監控交換器運作狀況
Install and maintain

NetApp
February 13, 2026

目錄

監控交換器運作狀況

交換器健康監控器概述

乙太網路交換器健康監視器 (CSHM) 負責確保叢集和儲存網路交換器的運作健康，並收集交換器日誌以進行偵錯。

配置交換器健康監控

配置概述

乙太網路交換器健康監視器 (CSHM) 負責確保叢集和儲存網路交換器的運作健康，並收集交換器日誌以進行偵錯。

- "配置日誌收集"
- "配置 SNMPv3（可選）"

配置日誌收集

乙太網路交換器健康監視器 (CSHM) 負責確保叢集和儲存網路交換器的運作健康，並收集交換器日誌以進行偵錯。此流程引導您完成設定收集、請求詳細的*支援*日誌以及啟用由AutoSupport收集的*定期*資料的每小時收集流程。

注意： 如果啟用 FIPS 模式，則必須完成以下步驟：

1. 依照廠商提供的說明，在交換器上重新產生 SSH 金鑰。
2. 使用ONTAP重新產生 SSH 金鑰 `debug system regenerate-systemshell-key-pair`
3. 使用以下方式重新執行日誌收集設定例程： `system switch ethernet log setup-password`命令

開始之前

- 使用者必須有權存取該開關。 `show`命令。如果這些使用者不可用，請建立一個新使用者並授予該使用者必要的權限。
- 必須為交換器啟用交換器健康監控功能。透過確保以下方式驗證這一點： `Is Monitored:`輸出中該欄位設定為*true* `system switch ethernet show`命令。
- 用於收集博通和Cisco交換器的日誌：
  - 本機使用者必須具有網路管理員權限。
  - 對於每個啟用了日誌收集的叢集設置，都應該在交換器上建立一個新使用者。這些交換器不支援同一用戶使用多個 SSH 金鑰。任何額外的日誌收集設定都會覆蓋使用者的任何現有 SSH 金鑰。
- 為了支援使用NVIDIA交換器收集日誌，必須允許用於日誌收集的_user_ 執行此交換器。 `cl-support`無需提供密碼即可執行命令。若要啟用此用法，請執行下列命令：

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

步驟

ONTAP 9.15.1 及更高版本

1. 若要設定日誌收集，請對每個交換器執行以下命令。系統會提示您輸入用於日誌收集的交換器名稱、使用者名稱和密碼。

   注意： 如果對使用者規範提示回答 **y**，請確保使用者擁有必要的權限，如下所述：[開始之前] 。

```
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>
```

對於 CL 5.11.1，建立使用者 **cumulus** 並對以下提示回答 **y**：您是否要指定 admin 以外的使用者進行日誌收集？ {y|n}: **y**

1. 步驟2：啟用定期日誌收集。

```
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. 請求支援日誌收集：

```
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. 要查看日誌收集的所有詳細信息，包括定期收集的啟用情況、狀態訊息、上一個時間戳和文件名，以及支援收集的請求狀態、狀態訊息、上一個時間戳和文件名，請使用以下命令：

```
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 及更早版本

1. 若要設定日誌收集，請對每個交換器執行以下命令。系統會提示您輸入用於日誌收集的交換器名稱、使用者名稱和密碼。

   注意： 如果回答 `y`根據使用者規格提示，確保使用者擁有必要的權限，具體權限要求請參閱相關文件。[開始之前] 。

```
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>
```

對於 CL 5.11.1，建立使用者 **cumulus** 並對以下提示回答 **y**：您是否要指定 admin 以外的使用者進行日誌收集？ {y|n}: **y**

1. 若要要求支援日誌收集並啟用定期收集，請執行下列命令。這將啟動兩種類型的日誌收集：詳細日誌收集和詳細日誌收集。 `Support`日誌和每小時收集的數據 `Periodic`數據。

```
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.
```

等待 10 分鐘，然後檢查日誌收集是否完成：

