



# **Monitorar a integridade do switch IP do MetroCluster**

ONTAP MetroCluster

NetApp  
February 13, 2026

# Índice

|   |    |
|---|----|
| Monitorar a integridade do switch IP do MetroCluster .....  | 1  |
| Saiba mais sobre o monitoramento da integridade do switch em uma configuração de IP do MetroCluster ..... | 1  |
| Notas importantes para configurar o CSHM em uma configuração de IP do MetroCluster .....                  | 1  |
| Configurar SNMPv3 para monitorar a integridade dos switches IP do MetroCluster .....                      | 1  |
| Configurar coleta de logs em um switch IP do MetroCluster .....   | 19 |
| Antes de começar .....  | 20 |
| Passos .....  | 20 |
| Gerenciar o monitoramento de switches Ethernet em uma configuração IP do MetroCluster .....               | 26 |
| Crie uma entrada de switch para que o ONTAP possa monitorá-la .....                                       | 26 |
| Desative a monitorização sem eliminar o interruptor .....   | 27 |
| Remova um switch que você não precisa mais .....  | 27 |
| Verificar o monitoramento do switch Ethernet em uma configuração de IP do MetroCluster .....              | 27 |
| Confirme o monitoramento dos switches Ethernet conectados .....   | 28 |
| Confirme se as versões do firmware e do RCF estão atualizadas .....                                       | 28 |
| Confirme a conexão de rede de gerenciamento .....   | 28 |

# Monitorar a integridade do switch IP do MetroCluster

## Saiba mais sobre o monitoramento da integridade do switch em uma configuração de IP do MetroCluster

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir a integridade operacional dos switches de rede Cluster e Storage e coletar logs de switch para fins de depuração.

### Notas importantes para configurar o CSHM em uma configuração de IP do MetroCluster

Esta seção contém as etapas genéricas para configurar SNMPv3 e coleta de logs em switches Cisco, Broadcom e NVIDIA SN2100. Você deve seguir as etapas para uma versão de firmware de switch compatível com uma configuração de IP do MetroCluster. Consulte a seção ["Hardware Universe"](#) para verificar as versões de firmware suportadas.

Em uma configuração do MetroCluster, você configura o monitoramento de integridade somente nos switches do cluster local.

Para coleta de logs com switches Broadcom e Cisco, um novo usuário deve ser criado no switch para cada cluster com coleta de logs habilitada. Em uma configuração MetroCluster, isso significa que o MetroCluster 1, o MetroCluster 2, o MetroCluster 3 e o MetroCluster 4 exigem a configuração de um usuário separado nos switches. Esses switches não suportam várias chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleção de logs executada substitui quaisquer chaves SSH pré-existentes para o usuário.

Antes de configurar o CSHM, você deve desabilitar ISLs não utilizados para evitar alertas de ISL desnecessários.

## Configurar SNMPv3 para monitorar a integridade dos switches IP do MetroCluster

Nas configurações IP do MetroCluster, você pode configurar o SNMPv3 para monitorar a integridade dos switches IP.

Este procedimento mostra as etapas genéricas para configurar o SNMPv3 em um switch. Algumas das versões de firmware de switch listadas podem não ser suportadas em uma configuração de IP do MetroCluster.

Você deve seguir as etapas para uma versão de firmware do switch compatível com uma configuração de IP do MetroCluster. Consulte a ["Hardware Universe"](#) para verificar as versões de firmware suportadas.



- O SNMPv3 só é suportado no ONTAP 9.12,1 e posterior.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 e versões posteriores corrigem estes dois problemas:
  - "Para monitoramento de integridade ONTAP de switches Cisco, o tráfego SNMPv2 ainda pode ser visto após a mudança para SNMPv3 para monitoramento"
  - "Alertas de energia e ventilador de switch falso-positivos quando ocorrem falhas de SNMP"

#### Sobre esta tarefa

Os comandos a seguir são usados para configurar um nome de usuário SNMPv3 nos switches **Broadcom**, **Cisco** e **NVIDIA**:

## Switches Broadcom

Configure um OPERADOR DE REDE de nome de usuário SNMPv3 em switches Broadcom BES-53248.

- Para **sem autenticação**:

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

- Para **MD5/SHA autenticação**:

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

- Para autenticação **MD5/SHA com criptografia AES/DES**:

