Switch-Zustandsüberwachung konfigurieren

Install and maintain

NetApp
February 13, 2026

Inhalt

Switch-Zustandsüberwachung konfigurieren

Konfigurationsübersicht

Der Ethernet Switch Health Monitor (CSHM) ist dafür zuständig, den Betriebszustand der Cluster- und Speichernetzwerk-Switches sicherzustellen und Switch-Protokolle zu Debugging-Zwecken zu sammeln.

- "Protokollerfassung konfigurieren"
- "SNMPv3 konfigurieren (optional)"

Protokollerfassung konfigurieren

Der Ethernet Switch Health Monitor (CSHM) ist dafür zuständig, den Betriebszustand der Cluster- und Speichernetzwerk-Switches sicherzustellen und Switch-Protokolle zu Debugging-Zwecken zu sammeln. Dieses Verfahren führt Sie durch den Prozess der Einrichtung der Datenerfassung, der Anforderung detaillierter **Support**-Protokolle und der Aktivierung einer stündlichen Erfassung von **periodischen** Daten, die von AutoSupport erfasst werden.

HINWEIS: Wenn Sie den FIPS-Modus aktivieren, müssen Sie Folgendes durchführen:

1. Generieren Sie die SSH-Schlüssel auf dem Switch gemäß den Anweisungen des Herstellers neu.
2. SSH-Schlüssel in ONTAP neu generieren mit `debug system regenerate-systemshell-key-pair`
3. Führen Sie die Routine zur Einrichtung der Protokollsammlung erneut aus. `system switch ethernet log setup-password` Befehl

Bevor Sie beginnen

- Der Benutzer muss Zugriff auf den Schalter haben. `show` Befehle. Falls diese nicht verfügbar sind, erstellen Sie einen neuen Benutzer und erteilen Sie diesem die erforderlichen Berechtigungen.
- Die Zustandsüberwachung des Switches muss aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass `Is Monitored:` Das Feld wird in der Ausgabe auf **true** gesetzt. `system switch ethernet show` Befehl.
- Für die Protokollerfassung mit Broadcom- und Cisco -Switches:
  - Der lokale Benutzer muss über Netzwerkadministratorrechte verfügen.
  - Für jede Clusterkonfiguration, bei der die Protokollerfassung aktiviert ist, sollte ein neuer Benutzer auf dem Switch angelegt werden. Diese Switches unterstützen keine mehreren SSH-Schlüssel für denselben Benutzer. Jede zusätzliche Konfiguration der Protokollerfassung überschreibt alle bereits vorhandenen SSH-Schlüssel des Benutzers.
- Für die Protokollerfassung mit NVIDIA -Switches muss dem Benutzer, der für die Protokollerfassung zuständig ist, die Berechtigung zum Ausführen des Programms erteilt werden. `cl-support` Befehle ausführen, ohne ein Passwort angeben zu müssen. Um diese Verwendung zu ermöglichen, führen Sie

folgenden Befehl aus:

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

Schritte

ONTAP 9.15.1 und höher

1. Um die Protokollerfassung einzurichten, führen Sie für jeden Switch den folgenden Befehl aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Passwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie die Benutzerspezifikationsabfrage mit **j** beantworten, stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, wie in der Dokumentation beschrieben.Bevor Sie beginnen Die

   ```
   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>
   ```

   Für CL 5.11.1 erstellen Sie den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie einen anderen Benutzer als admin für die Protokollerfassung angeben? {y|n}: **y**

1. Aktivieren Sie die regelmäßige Protokollerfassung:

```
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. Anforderung von Support-Protokollsammlung:

```
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. Um alle Details der Protokollerfassung anzuzeigen, einschließlich Aktivierung, Statusmeldung, vorherigem Zeitstempel und Dateinamen der periodischen Erfassung, Anforderungsstatus, Statusmeldung, vorherigem Zeitstempel und Dateinamen der Support-Erfassung, verwenden Sie Folgendes:

```
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 und früher

1. Um die Protokollerfassung einzurichten, führen Sie für jeden Switch den folgenden Befehl aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Passwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie antworten `y` Stellen Sie bei der Eingabeaufforderung für die Benutzerspezifikation sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, wie in der folgenden Beschreibung aufgeführt:Bevor Sie beginnen Die

   ```
   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>
```

Für CL 5.11.1 erstellen Sie den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie einen anderen Benutzer als admin für die Protokollerfassung angeben? {y|n}: **y**

1. Um die Erfassung von Support-Protokollen anzufordern und die regelmäßige Erfassung zu aktivieren, führen Sie den folgenden Befehl aus. Damit werden beide Arten der Protokollerfassung gestartet: die detaillierte `Support` Protokolle und eine stündliche Erfassung von `Periodic` Daten.