```
system switch ethernet log show
```

如果日誌收集功能報告了任何錯誤狀態（在輸出中可見），`system switch ethernet log show`），看"排查日誌收集問題"更多詳情請見下文。

下一步是什麼？

"配置 SNMPv3（可選）"。

為交換器配置 **SNMPv3**（可選）

SNMP 用於監控交換器。請依照以下步驟設定 SNMPv3 監控。

乙太網路交換器健康監視器 (CSHM) 利用 SNMP 來監視叢集交換器和儲存交換器的運作狀況和效能。預設情況下，SNMPv2c 透過參考設定檔 (RCF) 自動設定。 SNMPv3 比 SNMPv2 更安全，因為它引入了強大的安全功能，例如身份驗證、加密和訊息完整性，這些功能可以防止未經授權的訪問，並確保傳輸過程中資料的機密性和完整性。

- ONTAP 9.12.1 及更高版本僅支援 SNMPv3。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 及更高版本修復了這兩個問題：
  - "對於使用ONTAP對Cisco交換器進行健康監控的情況，即使切換到 SNMPv3 進行監控，可能仍會看到 SNMPv2 流量。"
  - "當 SNMP 故障發生時，交換器風扇和電源警報可能會出現誤報。"

關於此任務

以下命令用於在 Broadcom、 Cisco和NVIDIA交換器上設定 SNMPv3 使用者名稱：

博通交換機

在 Broadcom BES-53248 交換器上設定 SNMPv3 使用者名稱 NETWORK-OPERATOR。

- 對於*無需身份驗證*的情況：

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

- 用於 **MD5/SHA** 認證：

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

- 用於*MD5/SHA認證與AES/DES加密*：

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

以下指令在ONTAP端設定 SNMPv3 使用者名稱：

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

以下命令用於在 CSHM 中建立 SNMPv3 使用者名稱：

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

步驟

1. 在交換器上設定 SNMPv3 使用者以使用身份驗證和加密：

```
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. 在ONTAP端設定 SNMPv3 用戶：

```
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. 設定 CSHM 以使用新的 SNMPv3 使用者進行監控：

```
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. 等待 CSHM 輪詢週期結束後，確認乙太網路交換器的序號已填入。

```
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
```

Cisco交換機

在Cisco 9336C-FX2 交換器上設定 SNMPv3 使用者名稱 SNMPv3_USER：

- 對於*無需身份驗證*的情況：

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

- 用於 **MD5/SHA** 認證：

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

- 用於*MD5/SHA認證與AES/DES加密*：

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

以下指令在ONTAP端設定 SNMPv3 使用者名稱：

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

以下命令用於在 CSHM 中建立 SNMPv3 使用者名稱：

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

步驟

1. 在交換器上設定 SNMPv3 使用者以使用身份驗證和加密：

```
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. 在ONTAP端設定 SNMPv3 用戶：

```
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. 設定 CSHM 以使用新的 SNMPv3 使用者進行監控：

```
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. 在 CSHM 輪詢週期結束後，驗證使用新建立的 SNMPv3 使用者查詢的序號是否與上一個步驟中詳細說明的序號相同。

```
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

在執行 CLI 5.4.0 的NVIDIA SN2100 交換器上設定 SNMPv3 使用者名稱 SNMPv3_USER：

- 對於*無需身份驗證*的情況：

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

- 用於 **MD5/SHA** 認證：

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

- 用於*MD5/SHA認證與AES/DES加密*：

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

以下指令在ONTAP端設定 SNMPv3 使用者名稱：

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

以下命令用於在 CSHM 中建立 SNMPv3 使用者名稱：

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

步驟

1. 在交換器上設定 SNMPv3 使用者以使用身份驗證和加密：

```
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. 在ONTAP端設定 SNMPv3 用戶：

```
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. 設定 CSHM 以使用新的 SNMPv3 使用者進行監控：

```
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. 在 CSHM 輪詢週期結束後，驗證使用新建立的 SNMPv3 使用者查詢的序號是否與上一個步驟中詳細說明的序號相同。

```
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

在執行 CLI 5.11.0 的NVIDIA SN2100 交換器上設定 SNMPv3 使用者名稱 SNMPv3_USER：

- 對於*無需身份驗證*的情況：

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

- 用於 **MD5/SHA** 認證：

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

- 用於*MD5/SHA認證與AES/DES加密*：

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

以下指令在ONTAP端設定 SNMPv3 使用者名稱：

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

以下命令用於在 CSHM 中建立 SNMPv3 使用者名稱：

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

步驟

1. 在交換器上設定 SNMPv3 使用者以使用身份驗證和加密：

```
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. 在ONTAP端設定 SNMPv3 用戶：

```
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. 設定 CSHM 以使用新的 SNMPv3 使用者進行監控：

```
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. 在 CSHM 輪詢週期結束後，驗證使用新建立的 SNMPv3 使用者查詢的序號是否與上一個步驟中詳細說明的序號相同。

