true        scheduled
initiated
2 entries were displayed.
```

3. Pour afficher tous les détails de la collecte des journaux, y compris l'activation, le message d'état, l'horodatage précédent et le nom de fichier de la collecte périodique, l'état de la demande, le message d'état, ainsi que l'horodatage précédent et le nom de fichier de la collection de support, utilisez les éléments suivants :

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

                    Switch Name: cs1
           Periodic Log Enabled: true
            Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
    Last Periodic Log Timestamp: 3/11/2024 11:02:59
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:14:20
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

                    Switch Name: cs2
           Periodic Log Enabled: false
            Periodic Log Status: Periodic collection has been
halted.
    Last Periodic Log Timestamp: 3/11/2024 11:05:18
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:18:54
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

ONTAP 9.14.1 et versions antérieures

1. Pour configurer la collecte des journaux, exécutez la commande suivante pour chaque commutateur. Vous êtes invité à entrer le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

   REMARQUE : si vous répondez à `y` l'invite de spécification de l'utilisateur, assurez-vous que l'utilisateur dispose des autorisations nécessairesAvant de commencer, comme indiqué dans .

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Pour CL 5.11.1, créez l'utilisateur **cumulus** et répondez **y** à l'invite suivante : Souhaitez-vous spécifier un utilisateur autre qu'admin pour la collecte des journaux ? {y|n} : **y**

1. Pour demander la collecte des journaux d'assistance et activer la collecte périodique, exécutez la commande suivante. Ceci lance les deux types de collecte de journaux : les journaux détaillés `Support` et une collecte de données toutes les heures `Periodic` .

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Attendez 10 minutes, puis vérifiez que la collecte des journaux se termine :

```
system switch ethernet log show
```

Si des États d'erreur sont signalés par la fonction de collecte de journaux (visible dans la sortie de `system switch ethernet log show`), voir "Dépannage de la collecte des journaux" pour plus de détails.

Gérer la surveillance des commutateurs Ethernet dans une configuration IP MetroCluster

Dans la plupart des cas, les commutateurs Ethernet sont automatiquement détectés par ONTAP et surveillés par CSHM. Le fichier de configuration de référence (RCF) appliqué au commutateur, entre autres, active le protocole CDP (Cisco Discovery Protocol) et/ou le protocole LLDP (Link Layer Discovery Protocol). Cependant, vous devrez peut-être ajouter manuellement un commutateur qui n'est pas détecté ou supprimer un commutateur qui n'est plus utilisé. Vous pouvez également arrêter la surveillance active tout en maintenant le commutateur dans la configuration, par exemple pendant la maintenance.

Créez une entrée de commutateur afin que ONTAP puisse la surveiller

Description de la tâche

Utilisez `system switch ethernet create` la commande pour configurer et activer manuellement la surveillance d'un commutateur Ethernet spécifié. Ceci est utile si ONTAP n'ajoute pas automatiquement le commutateur, ou si vous avez précédemment supprimé le commutateur et souhaitez le rajouter.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type
cluster-network
```

Un exemple type est l'ajout d'un commutateur nommé [DeviceName], avec l'adresse IP 1.2.3.4, et les informations d'identification SNMPv2c définies sur **cshm1!**. Utilisez `-type storage-network` plutôt que `-type cluster-network` si vous configurez un commutateur de stockage.

Désactiver la surveillance sans supprimer le commutateur

Si vous souhaitez mettre en pause ou arrêter la surveillance d'un certain commutateur, mais le conserver pour une surveillance future, modifiez son `is-monitoring-enabled-admim` paramètre au lieu de le supprimer.

Par exemple :

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Cela vous permet de préserver les détails et la configuration du commutateur sans générer de nouvelles alertes ou de nouvelles découvertes.

Retirez un commutateur dont vous n'avez plus besoin

Utiliser `system switch ethernet delete` pour supprimer un commutateur qui a été déconnecté ou n'est plus nécessaire :

```
system switch ethernet delete -device DeviceName
```

Par défaut, cette commande réussit uniquement si ONTAP ne détecte pas actuellement le commutateur via CDP ou LLDP. Pour supprimer un commutateur découvert, utilisez le `-force` paramètre :

```
system switch ethernet delete -device DeviceName -force
```

Lorsque `-force` est utilisé, le commutateur peut être ajouté automatiquement si ONTAP le détecte à nouveau.

Vérifier la surveillance du commutateur Ethernet dans une configuration IP MetroCluster

Le moniteur d'état du commutateur Ethernet (CSHM) tente automatiquement de surveiller les commutateurs qu'il découvre ; cependant, la surveillance peut ne pas se produire automatiquement si les commutateurs ne sont pas configurés correctement. Vérifiez que le contrôle de l'état est correctement configuré pour surveiller les commutateurs.

Confirmez la surveillance des commutateurs Ethernet connectés

Description de la tâche

Pour vérifier que les commutateurs Ethernet connectés sont surveillés, exécutez :

```
system switch ethernet show
```

Si la colonne affiche **OTHER** ou si `Model` le `IS Monitored` champ affiche **FALSE**, ONTAP ne peut pas surveiller le commutateur. Une valeur de **AUTRE** indique généralement que ONTAP ne prend pas en charge ce commutateur pour la surveillance de l'intégrité.

Le `IS Monitored` champ est défini sur **FALSE** pour la raison spécifiée dans le `Reason` champ.

> Si un commutateur n'est pas répertorié dans la sortie de commande, ONTAP ne l'a probablement pas découvert. Vérifiez que le commutateur est correctement câblé. Si nécessaire, vous pouvez ajouter le commutateur manuellement. Voir "Gérer la surveillance des commutateurs Ethernet" pour plus de détails.

Vérifiez que les versions du firmware et des fichiers RCF sont à jour

Assurez-vous que le commutateur exécute le micrologiciel le plus récent pris en charge et qu'un fichier RCF compatible a été appliqué. Plus d'informations sont disponibles sur le "Page des téléchargements du support NetApp".

Par défaut, le moniteur d'intégrité utilise SNMPv2c avec la chaîne de communauté **cshm1!** pour la surveillance, mais SNMPv3 peut également être configuré.

Si vous devez modifier la chaîne de communauté SNMPv2c par défaut, assurez-vous que la chaîne de communauté SNMPv2c souhaitée a été configurée sur le commutateur.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c
-community-or-username newCommunity!
```

> Pour plus d'informations sur la configuration de SNMPv3 pour utilisation, reportez-vous à la section"Facultatif : configurer SNMPv3".

Confirmez la connexion au réseau de gestion

Vérifiez que le port de gestion du commutateur est connecté au réseau de gestion.

Une connexion de port de gestion correcte est requise pour que ONTAP puisse effectuer des requêtes SNMP et collecter des journaux.

Informations associées

- "Résolution des alertes"