```
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.
```

Warten Sie 10 Minuten und überprüfen Sie dann, ob die Protokollerfassung abgeschlossen ist:

```
system switch ethernet log show
```

Wenn von der Protokollerfassungsfunktion Fehlerstatus gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), sehen"Fehlerbehebung bei der Protokollerfassung" für weitere Einzelheiten.

Wie geht es weiter?

"SNMPv3 konfigurieren (optional)".

Konfigurieren Sie SNMPv3 für Ihren Switch (optional).

SNMP wird zur Überwachung der Switches verwendet. Die Überwachung mittels SNMPv3 wird durch Befolgen der folgenden Vorgehensweise konfiguriert.

Der Ethernet Switch Health Monitor (CSHM) nutzt SNMP, um den Zustand und die Leistung von Cluster- und Speicherswitches zu überwachen. Standardmäßig wird SNMPv2c automatisch über die Referenzkonfigurationsdatei (RCF) konfiguriert. SNMPv3 ist sicherer als SNMPv2, da es robuste Sicherheitsfunktionen wie Authentifizierung, Verschlüsselung und Nachrichtenintegrität einführt, die vor unberechtigtem Zugriff schützen und die Vertraulichkeit und Integrität der Daten während der Übertragung gewährleisten.

- SNMPv3 wird nur auf ONTAP 9.12.1 und höher unterstützt.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 und spätere Versionen beheben diese beiden Probleme:
  - "Bei der ONTAP Zustandsüberwachung von Cisco -Switches kann es vorkommen, dass SNMPv2-Datenverkehr auch nach der Umstellung auf SNMPv3 für die Überwachung noch sichtbar ist."
  - "Fehlalarme bezüglich Lüfter und Stromversorgung bei SNMP-Fehlern"

Informationen zu diesem Vorgang

Die folgenden Befehle werden verwendet, um einen SNMPv3-Benutzernamen auf **Broadcom**-, * Cisco*- und * NVIDIA*-Switches zu konfigurieren:

Broadcom-Schalter

Konfigurieren Sie einen SNMPv3-Benutzernamen NETWORK-OPERATOR auf Broadcom BES-53248 Switches.

- Für **keine Authentifizierung**:

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

- Für die **MD5/SHA-Authentifizierung**:

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

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

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

Der folgende Befehl konfiguriert einen SNMPv3-Benutzernamen auf der ONTAP Seite:

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

Der folgende Befehl richtet den SNMPv3-Benutzernamen bei CSHM ein:

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

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass er Authentifizierung und Verschlüsselung verwendet:

```
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. Richten Sie den SNMPv3-Benutzer auf der ONTAP Seite ein:

```
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. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
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. Nach Ablauf der CSHM-Abfrageperiode überprüfen Sie, ob die Seriennummer für den Ethernet-Switch eingetragen ist.

```
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 Switches

Konfigurieren eines SNMPv3-Benutzernamens SNMPv3_USER auf Cisco 9336C-FX2-Switches:

- Für **keine Authentifizierung**:

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

- Für die **MD5/SHA-Authentifizierung**:

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

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

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

Der folgende Befehl konfiguriert einen SNMPv3-Benutzernamen auf der ONTAP Seite:

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

Der folgende Befehl richtet den SNMPv3-Benutzernamen bei CSHM ein:

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

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass er Authentifizierung und Verschlüsselung verwendet:

   ```
   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. Richten Sie den SNMPv3-Benutzer auf der ONTAP Seite ein:

```
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. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
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. Überprüfen Sie nach Abschluss des CSHM-Abfragezeitraums, ob die abzufragende Seriennummer des neu erstellten SNMPv3-Benutzers mit der im vorherigen Schritt angegebenen übereinstimmt.

```
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

Konfigurieren eines SNMPv3-Benutzernamens SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.4.0:

- Für **keine Authentifizierung**:

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

- Für die **MD5/SHA-Authentifizierung**:

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

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

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

Der folgende Befehl konfiguriert einen SNMPv3-Benutzernamen auf der ONTAP Seite:

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

Der folgende Befehl richtet den SNMPv3-Benutzernamen bei CSHM ein:

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

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass er Authentifizierung und Verschlüsselung verwendet:

```
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. Richten Sie den SNMPv3-Benutzer auf der ONTAP Seite ein:

```
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. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
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. Überprüfen Sie nach Abschluss des CSHM-Abfragezeitraums, ob die abzufragende Seriennummer des neu erstellten SNMPv3-Benutzers mit der im vorherigen Schritt angegebenen übereinstimmt.

```
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

Konfigurieren eines SNMPv3-Benutzernamens SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.11.0:

- Für **keine Authentifizierung**:

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

- Für die **MD5/SHA-Authentifizierung**:

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

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

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

Der folgende Befehl konfiguriert einen SNMPv3-Benutzernamen auf der ONTAP Seite:

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

Der folgende Befehl richtet den SNMPv3-Benutzernamen bei CSHM ein:

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

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass er Authentifizierung und Verschlüsselung verwendet:

   ```
   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. Richten Sie den SNMPv3-Benutzer auf der ONTAP Seite ein:

   ```
   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. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
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. Überprüfen Sie nach Abschluss des CSHM-Abfragezeitraums, ob die abzufragende Seriennummer des neu erstellten SNMPv3-Benutzers mit der im vorherigen Schritt angegebenen übereinstimmt.

```
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
```