监控交换机运行状况

Install and maintain

NetApp
February 13, 2026

目录

监控交换机运行状况

交换机健康监控器概述

以太网交换机健康监视器 (CSHM) 负责确保集群和存储网络交换机的运行健康，并收集交换机日志以进行调试。

配置交换机健康监控

配置概述

以太网交换机健康监视器 (CSHM) 负责确保集群和存储网络交换机的运行健康，并收集交换机日志以进行调试。

- "配置日志收集"
- "配置 SNMPv3（可选）"

配置日志收集

以太网交换机健康监视器 (CSHM) 负责确保集群和存储网络交换机的运行健康，并收集交换机日志以进行调试。此流程指导您完成设置收集、请求详细的*支持*日志以及启用由AutoSupport收集的*定期*数据的每小时收集过程。

注意： 如果启用 FIPS 模式，则必须完成以下步骤：

1. 按照厂商提供的说明，在交换机上重新生成 SSH 密钥。
2. 使用ONTAP重新生成 SSH 密钥 `debug system regenerate-systemshell-key-pair`
3. 使用以下方式重新运行日志收集设置例程： `system switch ethernet log setup-password`命令

开始之前

- 用户必须有权访问该开关。 `show`命令。如果这些用户不可用，请创建一个新用户并授予该用户必要的权限。
- 必须为交换机启用交换机健康监控功能。通过确保以下方式验证这一点： `Is Monitored:`输出中该字段设置为*true* `system switch ethernet show`命令。
- 用于收集博通和Cisco交换机的日志：
  - 本地用户必须具有网络管理员权限。
  - 对于每个启用了日志收集的集群设置，都应该在交换机上创建一个新用户。这些交换机不支持同一用户使用多个 SSH 密钥。任何额外的日志收集设置都会覆盖用户的任何现有 SSH 密钥。
- 为了支持使用NVIDIA交换机收集日志，必须允许用于日志收集的_user_ 运行该交换机。 `cl-support`无需提供密码即可执行命令。要启用此用法，请运行以下命令：

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

步骤

ONTAP 9.15.1 及更高版本

1. 要设置日志收集，请对每个交换机运行以下命令。系统会提示您输入用于日志收集的交换机名称、用户名和密码。

   注意： 如果对用户规范提示回答 **y**，请确保用户拥有必要的权限，如以下所述：[开始之前] 。

```
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>
```

对于 CL 5.11.1，创建用户 **cumulus** 并对以下提示回答 **y**：您是否要指定除 admin 之外的用户进行日志收集？ {y|n}: **y**

1. 步骤2：启用定期日志收集。

```
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. 请求支持日志收集：

```
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. 要查看日志收集的所有详细信息，包括定期收集的启用状态、状态消息、上一个时间戳和文件名，以及支持收集的请求状态、状态消息、上一个时间戳和文件名，请使用以下命令：

```
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. 要设置日志收集，请对每个交换机运行以下命令。系统会提示您输入用于日志收集的交换机名称、用户名和密码。

   注意： 如果回答 `y`根据用户规范提示，确保用户拥有必要的权限，具体权限要求请参见相关文档。[开始之前] 。

```
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>
```

对于 CL 5.11.1，创建用户 **cumulus** 并对以下提示回答 **y**：您是否要指定除 admin 之外的用户进行日志收集？ {y|n}: **y**

1. 要请求支持日志收集并启用定期收集，请运行以下命令。这将启动两种类型的日志收集：详细日志收集和详细日志收集。 `Support`日志和每小时收集的数据 `Periodic`数据。

```
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 分钟，然后检查日志收集是否完成：

```
system switch ethernet log show
```

如果日志收集功能报告了任何错误状态（在输出中可见），`system switch ethernet log show`），看"排查日志收集问题"更多详情请见下文。

下一步是什么?

