



Configurar la monitorización del estado del switch

Install and maintain

NetApp
February 13, 2026

Tabla de contenidos

- Configurar la monitorización del estado del switch 1
 - Descripción general de la configuración 1
 - Configurar la recopilación de registros 1
 - Antes de empezar 1
 - Pasos 2
 - Configure SNMPv3 para su switch (opcional) 8

Configurar la monitorización del estado del switch

Descripción general de la configuración

El monitor de estado del conmutador Ethernet (CSHM) es responsable de garantizar el buen funcionamiento de los conmutadores de red de clúster y almacenamiento y de recopilar los registros de los conmutadores con fines de depuración.

- ["Configurar la recopilación de registros"](#)
- ["Configurar SNMPv3 \(opcional\)"](#)

Configurar la recopilación de registros

El monitor de estado del conmutador Ethernet (CSHM) es responsable de garantizar el buen funcionamiento de los conmutadores de red de clúster y almacenamiento y de recopilar los registros de los conmutadores con fines de depuración. Este procedimiento le guía a través del proceso de configuración de la recopilación, la solicitud de registros detallados de **Soporte** y la habilitación de una recopilación horaria de datos **Periódicos** que recopila AutoSupport.

NOTA: Si activa el modo FIPS, deberá completar lo siguiente:



1. Regenera las claves SSH en el switch siguiendo las instrucciones del proveedor.
2. Regenerar claves SSH en ONTAP usando `debug system regenerate-systemshell-key-pair`
3. Vuelva a ejecutar la rutina de configuración de recopilación de registros utilizando `system switch ethernet log setup-password dominio`

Antes de empezar

- El usuario debe tener acceso al interruptor. `show` comandos. Si estos no están disponibles, cree un nuevo usuario y otórguele los permisos necesarios.
- La monitorización del estado del switch debe estar habilitada. Verifique esto asegurándose de que `Is Monitored:` El campo se establece en **verdadero** en la salida de `system switch ethernet show dominio`.
- Para la recopilación de registros con switches Broadcom y Cisco :
 - El usuario local debe tener privilegios de administrador de red.
 - Se debe crear un nuevo usuario en el switch para cada configuración de clúster con la recopilación de registros habilitada. Estos conmutadores no admiten varias claves SSH para el mismo usuario. Cualquier configuración adicional de recopilación de registros que se realice sobrescribirá las claves SSH preexistentes del usuario.
- Para admitir la recopilación de registros con conmutadores NVIDIA , el *usuario* encargado de la recopilación de registros debe tener permiso para ejecutar el `cl-support` comando sin necesidad de

proporcionar una contraseña. Para permitir este uso, ejecute el comando:

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

Pasos

ONTAP 9.15.1 y posteriores

1. Para configurar la recopilación de registros, ejecute el siguiente comando para cada conmutador. Se le solicita que ingrese el nombre del switch, el nombre de usuario y la contraseña para la recopilación de registros.

NOTA: Si responde **sí** a la solicitud de especificación de usuario, asegúrese de que el usuario tenga los permisos necesarios, tal como se describe en [Antes de empezar](#).

```
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>
```



Para CL 5.11.1, cree el usuario **cumulus** y responda **y** a la siguiente pregunta: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. Habilitar la recopilación periódica de registros:

```
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. Recopilación de registros de soporte de solicitudes:

```
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. Para ver todos los detalles de la recopilación de registros, incluyendo la habilitación, el mensaje de estado, la marca de tiempo anterior y el nombre de archivo de la recopilación periódica, el estado de la solicitud, el mensaje de estado y la marca de tiempo anterior y el nombre de archivo de la recopilación de soporte, utilice lo siguiente:

```
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 y anteriores

1. Para configurar la recopilación de registros, ejecute el siguiente comando para cada conmutador. Se le solicita que ingrese el nombre del switch, el nombre de usuario y la contraseña para la recopilación de registros.

NOTA: Si responde y En la solicitud de especificación de usuario, asegúrese de que el usuario tenga los permisos necesarios como se describe en [Antes de empezar](#) .

```
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>
```



Para CL 5.11.1, cree el usuario **cumulus** y responda **y** a la siguiente pregunta: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. Para solicitar la recopilación de registros de soporte y habilitar la recopilación periódica, ejecute el siguiente comando. Esto inicia ambos tipos de recopilación de registros: la detallada. Support registros y una recopilación horaria de Periodic datos.

```
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.

Espere 10 minutos y luego compruebe que la recopilación de registros se haya completado:

```
system switch ethernet log show
```



Si la función de recopilación de registros informa de algún estado de error (visible en la salida de `system switch ethernet log show`), ver ["Solución de problemas de la recopilación de registros"](#) Para obtener más detalles.