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

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

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

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

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

## Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
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 o usuário SNMPv3 no 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 o CSHM para monitorar com o novo usuário 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. Após aguardar o período de pesquisa do CSHM, verifique se o número de série do switch Ethernet está preenchido.

```

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 um nome de usuário SNMPv3 SNMPv3\_USER em switches Cisco 9336C-FX2:

- Para **sem autenticação**:

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

- Para **MD5/SHA autenticação**:

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

- Para autenticação **MD5/SHA com criptografia AES/DES**:

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

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

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



O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

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

## Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
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 o usuário SNMPv3 no 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 o CSHM para monitorar com o novo usuário 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 se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```
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 um nome de usuário SNMPv3 SNMPv3\_USER em switches NVIDIA SN2100 executando CLI 5.4.0:

- Para **sem autenticação**:

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

- Para **MD5/SHA autenticação**:

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

- Para autenticação **MD5/SHA com criptografia AES/DES**:

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

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

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

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

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

## Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
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
  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<br>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 o usuário SNMPv3 no 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 o CSHM para monitorar com o novo usuário 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 se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```

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 um nome de usuário SNMPv3 SNMPv3\_USER em switches NVIDIA SN2100 executando CLI 5.11.0:

- Para **sem autenticação**:

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

- Para **MD5/SHA autenticação**:

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

- Para autenticação **MD5/SHA com criptografia AES/DES**:

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

O seguinte comando configura um nome de usuário SNMPv3 no lado ONTAP:

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

O seguinte comando estabelece o nome de usuário SNMPv3 com CSHM:

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

## Passos

1. Configure o usuário SNMPv3 no switch para usar autenticação e criptografia:

```
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 o usuário SNMPv3 no 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 o CSHM para monitorar com o novo usuário 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 se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo que detalhado na etapa anterior após o período de polling CSHM ter sido concluído.

```
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 coleta de logs em um switch IP do MetroCluster

Em uma configuração de IP do MetroCluster, você pode configurar a coleta de logs para coletar logs de switches para fins de depuração.



Em switches Broadcom e Cisco, um novo usuário é necessário para cada cluster com coleta de logs. Por exemplo, MetroCluster 1, MetroCluster 2, MetroCluster 3 e MetroCluster 4 exigem a configuração de um usuário separado nos switches. Não há suporte para várias chaves SSH para o mesmo usuário.

### Sobre esta tarefa

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir a integridade operacional dos switches de rede Cluster e Storage e coletar logs de switch para fins de depuração. Este procedimento orienta você pelo processo de configuração da coleta, solicitando Registros detalhados de **suporte** e permitindo uma coleta por hora de dados **Periódicos** coletados pela AutoSupport.

**NOTA:** se você ativar o modo FIPS, você deve concluir o seguinte:



1. Regenerar chaves SSH no switch usando as instruções do fornecedor.
2. Regenerar chaves SSH no ONTAP usando `debug system regenerate-systemshell-key-pair`
3. Execute novamente a rotina de configuração da coleção de logs usando o `system switch ethernet log setup-password` comando

## Antes de começar

- O usuário deve ter acesso aos comandos do switch `show`. Se não estiverem disponíveis, crie um novo usuário e conceda as permissões necessárias ao usuário.
- A monitorização do estado do interruptor tem de estar ativada para o interruptor. Verifique isso garantindo que o `Is Monitored:` campo esteja definido como **true** na saída do `system switch ethernet show` comando.
- Para coleta de logs com switches Broadcom e Cisco:
  - O usuário local deve ter privilégios de administrador de rede.
  - Um novo usuário deve ser criado no switch para cada configuração de cluster com a coleção de logs ativada. Esses switches não suportam várias chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleção de logs executada substitui quaisquer chaves SSH pré-existentes para o usuário.
- Para a coleta de logs de suporte com switches NVIDIA, o `user` para coleta de logs deve ter permissão para executar o `cl-support` comando sem ter que fornecer uma senha. Para permitir esse uso, execute o comando:

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

## Passos

## ONTAP 9.15,1 e posterior

1. Para configurar a coleção de logs, execute o seguinte comando para cada switch. Você será solicitado a digitar o nome do switch, nome de usuário e senha para a coleta de logs.

**NOTA:** Se responder **y** ao prompt de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias, conforme descrito em [Antes de começar](#).

```
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, crie o usuário **cumulus** e responda **y** ao seguinte prompt: Gostaria de especificar um usuário diferente de admin para coleta de logs? {y|n}: **y**

1. Habilitar coleta periódica de logs:

```
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 coleção de logs de suporte:

```
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 exibir todos os detalhes da coleção de logs, incluindo a habilitação, mensagem de status, carimbo de data/hora anterior e nome do arquivo da coleção periódica, o status da solicitação, a mensagem de status e o carimbo de data/hora e nome do arquivo anterior da coleção de suporte, use o seguinte:

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

Switch Name: cs1
Periodic Log Enabled: true
Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
Last Periodic Log Timestamp: 3/11/2024 11:02:59
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:14:20
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

Switch Name: cs2
Periodic Log Enabled: false
Periodic Log Status: Periodic collection has been
halted.
Last Periodic Log Timestamp: 3/11/2024 11:05:18
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:18:54
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

#### ONTAP 9.14,1 e anteriores

1. Para configurar a coleção de logs, execute o seguinte comando para cada switch. Você será solicitado a digitar o nome do switch, nome de usuário e senha para a coleta de logs.