```
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
```

檢查交換機健康狀況

健康檢查概述

健康監控器會主動監控叢集中的某些關鍵狀況，並在偵測到故障或風險時發出警報。

若要查看目前已觸發的乙太網路交換器健康監控警報，請執行以下命令： `system health alert show -monitor ethernet-switch`

若要查看可用的乙太網路交換器健康監控警報，請執行以下命令： `system health alert definition show -monitor ethernet-switch`

管理乙太網路交換器的監控

大多數情況下，乙太網路交換器由ONTAP自動發現，並由 CSHM 監控。應用於交換器的參考設定檔 (RCF) 除其他功能外，還啟用Cisco發現協定 (CDP) 和/或連結層發現協定 (LLDP)。但是，您可能需要手動新增未被發現的交換機，或刪除不再使用的交換器。您也可以在保留交換器設定的情況下停止主動監控，例如在維護期間。

建立交換器條目，以便**ONTAP**可以對其進行監控。

使用 `system switch ethernet create`手動設定並啟用指定乙太網路交換器的監控命令。如果ONTAP沒有自動添加交換機，或者您之前刪除了交換器並想重新添加它，這將很有幫助。

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

一個典型的例子是新增一個名為 [DeviceName] 的交換機，其 IP 位址為 1.2.3.4，SNMPv2c 憑證設定為 **cshm1!**。使用 `-type storage-network`而不是 `-type cluster-network`如果您正在設定儲存交換器。

停用監控而不刪除開關

如果您想暫停或停止對某個交換器的監控，但仍希望保留該交換器以供日後監控，請修改其設定。 `is-monitoring-enabled-admim`保留參數而不是刪除它。

例如：

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

這樣可以保留交換器的詳細資訊和配置，而不會產生新的警報或重新發現。

移除不再需要的開關

使用 `system switch ethernet delete`刪除已斷開連接或不再需要的開關：

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

預設情況下，只有當ONTAP目前未透過 CDP 或 LLDP 偵測到交換器時，此指令才會成功。若要移除已發現的交換機，請使用 `-force`範圍：

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

什麼時候 `-force`如果使用此開關，當ONTAP再次偵測到該開關時，可能會自動重新新增該開關。

驗證乙太網路交換器的監控情況

乙太網路交換器健康監視器 (CSHM) 會自動嘗試監視它發現的交換器；但是，如果交換器設定不正確，則監視可能不會自動進行。您應該確認運作狀況監控器已正確配置，可以監控您的交換器。

確認對已連接的乙太網路交換器進行監控

若要確認已連接的乙太網路交換器正在被監控，請運作：

```
system switch ethernet show
```

如果 `Model`列顯示“其他”或 `IS Monitored`如果欄位顯示*false*，則ONTAP無法監控交換器。 **OTHER** 值通常表示ONTAP不支援此開關進行健康監測。

這 `IS Monitored`該欄位的值設定為*false*，原因已在文中說明。 `Reason`場地。

如果命令輸出中未列出交換機，則ONTAP可能尚未發現該交換器。確認交換器接線正確。如有必要，您可以手動新增開關。看"管理乙太網路交換器的監控"更多詳情請見下文。

請確認韌體和 **RCF** 版本均為最新版本。

確保交換器運作的是最新支援的韌體，並且已套用相容的參考設定檔（RCF）。更多資訊請造訪[此處]。https://mysupport.netapp.com/site/downloads["NetApp支援下載頁面"^]。

預設情況下，健康監視器使用 SNMPv2c 和群組字串 **cshm1!** 進行監視，但也可以設定 SNMPv3。

如果需要變更預設的 SNMPv2c 團體字串，請確保已在交換器上設定所需的 SNMPv2c 團體字串。

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

看"可選：配置 SNMPv3"有關配置 SNMPv3 的詳細資訊。

確認管理網路連接

確認交換器的管理連接埠已連接至管理網路。

ONTAP需要正確的管理連接埠連線才能執行 SNMP 查詢和日誌收集。

故障排除警報

如果叢集中的乙太網路交換器偵測到故障、風險或嚴重情況，則會發出警報。

如果發出警報，系統健康狀況報告群集狀態下降。發出的警報包含您需要應對系統健康狀況下降的資訊。

若要查看可用的乙太網路交換器健康監控警報，請執行以下命令： `system health alert definition show -monitor ethernet-switch`

請參閱知識庫文章 "Switch 健康監控器警報解決指南"有關警報的高級解析詳情。

日誌收集

日誌收集概覽

設定日誌收集後，您可以啟用AutoSupport每小時收集的定期數據，並要求詳細的支援日誌。

看"配置日誌收集"更多詳情請見下文。

排查日誌收集問題

如果您遇到日誌收集功能報告的以下任何錯誤狀態（可在輸出中查看），`system switch ethernet log show`命令），嘗試對應的調試步驟：

日誌收集錯誤狀態	解決
RSA金鑰不存在	重新產生ONTAP SSH 金鑰。
切換密碼錯誤	驗證憑證，測試 SSH 連接，並重新產生ONTAP SSH 金鑰。請查閱交換器文件或聯絡NetApp支援以取得說明。
FIPS 系統中不存在 **ECDSA** 金鑰	如果啟用了 FIPS 模式，則需要在交換器上產生 ECDSA 金鑰，然後再重試。
發現已存在的日誌	刪除交換器上之前的日誌收集檔案。
交換器轉儲日誌錯誤	請確保切換使用者擁有日誌收集權限。請參考以上先決條件。

如果上述解決方案無效，請聯絡NetApp支援。