¿Que sigue?

["Configurar SNMPv3 \(opcional\)"](#).

Configure SNMPv3 para su switch (opcional)

SNMP se utiliza para monitorizar los switches. La monitorización mediante SNMPv3 se configura siguiendo este procedimiento.

El monitor de estado del conmutador Ethernet (CSHM) utiliza SNMP para supervisar el estado y el rendimiento de los conmutadores de clúster y de almacenamiento. Por defecto, SNMPv2c se configura automáticamente a través del archivo de configuración de referencia (RCF). SNMPv3 es más seguro que SNMPv2 porque introduce características de seguridad robustas como la autenticación, el cifrado y la integridad de los mensajes, que protegen contra el acceso no autorizado y garantizan la confidencialidad e integridad de los datos durante la transmisión.



- SNMPv3 solo es compatible con ONTAP 9.12.1 y versiones posteriores.
- Las versiones ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 y posteriores solucionan estos dos problemas:
 - "Para la monitorización del estado de los switches Cisco ONTAP , es posible que aún se observe tráfico SNMPv2 después de cambiar a SNMPv3 para la monitorización."
 - "Alertas falsas positivas de ventilador y alimentación cuando se producen fallos SNMP"

Acerca de esta tarea

Los siguientes comandos se utilizan para configurar un nombre de usuario SNMPv3 en switches **Broadcom**, * Cisco* y * NVIDIA*:

conmutadores Broadcom

Configure un nombre de usuario SNMPv3 NETWORK-OPERATOR en los switches Broadcom BES-53248.

- Para **sin autenticación**:

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

- Para la **autenticación MD5/SHA**:

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

- Para la **autenticación MD5/SHA con cifrado AES/DES**:

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

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP :

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

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM:

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

Pasos

1. Configure el usuario SNMPv3 en el switch para usar autenticación y cifrado:

```
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 Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

2. Configure el usuario SNMPv3 en el lado 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. Configure CSHM para que realice la monitorización con el nuevo usuario 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: cshml!
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. Tras esperar el período de sondeo CSHM, verifique que el número de serie esté registrado para el conmutador 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

```

conmutadores Cisco

Configure un nombre de usuario SNMPv3_USER en los switches Cisco 9336C-FX2:

- Para **sin autenticación**:

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

- Para la **autenticación MD5/SHA**:

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

- Para la **autenticación MD5/SHA con cifrado AES/DES**:

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

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP :

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

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM:

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

Pasos

1. Configure el usuario SNMPv3 en el switch para usar autenticación y cifrado:

```
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. Configure el usuario SNMPv3 en el lado 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. Configure CSHM para que realice la monitorización con el nuevo usuario 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: cshml!
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. Verifique que el número de serie que se consultará con el usuario SNMPv3 recién creado sea el mismo que se detalla en el paso anterior una vez finalizado el período de sondeo de 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

Configure un nombre de usuario SNMPv3_USER en switches NVIDIA SN2100 con CLI 5.4.0:

- Para **sin autenticación**:

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

- Para la **autenticación MD5/SHA**:

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

- Para la **autenticación MD5/SHA con cifrado AES/DES**:

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

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP :

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

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM:

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

Pasos

1. Configure el usuario SNMPv3 en el switch para usar autenticación y cifrado:

```
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 laErrorMessage "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 1.3.6.1.2.1.31.1.1.18
/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. Configure el usuario SNMPv3 en el lado 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. Configure CSHM para que realice la monitorización con el nuevo usuario 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-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. Verifique que el número de serie que se consultará con el usuario SNMPv3 recién creado sea el mismo que se detalla en el paso anterior una vez finalizado el período de sondeo de 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-LLDP Aug-18-2022

```

NVIDIA - CL 5.11.0

Configure un nombre de usuario SNMPv3_USER en switches NVIDIA SN2100 con CLI 5.11.0:

- Para **sin autenticación**:

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

- Para la **autenticación MD5/SHA**:

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

- Para la **autenticación MD5/SHA con cifrado AES/DES**:

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

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP :

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

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM:

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

Pasos

1. Configure el usuario SNMPv3 en el switch para usar autenticación y cifrado:

```
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. Configure el usuario SNMPv3 en el lado 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. Configure CSHM para que realice la monitorización con el nuevo usuario 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-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. Verifique que el número de serie que se consultará con el usuario SNMPv3 recién creado sea el mismo que se detalla en el paso anterior una vez finalizado el período de sondeo de 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

```

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.