



Surveiller l'état du commutateur

Install and maintain

NetApp

February 13, 2026

Sommaire

- Surveiller l'état du commutateur 1
 - Aperçu du moniteur d'état des commutateurs 1
 - Configurer la surveillance de l'état du commutateur 1
 - Présentation de la configuration 1
 - Configurer la collecte des journaux 1
 - Configurez SNMPv3 pour votre commutateur (facultatif) 8
- Vérifier l'état du commutateur 26
 - Aperçu du bilan de santé 26
 - Gérer la surveillance des commutateurs Ethernet 26
 - Vérifier la surveillance des commutateurs Ethernet 28
 - Dépannage des alertes 29
- Collecte des journaux 29
 - Aperçu de la collecte des journaux 29
 - Résolution des problèmes liés à la collecte des journaux 29

Surveiller l'état du commutateur

Aperçu du moniteur d'état des commutateurs

Le moniteur d'intégrité des commutateurs Ethernet (CSHM) est responsable de garantir l'intégrité opérationnelle des commutateurs réseau de cluster et de stockage et de collecter les journaux de commutation à des fins de débogage.

Configurer la surveillance de l'état du commutateur

Présentation de la configuration

Le moniteur d'intégrité des commutateurs Ethernet (CSHM) est responsable de garantir l'intégrité opérationnelle des commutateurs réseau de cluster et de stockage et de collecter les journaux de commutation à des fins de débogage.

- ["Configurer la collecte des journaux"](#)
- ["Configurer SNMPv3 \(facultatif\)"](#)

Configurer la collecte des journaux

Le moniteur d'intégrité des commutateurs Ethernet (CSHM) est responsable de garantir l'intégrité opérationnelle des commutateurs réseau de cluster et de stockage et de collecter les journaux de commutation à des fins de débogage. Cette procédure vous guide tout au long du processus de configuration de la collecte, de la demande de journaux **Support** détaillés et de l'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. Régénérez 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 en utilisant `system switch ethernet log setup-password` commande

Avant de commencer

- L'utilisateur doit avoir accès à l'interrupteur `show` commandes. Si ces éléments ne sont pas disponibles, créez un nouvel utilisateur et accordez-lui les autorisations nécessaires.
- La surveillance de l'état du commutateur doit être activée pour celui-ci. Vérifiez cela en vous assurant que `Is Monitored:` Le champ est défini sur **vrai** dans la sortie de `system switch ethernet show` commande.
- Pour la collecte des 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 collecte de journaux activée. Ces commutateurs ne prennent pas en charge plusieurs clés SSH pour un même utilisateur. Toute configuration supplémentaire de collecte de journaux effectuée écrase toutes les clés SSH préexistantes de l'utilisateur.
- Pour la collecte des journaux de support avec les commutateurs NVIDIA , l'utilisateur chargé de la collecte des journaux doit être autorisé à exécuter le programme. `cl-support` commander sans avoir à fournir de mot de passe. Pour autoriser cette utilisation, exécutez 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 saisir le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

REMARQUE : Si vous répondez « oui » à l'invite de spécification de l'utilisateur, assurez-vous que celui-ci 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 que admin pour la collecte des journaux ? {o|n}: **o**

1. [[étape 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.

2. Collecte des journaux de support demandée :

```
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 consulter tous les détails de la collecte des journaux, y compris l'activation, le message d'état, l'horodatage et le nom de fichier de la collecte périodique précédente, l'état de la requête, le message d'état, ainsi que l'horodatage et le nom de fichier de la collecte de support précédente, 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 saisir le nom du commutateur, le nom d'utilisateur et le mot de passe pour la collecte des journaux.

REMARQUE : Si vous répondez y Lors de l'invite de spécification de l'utilisateur, assurez-vous que celui-ci 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 que admin pour la collecte des journaux ? {o|n}: **o**

1. [[étape 2]] Pour demander la collecte des journaux de support et activer la collecte périodique, exécutez la commande suivante. Cela lance les deux types de collecte de journaux : la collecte détaillée Support journaux et une collecte horaire de Periodic données.

