



Supervise el estado del interruptor

Cluster and storage switches

NetApp
August 09, 2024

Tabla de contenidos

- Supervise el estado del interruptor 1
 - Descripción general del monitor de estado del switch 1
 - Configure la supervisión de estado del switch 1
 - Compruebe el estado del interruptor 22
 - Recopilación de registros 23

Supervise el estado del interruptor

Descripción general del monitor de estado del switch

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.

Configure la supervisión de estado del switch

Información general de configuración

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.

- ["Configure la recopilación de registros"](#)
- ["Opcional: Configure SNMPv3"](#)

Configure la recopilación de registros

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 teclas ssh en el interruptor, según las instrucciones del proveedor.
2. Regenerar las teclas ssh en el lado de ONTAP mediante `debug system regenerate-systemshell-key-pair`
3. Volver a ejecutar la rutina de configuración de la recopilación de registros mediante `system switch ethernet log setup-password`

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 el `Is Monitored:` el campo se establece en **true** en la salida del `system switch ethernet show` comando.
- Para los switches NVIDIA, el usuario para la recopilación de registros debe tener permiso para ejecutar los comandos de recopilación de registros sin mostrar una solicitud de contraseña. Para permitir este uso,

ejecute el comando: `echo '<username> ALL = NOPASSWD: /usr/cumulus/bin/cl-support, /usr/sbin/csmgrctl' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus`

Pasos

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.

```
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>
```

2. Para solicitar la recopilación de registros de soporte y activar 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
```

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.

```
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>
```

2. Activar Recopilación Periódica de Log:

```
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.

3. 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.
```

4. 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.
```



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.

El futuro

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

Opcional: Configure SNMPv3 para su switch

SNMP se utiliza para supervisar los switches. El monitor de estado del switch Ethernet (CSHM) utiliza SNMP para supervisar el estado y el rendimiento del clúster y los switches de almacenamiento. De forma predeterminada, 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 y la integridad de los datos durante la transmisión.



SNMPv3 solo es compatible con ONTAP 9.12.1 y versiones posteriores.

Siga este procedimiento para configurar SNMPv3 para su conmutador específico, que es compatible con CSHM.

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. 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: 10.228.136.24
                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: CLI 5,4

Configure un nombre de usuario SNMPv3 SNMPv3_USER en los switches NVIDIA SN2100 que ejecutan CLI 5,4:

- Para **sin autenticación**:

```
net add snmp-server username SNMPv3_USER auth-none
```

- Para **autenticación MD5/SHA**:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-
PASSWORD
```

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

```
net add 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 4.4.3 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
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 4.4.3 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

```

Compruebe el estado del interruptor

Información general de la comprobación del estado

Los monitores de estado supervisan proactivamente ciertas condiciones críticas de su clúster y generan alertas si detectan una falla o un riesgo.

Para ver las alertas del monitor de estado del switch Ethernet actualmente elevadas, ejecute el comando: `system health alert show -monitor ethernet-switch`

Para ver las alertas de control de estado del switch Ethernet disponibles, ejecute el comando: `system health alert definition show -monitor ethernet-switch`

Solucionar problemas de alertas

Las alertas se generan si se detecta un fallo, un riesgo o una condición crítica en un switch Ethernet de su clúster.

Si hay alertas activas, el estado del sistema informa del estado Degradado del clúster. Las alertas emitidas incluyen la información que necesita para responder al estado del sistema degradado.

Para ver las alertas de control de estado del switch Ethernet disponibles, ejecute el comando: `system health alert definition show -monitor ethernet-switch`

Consulte el artículo de la base de conocimientos ["Guía de resolución de alertas del monitor de estado del switch"](#) para obtener información detallada sobre la resolución avanzada de las alertas.

Recopilación de registros

Descripción general de la recopilación de registros

Al configurar la recogida de registros, es posible habilitar una recogida horaria de datos periódicos recogidos por AutoSupport, y solicitar registros de soporte detallados.

Consulte ["Configure la recopilación de registros"](#) para obtener más información.

Solución de problemas de recopilación de registros

Si encuentra alguno de los siguientes estados de error indicados por la función de recopilación de registros (visibles en la salida del `system switch ethernet log show` comando), intente los pasos de depuración correspondientes:

| Estado de error de recopilación de registros | Resolución |
|---|--|
| Las claves RSA no están presentes | Vuelva a generar las claves SSH de ONTAP. |
| Error de contraseña de cambio | Verifique las credenciales, pruebe la conectividad SSH y vuelva a generar las claves SSH de ONTAP. Revise la documentación del switch o póngase en contacto con el soporte de NetApp para obtener instrucciones. |
| Las claves ECDSA no están presentes para FIPS | Si el modo FIPS está activado, es necesario generar claves ECDSA en el conmutador antes de volver a intentarlo. |
| Registro preexistente encontrado | Elimine el archivo de recopilación de registros anterior del conmutador. |
| Error de registro de volcado del interruptor | Asegúrese de que el usuario del conmutador tiene permisos de recopilación de registros. Consulte los requisitos previos anteriores. |



Si los detalles de la resolución no funcionan, póngase en contacto con el soporte de NetApp.

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.