



Supervisar el estado del conmutador IP de MetroCluster

ONTAP MetroCluster

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap-metrocluster/install-ip/configure-cshm-mccip.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Supervisar el estado del conmutador IP de MetroCluster 1
 - Obtenga información sobre la supervisión del estado del conmutador en una configuración IP de MetroCluster..... 1
 - Notas importantes para configurar CSHM en una configuración IP de MetroCluster 1
 - Configurar SNMPv3 para supervisar el estado de los conmutadores IP de MetroCluster 1
 - Configurar la recopilación de registros en un conmutador IP de MetroCluster 19
 - Antes de empezar 20
 - Pasos 20
 - Administrar la monitorización de conmutadores Ethernet en una configuración IP de MetroCluster 26
 - Cree una entrada de conmutador para que ONTAP pueda supervisarla 26
 - Desactive la supervisión sin eliminar el conmutador 27
 - Retire un interruptor que ya no necesite 27
 - Verificar la monitorización del conmutador Ethernet en una configuración IP de MetroCluster 27
 - Confirmar la supervisión de los switches Ethernet conectados..... 28
 - Confirme que el firmware y las versiones de RCF están actualizadas 28
 - Confirme la conexión de red de gestión 28

Supervisar el estado del conmutador IP de MetroCluster

Obtenga información sobre la supervisión del estado del conmutador en una configuración IP de MetroCluster

El monitor de estado del switch Ethernet (CSHM) es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración.

Notas importantes para configurar CSHM en una configuración IP de MetroCluster

Esta sección contiene los pasos genéricos para configurar SNMPv3 y la recopilación de registros en switches Cisco, Broadcom y NVIDIA SN2100. Debe seguir los pasos para una versión de firmware de switch compatible con una configuración IP de MetroCluster. Consulte la ["Hardware Universe"](#) para verificar las versiones de firmware compatibles.

En una configuración de MetroCluster, se configura la supervisión del estado únicamente en los conmutadores del clúster local.

Para la recopilación de registros con switches Broadcom y Cisco, se debe crear un nuevo usuario en el switch para cada clúster que tenga habilitada la recopilación de registros. En una configuración MetroCluster, esto significa que MetroCluster 1, MetroCluster 2, MetroCluster 3 y MetroCluster 4 requieren la configuración de un usuario independiente en los switches. Estos switches no admiten varias claves SSH para el mismo usuario. Cualquier configuración de recopilación de registros adicional realizada sobrescribe las claves SSH preexistentes para el usuario.

Antes de configurar el CSHM, debe deshabilitar los ISL no utilizados para evitar alertas de ISL innecesarias.

Configurar SNMPv3 para supervisar el estado de los conmutadores IP de MetroCluster

En las configuraciones IP de MetroCluster, puede configurar SNMPv3 para supervisar el estado de los switches IP.

Este procedimiento muestra los pasos genéricos para configurar SNMPv3 en un conmutador. Es posible que algunas de las versiones de firmware del conmutador mencionadas no sean compatibles con una configuración IP de MetroCluster.

Debe seguir los pasos para una versión de firmware del conmutador compatible con una configuración IP de MetroCluster. Consulte la ["Hardware Universe"](#) para verificar las versiones de firmware compatibles.



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

Acerca de esta tarea

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

Switches Broadcom

Configure un OPERADOR DE RED DE nombre de usuario SNMPv3 en los conmutadores Broadcom BES-53248.

- Para **sin autenticación**:

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

- Para **autenticación MD5/SHA**:

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

- Para 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 conmutador para que utilice 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 monitorizar con el nuevo usuario de 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. Después de esperar el período de sondeo de CSHM, verifique que el número de serie esté completo 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

```

Switches Cisco

Configure un nombre de usuario SNMPv3_USER de SNMPv3 en switches Cisco 9336C-FX2:

- Para **sin autenticación**:

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

- Para **autenticación MD5/SHA**:

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

- Para 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 conmutador para que utilice 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 monitorizar con el nuevo usuario de 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. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado 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 SNMPv3_USER en los conmutadores NVIDIA SN2100 que ejecutan CLI 5.4.0:

- Para **sin autenticación**:

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

- Para **autenticación MD5/SHA**:

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

- Para 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 conmutador para que utilice 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 1.3.6.1.2.1.31.1.1.1.18
/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
syservices 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 monitorizar con el nuevo usuario de 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. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado 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 `SNMPv3_USER` en los conmutadores NVIDIA SN2100 que ejecutan CLI 5.11.0:

- Para **sin autenticación**:

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

- Para **autenticación MD5/SHA**:

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

- Para 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 conmutador para que utilice 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 monitorizar con el nuevo usuario de 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. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado 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

```

Configurar la recopilación de registros en un conmutador IP de MetroCluster

En una configuración de IP de MetroCluster, puede configurar la recopilación de registros para recopilar registros de conmutadores con fines de depuración.



En los switches Broadcom y Cisco, se requiere un nuevo usuario para cada clúster con recopilación de registros. Por ejemplo, MetroCluster 1, MetroCluster 2, MetroCluster 3 y MetroCluster 4 requieren la configuración de un usuario independiente en los switches. No se admiten varias claves SSH para el mismo usuario.

Acerca de esta tarea

El monitor de estado del switch Ethernet (CSHM) es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración. Este procedimiento lo guía a través del proceso de configuración de la recopilación, solicitando registros detallados de **Soporte** y habilitando una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

NOTA: Si habilita el modo FIPS, debe completar lo siguiente:



1. Vuelva a generar las claves SSH en el switch siguiendo las instrucciones del proveedor.
2. Regenerar claves SSH en ONTAP mediante `debug system regenerate-systemshell-key-pair`
3. Volver a ejecutar la rutina de configuración de la recogida de registros con `system switch ethernet log setup-password` el comando

Antes de empezar

- El usuario debe tener acceso a los comandos de cambio `show`. Si no están disponibles, cree un nuevo usuario y otorgue los permisos necesarios al usuario.
- La monitorización del estado del interruptor debe estar activada para el interruptor. Verifique esto asegurándose de que `Is Monitored:` El campo se establece en **verdadero** en la salida del `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 usuario nuevo en el switch de cada configuración del clúster con la recopilación de registros habilitada. Estos switches no admiten varias claves SSH para el mismo usuario. Cualquier configuración de recopilación de registros adicional realizada sobrescribe las claves SSH preexistentes para el usuario.
- Para la recopilación de registros de soporte con conmutadores NVIDIA, se debe permitir que `user` para la recopilación de registros ejecute `cl-support` el comando sin tener que 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 versiones posteriores

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

NOTA: Si responde **y** a la solicitud de especificación del 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** al siguiente mensaje: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. **[[paso 2]]** 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. Solicitar recogida de registros de soporte:

```
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 recogida de registros, incluida la habilitación, el mensaje de estado, la marca de hora y el nombre de archivo anteriores de la recogida periódica, el estado de la solicitud, el mensaje de estado, y la marca de hora y el nombre de archivo anteriores de la recogida 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 pedirá que introduzca el nombre del switch, el nombre de usuario y la contraseña para la recopilación de registros.

NOTA: Si responde *y* a la solicitud de especificación del usuario, asegúrese de que el usuario tiene 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** al siguiente mensaje: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. **[[paso 2]]** 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: Los registros detallados `Support` y una recogida de datos por hora `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.

Espere 10 minutos y compruebe que se complete la recopilación de registros:

```
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`), consulte ["Solución de problemas de recopilación de registros"](#) para obtener más información.

Administrar la monitorización de conmutadores Ethernet en una configuración IP de MetroCluster

En la mayoría de los casos, los conmutadores Ethernet son descubiertos automáticamente por ONTAP y monitoreados por CSHM. El archivo de configuración de referencia (RCF) aplicado al switch, entre otras cosas, habilita el protocolo de detección de Cisco (CDP) y/o el protocolo de detección de capa de enlace (LLDP). Sin embargo, es posible que necesite agregar manualmente un conmutador que no se detecte o eliminar un conmutador que ya no esté en uso. También puede detener la supervisión activa mientras mantiene el interruptor en la configuración, como durante el mantenimiento.