```
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 est terminée :

```
system switch ethernet log show
```



Si des erreurs sont signalées par la fonction de collecte des journaux (visibles dans la sortie de `system switch ethernet log show`), voir ["Résolution des problèmes liés à la collecte des journaux"](#) pour plus de détails.

Quelle est la prochaine étape ?

["Configurer SNMPv3 \(facultatif\)".](#)

Configurez SNMPv3 pour votre commutateur (facultatif)

Le protocole SNMP est utilisé pour surveiller les commutateurs. La surveillance par SNMPv3 est configurée en suivant cette procédure.

Le moniteur d'état des commutateurs Ethernet (CSHM) utilise 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 sûr que SNMPv2 car il introduit des fonctionnalités de sécurité robustes telles que l'authentification, le chiffrement et l'intégrité des messages, qui protègent contre les accès non autorisés et garantissent la confidentialité et l'intégrité des données lors de la transmission.



- SNMPv3 n'est pris en charge que sur ONTAP 9.12.1 et versions ultérieures.
- Les versions ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 et ultérieures corrigent ces deux problèmes :
 - "Pour la surveillance de l'état des commutateurs Cisco ONTAP , le trafic SNMPv2 peut encore être observé après le passage à SNMPv3."
 - "Alertes erronées concernant le ventilateur et l'alimentation en cas de défaillance SNMP."

À propos de cette tâche

Les commandes suivantes permettent de configurer un nom d'utilisateur SNMPv3 sur les commutateurs **Broadcom**, * Cisco* et * NVIDIA* :

Commutateurs Broadcom

Configurez un nom d'utilisateur SNMPv3 NETWORK-OPERATOR sur les commutateurs Broadcom BES-53248.

- Pour les **sans 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 chiffrement 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 chiffrement :

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

2. Configurez l'utilisateur SNMPv3 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 effectuer la surveillance 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: cshml!
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

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

- Pour les **sans 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 chiffrement 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 chiffrement :

```
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 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 effectuer la surveillance 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: cshml!
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 détaillé à l'étape précédente une fois la période d'interrogation CSHM terminée.

```
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

Configurez un nom d'utilisateur SNMPv3 SNMPv3_USER sur les commutateurs NVIDIA SN2100 exécutant l'interface de ligne de commande 5.4.0 :

- Pour les **sans authentication** :

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

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

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

- Pour l'**authentication MD5/SHA avec chiffrement 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 chiffrement :

```
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 laErrorMessage "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 cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syservices 72
-rocommunity cshml! 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 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 effectuer la surveillance 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: cshml!
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 détaillé à l'étape précédente une fois la période d'interrogation CSHM terminée.

```
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 l'interface de ligne de commande 5.11.0 :

- Pour les **sans authentication** :

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

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

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

- Pour l'**authentication MD5/SHA avec chiffrement 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 chiffrement :

```
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 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 effectuer la surveillance 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: cshml!
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 détaillé à l'étape précédente une fois la période d'interrogation CSHM terminée.

```
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

```

Vérifier l'état du commutateur

Aperçu du bilan de santé

Les systèmes de surveillance de l'état de santé contrôlent de manière proactive certaines conditions critiques au sein de votre cluster et émettent des alertes en cas de détection d'une panne ou d'un risque.

Pour consulter les alertes de surveillance de l'état du commutateur Ethernet actuellement activées, exécutez la commande : `system health alert show -monitor ethernet-switch`

Pour consulter les alertes de surveillance de l'état du commutateur Ethernet disponibles, exécutez la commande : `system health alert definition show -monitor ethernet-switch`

Gérer la surveillance des commutateurs Ethernet

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 active, entre autres, le protocole de découverte Cisco (CDP) et/ou le protocole de découverte de couche de liaison (LLDP). Toutefois, vous pourriez avoir

besoin d'ajouter manuellement un commutateur non détecté ou de supprimer un commutateur qui n'est plus utilisé. Vous pouvez également interrompre la surveillance active tout en conservant le commutateur dans la configuration, par exemple lors d'une opération de maintenance.

Créez une entrée de commutation pour ONTAP puisse la surveiller.

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

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

Un exemple typique consiste à ajouter un commutateur nommé [DeviceName], avec l'adresse IP 1.2.3.4 et les informations d'identification SNMPv2c définies sur **cshml!**. Utiliser `-type storage-network` au lieu de `-type cluster-network` si vous configurez un commutateur de stockage.

Désactiver la surveillance sans supprimer le commutateur

Si vous souhaitez suspendre ou arrêter la surveillance d'un commutateur spécifique, tout en le conservant pour une surveillance ultérieure, modifiez ses paramètres. `is-monitoring-enabled-admin` 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 des commutateurs sans générer de nouvelles alertes ni de nouvelles redécouvertes.

Retirez un interrupteur dont vous n'avez plus besoin.

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

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

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

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

Quand `-force` Si le commutateur est utilisé, il pourra être rajouté automatiquement si ONTAP le détecte à

nouveau.

Vérifier la surveillance des commutateurs Ethernet

Le moniteur d'intégrité des commutateurs Ethernet (CSHM) tente automatiquement de surveiller les commutateurs qu'il découvre ; cependant, la surveillance peut ne pas se faire automatiquement si les commutateurs ne sont pas correctement configurés. Vous devez vérifier que le système de surveillance de l'état de vos commutateurs est correctement configuré.

Vérifier la surveillance des commutateurs Ethernet connectés

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

