



# **Monitorare lo stato degli switch**

Install and maintain

NetApp  
October 31, 2025

# Sommario

Monitorare lo stato degli switch . . . . .	1
Panoramica del monitor dello stato dello switch . . . . .	1
Configurare il monitoraggio dello stato dello switch . . . . .	1
Panoramica della configurazione . . . . .	1
Configurare la raccolta di log . . . . .	1
Configurare SNMPv3 per lo switch (facoltativo) . . . . .	8
Controllare lo stato dello switch . . . . .	26
Panoramica del controllo di stato . . . . .	26
Gestire il monitoraggio degli switch Ethernet . . . . .	26
Verificare il monitoraggio degli switch Ethernet . . . . .	28
Risolvere i problemi relativi agli avvisi . . . . .	29
Raccolta di log . . . . .	29
Panoramica della raccolta di log . . . . .	29
Risolvere i problemi relativi alla raccolta dei log . . . . .	29

# Monitorare lo stato degli switch

## Panoramica del monitor dello stato dello switch

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug.

## Configurare il monitoraggio dello stato dello switch

### Panoramica della configurazione

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug.

- "["Configurare la raccolta di log"](#)
- "["Configure SNMPv3 \(opzionale\)"](#)"

### Configurare la raccolta di log

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug. Questa procedura guida l'utente attraverso il processo di impostazione della raccolta, la richiesta di registri **supporto** dettagliati e l'abilitazione di una raccolta oraria di dati **periodici** raccolti da AutoSupport.

**NOTA:** se si attiva la modalità FIPS, è necessario completare quanto segue:

1. Rigenerare le chiavi SSH sullo switch utilizzando le istruzioni del fornitore.
2. Rigenerare le chiavi SSH in ONTAP utilizzando `debug system regenerate-systemshell-key-pair`
3. Eseguire nuovamente la routine di impostazione della raccolta di registri utilizzando il `system switch ethernet log setup-password` comando

### Prima di iniziare

- L'utente deve avere accesso ai comandi di commutazione `show`. Se non sono disponibili, creare un nuovo utente e concedere le autorizzazioni necessarie all'utente.
- Il monitoraggio dello stato dello switch deve essere abilitato per lo switch. Verificare questo assicurandosi che `Is Monitored`: il campo è impostato su **true** nell'output di `system switch ethernet show` comando.
- Per la raccolta dei registri con gli switch Broadcom e Cisco:
  - L'utente locale deve disporre dei privilegi di amministratore di rete.
  - È necessario creare un nuovo utente sullo switch per ogni configurazione del cluster con la raccolta di

log attivata. Questi switch non supportano più chiavi SSH per lo stesso utente. Qualsiasi impostazione di raccolta di log aggiuntiva eseguita sovrascrive qualsiasi chiave SSH preesistente per l'utente.

- Per la raccolta dei log di supporto con gli switch NVIDIA, la raccolta log *user* deve essere autorizzata ad eseguire il *cl-support* comando senza dover fornire una password. Per consentire questo utilizzo, eseguire il comando:

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

## Fasi

## ONTAP 9.15.1 e versioni successive

1. Per impostare la raccolta di log, eseguire il comando seguente per ogni switch. Viene richiesto di immettere il nome dello switch, il nome utente e la password per la raccolta del registro.

**NOTA:** Se si risponde **y** alla richiesta di specificazione dell'utente, assicurarsi che l'utente disponga delle autorizzazioni necessarie come descritto in [Prima di iniziare](#).

```
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>



Per CL 5.11.1, creare l'utente **cumulus** e rispondere **y** al seguente prompt: Si desidera specificare un utente diverso da admin per la raccolta dei log? {y|n}: **y**

1. Abilita la raccolta periodica dei registri:

```
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 State		
cs1	true	scheduled
never-run		
cs2	true	scheduled
never-run		

2 entries were displayed.

## 2. Richiedi raccolta registro assistenza:

```
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. Per visualizzare tutti i dettagli della raccolta di log, inclusi abilitazione, messaggio di stato, data e ora precedenti e nome del file della raccolta periodica, lo stato della richiesta, il messaggio di stato, l'indicatore data e ora precedenti e il nome del file della raccolta di supporto, utilizzare quanto segue:

```
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 e versioni precedenti

1. Per impostare la raccolta di log, eseguire il comando seguente per ogni switch. Viene richiesto di immettere il nome dello switch, il nome utente e la password per la raccolta del registro.

