



Konfigurieren Sie die Überwachung des Switch-Systemzustands

Install and maintain

NetApp
October 31, 2025

Inhalt

Konfigurieren Sie die Überwachung des Switch-Systemzustands	1
Konfigurationsübersicht	1
Konfigurieren der Protokollerfassung	1
Bevor Sie beginnen	1
Schritte	2
Konfigurieren Sie SNMPv3 für Ihren Switch (optional)	8

Konfigurieren Sie die Überwachung des Switch-Systemzustands

Konfigurationsübersicht

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich.

- "[Konfigurieren der Protokollerfassung](#)"
- "[SNMPv3 konfigurieren \(optional\)](#)"

Konfigurieren der Protokollerfassung

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung der Erfassung, der Anforderung detaillierter **Support** Protokolle und der Aktivierung einer stündlichen Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

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

1. Generieren Sie SSH-Schlüssel auf dem Switch mithilfe der Herstelleranweisungen neu.
2. Regenerieren Sie SSH-Schlüssel in ONTAP mit `debug system regenerate-systemshell-key-pair`
3. Führen Sie die Setup-Routine für die Protokollsammlung mit dem `system switch ethernet log setup-password` Befehl erneut aus



Bevor Sie beginnen

- Der Benutzer muss Zugriff auf die Switch-Befehle haben `show`. Wenn diese nicht verfügbar sind, erstellen Sie einen neuen Benutzer und erteilen Sie dem Benutzer die erforderlichen Berechtigungen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf `true` gesetzten `system switch ethernet show` Befehl.
- Für die Protokollerfassung mit Broadcom- und Cisco-Switches:
 - Der lokale Benutzer muss über Netzwerkadministratorrechte verfügen.
 - Für jedes Cluster-Setup sollte auf dem Switch ein neuer Benutzer erstellt werden, bei dem die Protokollerfassung aktiviert ist. Diese Switches unterstützen nicht mehrere SSH-Schlüssel für denselben Benutzer. Bei jeder weiteren Einrichtung der Protokollerfassung werden alle bereits vorhandenen SSH-Schlüssel für den Benutzer überschrieben.
- Für die Unterstützung der Log-Erfassung mit NVIDIA-Switches muss der `user` für die Log-Sammlung berechtigt sein `cl-support`, den Befehl auszuführen, ohne ein Passwort angeben zu müssen. Führen

Sie den folgenden Befehl aus, um diese Verwendung zuzulassen:

```
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. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

HINWEIS: Wenn Sie bei der Benutzerspezifikationsabfrage mit **y** antworten, stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, wie in [Bevor Sie beginnen](#).

```
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>
```



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

1. [[Schritt 2]]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. Support-Protokoll anfordern:

```
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  
Support Periodic Periodic  
Switch Log Enabled Log State  
Log State  
  
cs1 false halted  
initiated  
cs2 true scheduled  
initiated  
2 entries were displayed.
```

3. Um alle Details der Protokollsammlung anzuzeigen, einschließlich der Aktivierung, Statusmeldung, des vorherigen Zeitstempels und des Dateinamens der periodischen Erfassung, des Anforderungsstatus, der Statusmeldung und des vorherigen Zeitstempels und des Dateinamens der Support-Sammlung, 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 frühere Versionen

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

HINWEIS: Wenn Sie auf die Eingabeaufforderung der Benutzerspezifikation antworten **y**, stellen Sie sicher, dass der Benutzer die erforderlichen Berechtigungen hat [Bevor Sie beginnen](#), wie in beschrieben.

```
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>

```



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

1. [[Schritt 2]] Um die Erfassung des Support-Protokolls anzufordern und die regelmäßige Erfassung zu aktivieren, führen Sie den folgenden Befehl aus. Damit werden beide Arten der Protokollerfassung gestartet: Die detaillierten Support Protokolle und eine stündliche Datenerfassung Periodic .

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

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

```
system switch ethernet log show
```

 Wenn Fehlerzustände durch die Log-Collection-Funktion (sichtbar in der Ausgabe von `system switch ethernet log show`) gemeldet werden, siehe "[Fehlerbehebung bei der Protokollerfassung](#)" für weitere Details.

Was kommt als Nächstes?

["SNMPv3 konfigurieren \(optional\)"](#).

Konfigurieren Sie SNMPv3 für Ihren Switch (optional).

SNMP wird verwendet, um die Switches zu überwachen. Die Überwachung durch SNMPv3 wird durch Befolgen dieses Verfahrens konfiguriert.

Der Ethernet Switch Health Monitor (CSHM) verwendet SNMP zur Überwachung von Zustand und Performance von Cluster- und Speicher-Switches. SNMPv2c wird standardmäßig automatisch über die Referenzkonfigurationsdatei (RCF) konfiguriert. SNMPv3 ist sicherer als SNMPv2, da es robuste Sicherheitsfunktionen wie Authentifizierung, Verschlüsselung und Nachrichtenintegrität bietet, die vor unbefugtem 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-Integritätsüberwachung von Cisco-Switches kann der SNMPv2-Verkehr nach der Umstellung auf SNMPv3 zur Überwachung weiterhin sichtbar sein."
 - "Falsch-positive Switch-Lüfter- und Stromwarnungen bei SNMP-Fehlern"

Über diese Aufgabe

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

Broadcom-Switches

Konfigurieren Sie einen NETZWERKBETREIBER für SNMPv3-Benutzernamen auf Broadcom BES-53248-Switches.

- Für **keine Authentifizierung**:

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

- Für * 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]
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

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

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
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 Authentifizierung und Verschlüsselung verwendet werden:

```
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. Überprüfen Sie nach dem Abwarten der CSHM-Abfrageperiode, 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 Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf Cisco 9336C-FX2-Switches:

- Für **keine Authentifizierung**:

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

- Für * 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
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

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

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
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 Authentifizierung und Verschlüsselung verwendet werden:

```
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. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch 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: 10.231.80.212
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 Sie einen SNMPv3-Benutzernamen 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 * 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
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

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

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
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 Authentifizierung und Verschlüsselung verwendet werden:

```
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 cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
sysservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

User	Timestamp	Command
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username SNMPv3User auth-md5 <password> encrypt-aes <password>
cumulus@sw1:~\$		
cumulus@sw1:~\$ net show snmp status		
Simple Network Management Protocol (SNMP) Daemon.		
Current Status		active (running)
Reload Status		enabled
Listening IP Addresses		all vrf mgmt
Main snmpd PID		24253
Version 1 and 2c Community String		Configured
Version 3 Usernames		Configured <---- Configured
here		
cumulus@sw1:~\$		

2. 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-LDP 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. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch 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
(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-LDP Aug-18-2022

```

NVIDIA – CL 5.11.0

Konfigurieren Sie einen SNMPv3-Benutzernamen 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 * 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
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

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

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
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 Authentifizierung und Verschlüsselung verwendet werden:

```
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-LDP 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. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch 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
(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-LDP Aug-18-2022
```

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERWEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.