Surveiller l'état des commutateurs

Cluster and storage switches

NetApp
August 09, 2024

Sommaire

Surveiller l’état des commutateurs

Présentation du contrôle de l’état des switchs

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.

Configurer la surveillance de l’état des commutateurs

Présentation de la configuration

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.

- "Configurer la collecte des journaux"
- "Facultatif : configurer SNMPv3"

Configurer la collecte des journaux

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, conformément aux instructions du fournisseur.
2. Régénérer les clés ssh côté ONTAP à l’aide de `debug system regenerate-systemshell-key-pair`
3. Exécutez à nouveau la routine de configuration de la collecte des journaux à l’aide de `system switch ethernet log setup-password`

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 ceci en vous assurant que le `Is Monitored:` le champ est défini sur **true** dans la sortie du `system switch ethernet show` commande.
- Pour les switchs NVIDIA, l’utilisateur de la collecte de journaux doit être autorisé à exécuter les commandes de collecte de journaux sans afficher d’invite de mot de passe. Pour autoriser cette utilisation, lancer la commande : `echo '<username> ALL = NOPASSWD: /usr/cumulus/bin/cl-support,`

```
/usr/sbin/csmgrctl' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus
```

Étapes

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.

```
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>
```

2. Pour demander la collecte de journaux de support 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
```

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.

```
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>
```

2. 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.
```

3. 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.
```

4. 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.
```

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.

Et la suite ?

"Configurer SNMPv3 (facultatif)".

Facultatif : configurez SNMPv3 pour votre commutateur

SNMP est utilisé pour surveiller les commutateurs. Le contrôleur d'état du commutateur Ethernet (CSHM) utilise le protocole SNMP pour surveiller l'état et les performances des commutateurs de cluster et de stockage. Par défaut, SNMPv2c est configuré automatiquement via le fichier de configuration de référence (RCF).

SNMPv3 est plus sécurisé que SNMPv2 car il introduit des fonctionnalités de sécurité robustes telles que l'authentification, le cryptage et l'intégrité des messages, qui protègent contre les accès non autorisés et assurent la confidentialité et l'intégrité des données pendant la transmission.

SNMPv3 n'est pris en charge que sur ONTAP 9.12.1 et versions ultérieures.

Suivez cette procédure pour configurer SNMPv3 pour votre commutateur spécifique, qui prend en charge CSHM.

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. 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: 10.228.136.24
                                 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 : CLI 5.4

Configurer un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant CLI 5.4 :

- Pour **pas d'authentification** :

```
net add snmp-server username SNMPv3_USER auth-none
```

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

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-
PASSWORD
```

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

```
net add 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 4.4.3 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 4.4.3 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
```

Vérifier l’état du commutateur

Présentation du bilan de santé

Cette fonction surveille de manière proactive certaines conditions critiques du cluster et déclenche des alertes en cas de défaillance ou de risque.

Pour afficher les alertes de contrôle de l’état du commutateur Ethernet en cours, lancer la commande : `system health alert show -monitor ethernet-switch`

Pour afficher les alertes de contrôle de l’état des commutateurs Ethernet disponibles, lancer la commande : `system health alert definition show -monitor ethernet-switch`

Résolution des alertes

Les alertes sont générées si une panne, un risque ou une condition critique est détecté pour un commutateur Ethernet de votre cluster.

Si des alertes sont générées, l’état de santé du système indique une dégradation du cluster. Les alertes émises incluent les informations dont vous avez besoin pour remédier à la dégradation de l’état du système.

Pour afficher les alertes de contrôle de l'état des commutateurs Ethernet disponibles, lancer la commande : `system health alert definition show -monitor ethernet-switch`

Pour plus d'informations sur la résolution avancée des alertes, reportez-vous à l'article de la base de connaissances "Guide de résolution des alertes du moniteur d'intégrité des commutateurs" .

Collecte de journaux

Présentation de la collecte des journaux

Une fois la collecte des journaux configurée, vous pouvez activer une collecte horaire des données périodiques collectées par AutoSupport et demander des journaux de support détaillés.

Voir "Configurer la collecte des journaux" pour plus de détails.

Dépannage de la collecte des journaux

Si vous rencontrez l'un des États d'erreur suivants signalés par la fonction de collecte de journaux (visible dans la sortie de la `system switch ethernet log show` commande), essayez les étapes de débogage correspondantes :

Etat d'erreur de collecte de journaux	Résolution
Clés RSA non présentes	Régénérer les clés SSH ONTAP.
Erreur de mot de passe de commutateur	Vérifiez les identifiants, testez la connectivité SSH et régénérez les clés SSH ONTAP. Consultez la documentation du commutateur ou contactez le support NetApp pour obtenir des instructions.
Clés ECDSA non présentes pour FIPS	Si le mode FIPS est activé, les clés ECDSA doivent être générées sur le commutateur avant de réessayer.
Journal préexistant trouvé	Supprimez le fichier de collecte de journaux précédent sur le commutateur.
Erreur du journal de vidage de commutateur	Assurez-vous que l'utilisateur du commutateur dispose des autorisations de collecte de journaux. Reportez-vous aux conditions préalables ci-dessus.

Si les détails de la résolution ne fonctionnent pas, contactez le support NetApp.

Informations sur le copyright

Informations sur les marques commerciales