**OBSERVAÇÃO:** se responder y ao prompt de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias conforme descrito em [Antes de começar](#).

```
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, crie o usuário **cumulus** e responda **y** ao seguinte prompt: Gostaria de especificar um usuário diferente de admin para coleta de logs? {y|n}: **y**

1. Para solicitar a coleta de logs de suporte e habilitar a coleta periódica, execute o seguinte comando. Isso inicia ambos os tipos de coleta de log: Os logs detalhados Support e uma coleta de dados 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.

Aguarde 10 minutos e, em seguida, verifique se a coleção de registros é concluída:

```
system switch ethernet log show
```



Se algum estado de erro for comunicado pela funcionalidade de recolha de registos (visível na saída do `system switch ethernet log show`), consulte ["Solucionar problemas na coleta de logs"](#) para obter mais detalhes.

## Gerenciar o monitoramento de switches Ethernet em uma configuração IP do MetroCluster

Na maioria dos casos, os switches Ethernet são automaticamente descobertos pelo ONTAP e monitorados pelo CSHM. O arquivo de configuração de referência (RCF) aplicado ao switch, entre outras coisas, ativa o protocolo de descoberta de Cisco (CDP) e/ou o protocolo de descoberta de camada de enlace (LLDP). No entanto, talvez seja necessário adicionar manualmente um switch que não seja descoberto ou remover um switch que não esteja mais em uso. Também pode parar a monitorização ativa mantendo o interruptor na configuração, como durante a manutenção.

### Crie uma entrada de switch para que o ONTAP possa monitorá-la

#### Sobre esta tarefa

Use o `system switch ethernet create` comando para configurar e ativar manualmente o monitoramento de um switch Ethernet especificado. Isso é útil se o ONTAP não adicionar o switch automaticamente ou se você removeu o switch anteriormente e deseja adicioná-lo novamente.

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

Um exemplo típico é adicionar um switch chamado [deviceName], com endereço IP 1,2.3,4 e credenciais SNMPv2c definidas como **cshml!**. Use `-type storage-network` em vez de `-type cluster-network` se você estiver configurando um switch de armazenamento.

## Desative a monitorização sem eliminar o interruptor

Se você quiser pausar ou parar o monitoramento de um determinado switch, mas ainda mantê-lo para monitoramento futuro, modifique seu `is-monitoring-enabled-admin` parâmetro em vez de excluí-lo.

Por exemplo:

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

Isso permite que você preserve os detalhes e a configuração do switch sem gerar novos alertas ou redescobertas.

## Remova um switch que você não precisa mais

Utilize `system switch ethernet delete` para eliminar um interruptor que tenha sido desligado ou que já não seja necessário:

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

Por padrão, esse comando só será bem-sucedido se o ONTAP não detectar o switch atualmente através do CDP ou do LLDP. Para remover um switch descoberto, use o `-force` parâmetro:

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

`-force` Quando o é usado, o switch pode ser readicionado automaticamente se o ONTAP o detectar novamente.

## Verificar o monitoramento do switch Ethernet em uma configuração de IP do MetroCluster

O monitor de integridade do switch Ethernet (CSHM) tenta monitorar automaticamente os switches que ele descobre; no entanto, o monitoramento pode não acontecer automaticamente se os switches não estiverem configurados corretamente. Você deve

verificar se o monitor de integridade está configurado corretamente para monitorar seus switches.

## Confirme o monitoramento dos switches Ethernet conectados

### Sobre esta tarefa

Para confirmar se os switches Ethernet conectados estão sendo monitorados, execute:

```
system switch ethernet show
```

Se a `Model` coluna exibir **OTHER** ou o `IS Monitored` campo exibir **false**, o ONTAP não poderá monitorar o switch. Um valor de **OTHER** normalmente indica que o ONTAP não suporta esse switch para monitoramento de integridade.

O `IS Monitored` campo é definido como **false** pelo motivo especificado no `Reason` campo.



Se um switch não estiver listado na saída do comando, é provável que o ONTAP não o tenha descoberto. Confirme se o switch está conectado corretamente. Se necessário, você pode adicionar o switch manualmente. Consulte ["Gerenciar o monitoramento de switches Ethernet"](#) para mais detalhes.

## Confirme se as versões do firmware e do RCF estão atualizadas

Certifique-se de que o comutador está a executar o firmware suportado mais recente e de que foi aplicado um ficheiro de configuração de referência (RCF) compatível. Mais informações estão disponíveis no ["Página de transferências do suporte da NetApp"](#).

Por padrão, o monitor de integridade usa SNMPv2c com a string da comunidade **csbm1!** para monitoramento, mas SNMPv3 também pode ser configurado.

Se você precisar alterar a cadeia de caracteres padrão da comunidade SNMPv2c, certifique-se de que a string de comunidade SNMPv2c desejada tenha sido configurada no switch.

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



["Opcional: Configurar SNMPv3"](#) Consulte para obter detalhes sobre como configurar o SNMPv3 para uso.

## Confirme a conexão de rede de gerenciamento

Verifique se a porta de gerenciamento do switch está conectada à rede de gerenciamento.

Uma conexão de porta de gerenciamento correta é necessária para que o ONTAP execute consultas SNMP e coleta de logs.

### Informações relacionadas

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

## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

**LEGENDA DE DIREITOS LIMITADOS:** o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.