**NOTA:** se si risponde **y** al prompt delle specifiche dell'utente, assicurarsi che l'utente disponga delle autorizzazioni necessarie, come descritto in [Prima di iniziare](#).

```
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>

```



Per CL 5.11.1, creare l'utente **cumulus** e rispondere **y** al seguente prompt: Si desidera specificare un utente diverso da admin per la raccolta dei log? {y|n}: **y**

1. Per richiedere la raccolta del registro di supporto e abilitare la raccolta periodica, eseguire il seguente comando. Questo avvia entrambi i tipi di raccolta di log: I log dettagliati Support e una raccolta oraria di Periodic dati.

```
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.

Attendere 10 minuti, quindi verificare che la raccolta dei log sia completa:

```
system switch ethernet log show
```

 Se uno stato di errore viene segnalato dalla funzione di raccolta registri (visibile nell'output di system switch ethernet log show), vedere "[Risolvere i problemi relativi alla raccolta dei log](#)" per ulteriori dettagli.

**Quali sono le prossime novità?**

["Configure SNMPv3 \(opzionale\)"](#).

## Configurare SNMPv3 per lo switch (facoltativo)

SNMP viene utilizzato per monitorare gli switch. Il monitoraggio tramite SNMPv3 si configura seguendo questa procedura.

Il monitor stato switch Ethernet (CSHM) utilizza SNMP per monitorare lo stato e le prestazioni degli switch cluster e di storage. Per impostazione predefinita, SNMPv2c viene configurato automaticamente tramite il file di configurazione di riferimento (RCF). SNMPv3 è più sicuro di SNMPv2 perché introduce robuste funzionalità di sicurezza come autenticazione, crittografia e integrità dei messaggi, che proteggono da accessi non autorizzati e garantiscono la riservatezza e l'integrità dei dati durante la trasmissione.

- SNMPv3 è supportato solo su ONTAP 9.12.1 e versioni successive.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 e versioni successive risolvono questi due problemi:
  - "Per il monitoraggio dello stato ONTAP degli switch Cisco, il traffico SNMPv2 potrebbe essere ancora visualizzato dopo il passaggio a SNMPv3 per il monitoraggio"
  - "Avvisi falsi positivi di ventola e alimentazione dell'interruttore quando si verificano errori SNMP"

#### A proposito di questa attività

I seguenti comandi vengono utilizzati per configurare un nome utente SNMPv3 sugli switch **Broadcom**, **Cisco** e **NVIDIA**:

## Switch Broadcom

Configurare un OPERATORE DI RETE con nome utente SNMPv3 sugli switch Broadcom BES-53248.

- Per **nessuna autenticazione**:

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

- Per l'autenticazione **MD5/SHA**:

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

- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

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

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

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

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

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

## Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
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. Impostare l'utente SNMPv3 sul lato ONTAP:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: 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. Dopo aver atteso il periodo di polling CSHM, verificare che il numero di serie sia compilato per lo switch Ethernet.

```
system switch ethernet polling-interval show
```

```

cluster1::*> system switch ethernet polling-interval show
    Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
    Device Name: sw1
        IP Address: 10.228.136.24
        SNMP Version: SNMPv3
        Is Discovered: true
    DEPRECATED-Community String or SNMPv3 Username: -
        Community String or SNMPv3 Username: <username>
        Model Number: BES-53248
        Switch Network: cluster-network
        Software Version: 3.9.0.2
    Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
    Source Of Switch Version: CDP/ISDP
    Is Monitored ?: true
    Serial Number of the Device: QTFCU3826001C
    RCF Version: v1.8X2 for
Cluster/HA/RDMA

```

## Switch Cisco

Configurare un nome utente SNMPv3 SNMPv3\_USER sugli switch Cisco 9336C-FX2:

- Per **nessuna autenticazione**:

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

- Per l'autenticazione **MD5/SHA**:

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

- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

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

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

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

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

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

Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
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. Impostare l'utente SNMPv3 sul lato ONTAP:

```
security login create -user-or-group-name <username> -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1  
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true  
  
cluster1::*> security login create -user-or-group-name <username>  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)  
[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