"配置 SNMPv3（可选）"。

为交换机配置 SNMPv3（可选）

SNMP 用于监控交换机。按照以下步骤配置 SNMPv3 监控。

以太网交换机健康监视器 (CSHM) 利用 SNMP 来监视集群交换机和存储交换机的运行状况和性能。默认情况下，SNMPv2c 通过参考配置文件 (RCF) 自动配置。 SNMPv3 比 SNMPv2 更安全，因为它引入了强大的安全功能，例如身份验证、加密和消息完整性，这些功能可以防止未经授权的访问，并确保传输过程中数据的机密性和完整性。

- ONTAP 9.12.1 及更高版本仅支持 SNMPv3。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 及更高版本修复了这两个问题：
  - "对于使用ONTAP对Cisco交换机进行健康监控的情况，即使切换到 SNMPv3 进行监控，可能仍然会看到 SNMPv2 流量。"
  - "当 SNMP 故障发生时，交换机风扇和电源警报可能出现误报。"

关于此任务

以下命令用于在 Broadcom、 Cisco和NVIDIA交换机上配置 SNMPv3 用户名：

博通交换机

在 Broadcom BES-53248 交换机上配置 SNMPv3 用户名 NETWORK-OPERATOR。

- 对于*无需身份验证*的情况：

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

- 用于 **MD5/SHA** 认证：

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

- 用于*MD5/SHA认证与AES/DES加密*：

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

以下命令在ONTAP端配置 SNMPv3 用户名：

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

以下命令用于在 CSHM 中建立 SNMPv3 用户名：

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

步骤

1. 在交换机上配置 SNMPv3 用户以使用身份验证和加密：

```
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端设置 SNMPv3 用户：

```
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. 配置 CSHM 以使用新的 SNMPv3 用户进行监控：

```
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 轮询周期结束后，确认以太网交换机的序列号已填充。

```
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 交换机

在Cisco 9336C-FX2 交换机上配置 SNMPv3 用户名 SNMPv3_USER：

- 对于*无需身份验证*的情况：

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

- 用于 **MD5/SHA** 认证：

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

- 用于*MD5/SHA认证与AES/DES加密*：

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

以下命令在ONTAP端配置 SNMPv3 用户名：

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

以下命令用于在 CSHM 中建立 SNMPv3 用户名：

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

步骤

1. 在交换机上配置 SNMPv3 用户以使用身份验证和加密：

```
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端设置 SNMPv3 用户：

```
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. 配置 CSHM 以使用新的 SNMPv3 用户进行监控：

```
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 轮询周期结束后，验证使用新创建的 SNMPv3 用户查询的序列号是否与上一步中详细说明的序列号相同。

```
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

在运行 CLI 5.4.0 的NVIDIA SN2100 交换机上配置 SNMPv3 用户名 SNMPv3_USER：

- 对于*无需身份验证*的情况：

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

- 用于 **MD5/SHA** 认证：

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

- 用于*MD5/SHA认证与AES/DES加密*：

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

以下命令在ONTAP端配置 SNMPv3 用户名：

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

以下命令用于在 CSHM 中建立 SNMPv3 用户名：

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

步骤

1. 在交换机上配置 SNMPv3 用户以使用身份验证和加密：

```
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端设置 SNMPv3 用户：

```
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. 配置 CSHM 以使用新的 SNMPv3 用户进行监控：

```
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 轮询周期结束后，验证使用新创建的 SNMPv3 用户查询的序列号是否与上一步中详细说明的序列号相同。

```
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

在运行 CLI 5.11.0 的NVIDIA SN2100 交换机上配置 SNMPv3 用户名 SNMPv3_USER：

- 对于*无需身份验证*的情况：

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

- 用于 **MD5/SHA** 认证：

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

- 用于*MD5/SHA认证与AES/DES加密*：

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

以下命令在ONTAP端配置 SNMPv3 用户名：

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

以下命令用于在 CSHM 中建立 SNMPv3 用户名：

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

步骤

1. 在交换机上配置 SNMPv3 用户以使用身份验证和加密：

```
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端设置 SNMPv3 用户：

```
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. 配置 CSHM 以使用新的 SNMPv3 用户进行监控：

```
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 轮询周期结束后，验证使用新创建的 SNMPv3 用户查询的序列号是否与上一步中详细说明的序列号相同。