```
system switch ethernet show
```

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

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



Si un commutateur n'est pas répertorié dans le résultat de la commande, il est probable que ONTAP ne l'ait pas détecté. Vérifiez que le commutateur est correctement câblé. Si nécessaire, vous pouvez ajouter l'interrupteur manuellement. Voir "[Gérer la surveillance des commutateurs Ethernet](#)" pour plus de détails.

Vérifiez que les versions du firmware et du RCF sont à jour.

Assurez-vous que le commutateur exécute le dernier firmware pris en charge et qu'un fichier de configuration de référence (RCF) compatible a été appliqué. Plus d'informations sont disponibles sur [lehttps://mysupport.netapp.com/site/downloads\[\"Page de téléchargement du support NetApp\"\]](https://mysupport.netapp.com/site/downloads[\) .

Par défaut, le moniteur d'intégrité utilise SNMPv2c avec la chaîne de communauté **csbm1!** 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!
```



Voir "[Facultatif : Configurer SNMPv3](#)" pour plus de détails sur la configuration de SNMPv3 pour son utilisation.

Confirmer la connexion au réseau de gestion

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

Une connexion correcte au port de gestion est nécessaire pour ONTAP puisse effectuer des requêtes SNMP et collecter les journaux.

Dépannage des alertes

Des alertes sont émises en cas de défaut, de risque ou de condition critique détectée pour un commutateur Ethernet de votre cluster.

En cas d'alertes, l'état de santé du système signale un état dégradé pour le cluster. Les alertes émises contiennent les informations nécessaires pour réagir à une dégradation de l'état du système.

Pour consulter les alertes de surveillance de l'état du commutateur Ethernet disponibles, exécutez la commande : `system health alert definition show -monitor ethernet-switch`

Consultez l'article de la base de connaissances ["Guide de résolution des alertes du moniteur d'état du commutateur"](#) pour des détails de résolution avancée sur les alertes.

Collecte des journaux

Aperçu de la collecte des journaux

Une fois la collecte des journaux configurée, vous pouvez activer la collecte horaire des données périodiques collectées par AutoSupport et demander des journaux d'assistance détaillés.

Voir ["Configurer la collecte des journaux"](#) pour plus de détails.

Résolution des problèmes liés à la collecte des journaux

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

État d'erreur de collecte des journaux	Résolution
Clés RSA absentes	Régénérer les clés SSH ONTAP .
Erreur de mot de passe Switch	Vérifiez les informations d'identification, 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 absentes pour FIPS	Si le mode FIPS est activé, des clés ECDSA doivent être générées sur le commutateur avant de réessayer.
Journal préexistant trouvé	Supprimez le fichier de journalisation précédent sur le commutateur.

Erreur lors de la génération du journal de vidage du commutateur

Vérifiez que l'utilisateur du commutateur dispose des autorisations de collecte des journaux. Veuillez vous référer aux prérequis ci-dessus.



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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.