### 3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: 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. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

```
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

Configurare un nome utente SNMPv3 SNMPv3\_USER sugli switch NVIDIA SN2100 che eseguono CLI 5.4.0:

- Per **nessuna autenticazione**:

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

- Per l'autenticazione **MD5/SHA**:

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

- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

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

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

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

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

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

## Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
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. Impostare l'utente SNMPv3 sul lato ONTAP:

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::>* security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                         Device Name: sw1
(b8:59:9f:09:7c:22)
                                         IP Address: 10.231.80.212
                                         SNMP Version: SNMPv2c
                                         Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
                                         Community String or SNMPv3 Username: cshml!
                                         Model Number: MSN2100-CB2FC
                                         Switch Network: cluster-network
                                         Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                                         Reason For Not Monitoring: None
                                         Source Of Switch Version: LLDP
                                         Is Monitored ?: true
                                         Serial Number of the Device: MT2110X06399 <-----
serial number to check
                                         RCF Version: MSN2100-RCF-v1.9X6-
Cluster-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. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

```
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

Configurare un nome utente SNMPv3 SNMPv3\_USER sugli switch NVIDIA SN2100 che eseguono CLI 5.11.0:

- Per **nessuna autenticazione**:

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

- Per l'autenticazione **MD5/SHA**:

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

- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

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

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

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

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

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

## Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
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. Impostare l'utente SNMPv3 sul lato ONTAP:

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,  
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters  
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

### 3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                         Device Name: sw1
(b8:59:9f:09:7c:22)
                                         IP Address: 10.231.80.212
                                         SNMP Version: SNMPv2c
                                         Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
                                         Community String or SNMPv3 Username: cshml!
                                         Model Number: MSN2100-CB2FC
                                         Switch Network: cluster-network
                                         Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                                         Reason For Not Monitoring: None
                                         Source Of Switch Version: LLDP
                                         Is Monitored ?: true
                                         Serial Number of the Device: MT2110X06399 <-----
serial number to check
                                         RCF Version: MSN2100-RCF-v1.9X6-
Cluster-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. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

```
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

```

## Controllare lo stato dello switch

### Panoramica del controllo di stato

I monitor dello stato di salute monitorano in modo proattivo determinate condizioni critiche nel cluster e avvisano se rilevano un guasto o un rischio.

Per visualizzare gli avvisi di monitoraggio dello stato degli switch Ethernet attualmente generati, eseguire il comando: `system health alert show -monitor ethernet-switch`

Per visualizzare gli avvisi disponibili sul monitor dello stato dello switch Ethernet, eseguire il comando: `system health alert definition show -monitor ethernet-switch`

### Gestire il monitoraggio degli switch Ethernet

Nella maggior parte dei casi, gli switch Ethernet vengono rilevati automaticamente da ONTAP e monitorati da CSHM. Il file di configurazione di riferimento (RCF) applicato allo switch, tra le altre cose, attiva il protocollo di rilevamento Cisco (CDP) e/o il protocollo LLDP (link Layer Discovery Protocol). Tuttavia, potrebbe essere necessario aggiungere manualmente uno switch non rilevato o rimuovere uno switch non più in uso. È inoltre

possibile interrompere il monitoraggio attivo mantenendo l'interruttore nella configurazione, ad esempio durante la manutenzione.

### Creare una voce dello switch in modo che ONTAP possa monitorarla

Utilizzare il `system switch ethernet create` comando per configurare manualmente e attivare il monitoraggio per uno switch Ethernet specificato. Ciò è utile se ONTAP non aggiunge automaticamente lo switch o se lo switch è stato rimosso in precedenza e si desidera aggiungerlo nuovamente.

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

Un esempio tipico è l'aggiunta di uno switch denominato [deviceName], con l'indirizzo IP 1.2.3.4 e le credenziali SNMPv2c impostate su **cshm1!**. Utilizzare `-type storage-network` invece di `-type cluster-network` se si sta configurando uno switch di archiviazione.

### Disattivare il monitoraggio senza eliminare l'interruttore

Se si desidera sospendere o interrompere il monitoraggio di un determinato switch, ma conservarlo per il monitoraggio futuro, modificare il `is-monitoring-enabled-admin` parametro invece di eliminarlo.

Ad esempio:

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

In questo modo è possibile conservare i dettagli e la configurazione dello switch senza generare nuovi avvisi o nuove rilevazioni.

### Rimuovere uno switch non più necessario

Utilizzare `system switch ethernet delete` per eliminare un interruttore scollegato o non più necessario:

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

Per impostazione predefinita, questo comando funziona solo se ONTAP non rileva attualmente lo switch tramite CDP o LLDP. Per rimuovere uno switch rilevato, utilizzare il `-force` parametro:

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

Quando `-force` viene utilizzato, lo switch potrebbe essere aggiunto nuovamente automaticamente se ONTAP lo rileva nuovamente.