```
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
```

检查交换机健康状况

健康检查概述

健康监控器会主动监控集群中的某些关键状况，并在检测到故障或风险时发出警报。

要查看当前已触发的以太网交换机健康监控警报，请运行以下命令： `system health alert show -monitor ethernet-switch`

要查看可用的以太网交换机健康监控警报，请运行以下命令： `system health alert definition show -monitor ethernet-switch`

管理以太网交换机的监控

大多数情况下，以太网交换机由ONTAP自动发现，并由 CSHM 监控。应用于交换机的参考配置文件 (RCF) 除其他功能外，还启用Cisco发现协议 (CDP) 和/或链路层发现协议 (LLDP)。但是，您可能需要手动添加未被发现的交换机，或者删除不再使用的交换机。您也可以在保留交换机配置的情况下停止主动监控，例如在维护期间。

创建交换机条目，以便**ONTAP**可以对其进行监控。

使用 `system switch ethernet create`手动配置并启用指定以太网交换机的监控命令。如果ONTAP没有自动添加交换机，或者您之前删除了交换机并想重新添加它，这将很有帮助。

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

一个典型的例子是添加一个名为 [DeviceName] 的交换机，其 IP 地址为 1.2.3.4，SNMPv2c 凭据设置为 **cshm1!**。使用 `-type storage-network`而不是 `-type cluster-network`如果您正在配置存储交换机。

禁用监控而不删除开关

如果您想暂停或停止对某个交换机的监控，但仍希望保留该交换机以供将来监控，请修改其设置。 `is-monitoring-enabled-admim`保留参数而不是删除它。

例如：

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

这样可以保留交换机的详细信息和配置，而不会生成新的警报或重新发现。

移除不再需要的开关

使用 `system switch ethernet delete`删除已断开连接或不再需要的开关：

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

默认情况下，只有当ONTAP当前未通过 CDP 或 LLDP 检测到交换机时，此命令才会成功。要移除已发现的交换机，请使用 `-force`范围：

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

什么时候 `-force`如果使用该开关， ONTAP再次检测到该开关时，可能会自动重新添加该开关。

验证以太网交换机的监控情况

以太网交换机健康监视器 (CSHM) 会自动尝试监视它发现的交换机；但是，如果交换机配置不正确，则监视可能不会自动进行。您应该确认运行状况监控器已正确配置，可以监控您的交换机。

确认对已连接的以太网交换机进行监控

要确认已连接的以太网交换机正在被监控，请运行：

```
system switch ethernet show
```

如果 `Model`列显示“其他”或 `IS Monitored`如果字段显示*false*，则ONTAP无法监控交换机。 **OTHER** 值通常表示ONTAP不支持该开关进行健康监测。

这 `IS Monitored`该字段的值设置为*false*，原因已在文中说明。 `Reason`场地。

如果命令输出中未列出交换机，则ONTAP可能尚未发现该交换机。请确认交换机接线正确。如有必要，您可以手动添加开关。看"管理以太网交换机的监控"更多详情请见下文。

请确认固件和 **RCF** 版本均为最新版本。

确保交换机运行的是最新支持的固件，并且已应用兼容的参考配置文件（RCF）。更多信息请访问[此处]。https://mysupport.netapp.com/site/downloads["NetApp支持下载页面"^] 。

默认情况下，健康监视器使用 SNMPv2c 和团体字符串 **cshm1!** 进行监视，但也可以配置 SNMPv3。

如果需要更改默认的 SNMPv2c 团体字符串，请确保已在交换机上配置所需的 SNMPv2c 团体字符串。

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

看"可选：配置 SNMPv3"有关配置 SNMPv3 的详细信息。

确认管理网络连接

确认交换机的管理端口已连接到管理网络。

ONTAP需要正确的管理端口连接才能执行 SNMP 查询和日志收集。

故障排除警报

如果集群中的以太网交换机检测到故障、风险或严重情况，则会发出警报。

如果发出警报，系统健康状况报告集群状态下降。发出的警报包含您需要应对系统健康状况下降的信息。

要查看可用的以太网交换机健康监控警报，请运行以下命令： `system health alert definition show -monitor ethernet-switch`

请参阅知识库文章 "Switch 健康监控器警报解决指南"有关警报的高级解析详情。

收集日志

日志收集概览

设置日志收集后，您可以启用AutoSupport每小时收集的定期数据，并请求详细的支持日志。

看"配置日志收集"更多详情请见下文。

排查日志收集问题

如果您遇到日志收集功能报告的以下任何错误状态（可在输出中查看），`system switch ethernet log show`命令），尝试相应的调试步骤：

日志收集错误状态	解决
RSA密钥不存在	重新生成ONTAP SSH 密钥。
切换密码错误	验证凭据，测试 SSH 连接，并重新生成ONTAP SSH 密钥。请查阅交换机文档或联系NetApp支持以获取说明。
FIPS 系统中不存在 **ECDSA** 密钥	如果启用了 FIPS 模式，则需要在交换机上生成 ECDSA 密钥，然后再重试。
发现已存在的日志	删除交换机上之前的日志收集文件。
交换机转储日志错误	请确保切换用户拥有日志收集权限。请参考以上先决条件。

如果上述解决方案无效，请联系NetApp支持。