Cree una entrada de conmutador para que ONTAP pueda supervisarla

Acerca de esta tarea

Utilice `system switch ethernet create` el comando para configurar y activar manualmente la supervisión de un switch Ethernet especificado. Esto es útil si ONTAP no agrega el conmutador automáticamente, o si ya eliminó el conmutador y desea volver a agregarlo.

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

Un ejemplo típico es agregar un conmutador llamado [DeviceName], con la dirección IP 1.2.3.4, y las credenciales SNMPv2c establecidas en **cshml!**. Utilice `-type storage-network` en lugar de `-type cluster-network` si va a configurar un switch de almacenamiento.

Desactive la supervisión sin eliminar el conmutador

Si desea pausar o detener la supervisión de un determinado conmutador, pero aún así conservarlo para una supervisión futura, modifique su `is-monitoring-enabled-admin` parámetro en lugar de eliminarlo.

Por ejemplo:

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

Esto le permite conservar los detalles del switch y la configuración sin generar nuevas alertas o nuevas detecciones.

Retire un interruptor que ya no necesite

Se utiliza `system switch ethernet delete` para eliminar un interruptor que se ha desconectado o que ya no es necesario:

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

De manera predeterminada, este comando solo se ejecuta correctamente si ONTAP no detecta actualmente el switch a través de CDP o LLDP. Para quitar un conmutador detectado, utilice el `-force` parámetro:

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

Cuando `-force` se utiliza, el interruptor puede volver a añadirse automáticamente si ONTAP lo detecta de nuevo.

Verificar la monitorización del conmutador Ethernet en una configuración IP de MetroCluster

El monitor de estado del switch Ethernet (CSHM) intenta monitorizar automáticamente los conmutadores que detecta; sin embargo, es posible que la supervisión no se realice automáticamente si los conmutadores no están configurados correctamente. Debe verificar que el monitor de estado esté correctamente configurado para supervisar los switches.

Confirmar la supervisión de los switches Ethernet conectados

Acerca de esta tarea

Para confirmar que se están supervisando los conmutadores Ethernet conectados, ejecute:

```
system switch ethernet show
```

Si la `Model` columna muestra **OTHER** o el `IS Monitored` campo muestra **false**, ONTAP no puede monitorear el conmutador. Un valor de **OTHER** normalmente indica que ONTAP no admite ese cambio para el monitoreo de salud.

El `IS Monitored` campo se establece en **false** por el motivo especificado en el `Reason` campo.



Si un conmutador no aparece en la salida del comando, es probable que ONTAP no lo haya descubierto. Confirme que el interruptor esté cableado correctamente. Si es necesario, puede agregar el conmutador manualmente. Consulte ["Gestionar la supervisión de switches Ethernet"](#) Para más detalles.

Confirme que el firmware y las versiones de RCF están actualizadas

Asegúrese de que el switch esté ejecutando el firmware más reciente compatible y de que se haya aplicado un archivo de configuración de referencia compatible (RCF). Más información está disponible en el ["Página de descargas de soporte de NetApp"](#).

De forma predeterminada, el monitor de estado utiliza SNMPv2c con la cadena comunitaria **csbm1!** para el monitoreo, pero también se puede configurar SNMPv3.

Si necesita cambiar la cadena de comunidad SNMPv2c predeterminada, asegúrese de que la cadena de comunidad SNMPv2c deseada se haya configurado en el switch.

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



Consulte ["Opcional: Configure SNMPv3"](#) para obtener más información sobre la configuración de SNMPv3 para su uso.

Confirme la conexión de red de gestión

Compruebe que el puerto de gestión del switch está conectado a la red de gestión.

Se requiere una conexión de puerto de gestión correcta para que ONTAP ejecute consultas SNMP y recopile registros.

Información relacionada

- ["Solucionar problemas de alertas"](#)

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.