## Verificare il monitoraggio degli switch Ethernet

Il monitor dello stato dello switch Ethernet (CSHM) tenta automaticamente di monitorare gli switch rilevati; tuttavia, il monitoraggio potrebbe non avvenire automaticamente se gli switch non sono configurati correttamente. Verificare che il monitor dello stato di salute sia configurato correttamente per monitorare gli switch.

### Verificare il monitoraggio degli switch Ethernet collegati

Per confermare che gli switch Ethernet collegati siano monitorati, eseguire:

```
system switch ethernet show
```

Se la Model colonna visualizza **ALTRO** o il IS Monitored campo visualizza **falso**, ONTAP non è in grado di monitorare l'interruttore. Un valore **ALTRO** indica in genere che ONTAP non supporta tale switch per il monitoraggio dello stato.

Il IS Monitored campo è impostato su **false** per il motivo specificato nel Reason campo.



Se uno switch non è elencato nell'output del comando, è probabile che ONTAP non lo abbia rilevato. Verificare che l'interruttore sia cablato correttamente. Se necessario, è possibile aggiungere manualmente lo switch. Vedere "[Gestire il monitoraggio degli switch Ethernet](#)" per ulteriori dettagli.

### Verificare che le versioni firmware e RCF siano aggiornate

Assicurarsi che lo switch esegua il firmware più recente supportato e che sia stato applicato un file di configurazione di riferimento (RCF) compatibile. Ulteriori informazioni sono disponibili sul "[Pagina Support Downloads di NetApp](#)".

Per impostazione predefinita, il monitor sanitario utilizza SNMPv2c con la stringa di comunità **cshm1!** per il monitoraggio, ma è anche possibile configurare SNMPv3.

Se è necessario modificare la stringa di comunità SNMPv2c predefinita, assicurarsi che la stringa di comunità SNMPv2c desiderata sia stata configurata sullo switch.

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



Per ulteriori informazioni sulla configurazione di SNMPv3 per l'uso, vedere "[Opzionale: Configurare SNMPv3](#)".

### Confermare la connessione alla rete di gestione

Verificare che la porta di gestione dello switch sia collegata alla rete di gestione.

Per eseguire query SNMP e la ONTAP raccolta di log, è necessaria una connessione corretta alla porta di gestione.

## Risolvere i problemi relativi agli avvisi

Gli avvisi vengono generati in caso di rilevamento di un guasto, di un rischio o di una condizione critica per uno switch Ethernet nel cluster.

Se vengono generati degli avvisi, lo stato di salute del sistema indica uno stato degradato per il cluster. Gli avvisi generati includono le informazioni necessarie per rispondere a problemi di integrità del sistema.

Per visualizzare gli avvisi disponibili sul monitor dello stato dello switch Ethernet, eseguire il comando: `system health alert definition show -monitor ethernet-switch`

Per informazioni dettagliate sulla risoluzione avanzata degli avvisi, consultare l'articolo della Knowledge base ["Guida alla risoluzione degli avvisi dello switch Health Monitor"](#).

## Raccolta di log

### Panoramica della raccolta di log

Una volta impostata la raccolta dei log, è possibile abilitare una raccolta oraria di dati periodici raccolti da AutoSupport e richiedere log di supporto dettagliati.

Per ulteriori informazioni, vedere ["Configurare la raccolta di log"](#).

### Risolvere i problemi relativi alla raccolta dei log

Se si verifica uno dei seguenti stati di errore riportati dalla funzione di raccolta del registro (visibile nell'output del `system switch ethernet log show` comando), provare i passi di debug corrispondenti:

Stato errore raccolta log	Risoluzione
Chiavi RSA non presenti	Rigenerare le chiavi SSH ONTAP.
Errore di modifica della password	Verificare le credenziali, verificare la connettività SSH e rigenerare le chiavi SSH ONTAP. Per istruzioni, consultare la documentazione dello switch o contattare l'assistenza NetApp.
Chiavi ECDSA non presenti per FIPS	Se la modalità FIPS è attivata, le chiavi ECDSA devono essere generate sullo switch prima di riprovare.
Trovato log preesistente	Rimuovere il file di raccolta del registro precedente sullo switch.
Errore registro dump switch	Assicurarsi che l'utente dello switch disponga delle autorizzazioni per la raccolta dei registri. Fare riferimento ai prerequisiti riportati sopra.



Se i dettagli della risoluzione non funzionano, contattare l'assistenza NetApp.

## **Informazioni sul copyright**

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

**LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE:** l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## **Informazioni sul marchio commerciale**

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.