Monitorar o estado do interruptor

Install and maintain

NetApp
February 13, 2026

Índice

Monitorar o estado do interruptor

Visão geral do monitor de integridade do switch

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração.

Configure o monitoramento de integridade do switch.

Visão geral da configuração

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração.

- "Configurar coleta de logs"
- "Configurar SNMPv3 (Opcional)"

Configurar coleta de logs

O monitor de integridade do switch Ethernet (CSHM) é responsável por garantir o funcionamento adequado dos switches de rede do cluster e do armazenamento, além de coletar logs dos switches para fins de depuração. Este procedimento orienta você no processo de configuração da coleta, solicitação de registros detalhados de **Suporte** e ativação da coleta horária de dados **Periódicos** coletados pelo AutoSupport.

NOTA: Se você ativar o modo FIPS, deverá concluir o seguinte:

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

Antes de começar

- O usuário deve ter acesso ao interruptor. `show` comandos. Caso essas opções não estejam disponíveis, crie um novo usuário e conceda as permissões necessárias a ele.
- O monitoramento de integridade do switch deve estar ativado. Verifique isso certificando-se de que `Is Monitored:` O campo é definido como **verdadeiro** 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 coleta de logs

habilitada. Esses switches não suportam múltiplas chaves SSH para o mesmo usuário. Qualquer configuração adicional de coleta de logs realizada sobrescreverá quaisquer chaves SSH preexistentes do usuário.

- Para suporte à coleta de logs com switches NVIDIA , o *usuário* responsável pela coleta de logs deve ter permissão para executar o comando. `cl-support` comando sem precisar 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 coleta de logs, execute o seguinte comando para cada switch. Você será solicitado a inserir o nome do switch, o nome de usuário e a senha para a coleta de logs.

   NOTA: Se responder **s** à solicitação de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias, conforme descrito emAntes 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** à seguinte mensagem: Deseja especificar um usuário diferente de admin para a coleta de logs? {s|n}: **s**

1. [[passo 2]]Ativar a 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 suporte para coleta de registros:

```
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 visualizar todos os detalhes da coleta de logs, incluindo a ativação, a mensagem de status, o carimbo de data/hora anterior e o nome do arquivo da coleta periódica, bem como o status da solicitação, a mensagem de status e o carimbo de data/hora anterior e o nome do arquivo da coleta de suporte, utilize o seguinte comando:

```
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 coleta de logs, execute o seguinte comando para cada switch. Você será solicitado a inserir o nome do switch, o nome de usuário e a senha para a coleta de logs.

   NOTA: Se responder `y` Na solicitação de especificação do usuário, certifique-se de que o usuário tenha as permissões necessárias, conforme descrito emAntes 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** à seguinte mensagem: Deseja especificar um usuário diferente de admin para a coleta de logs? {s|n}: **s**

1. [[passo 2]] Para solicitar a coleta de logs de suporte e habilitar a coleta periódica, execute o seguinte comando. Isso inicia os dois tipos de coleta de logs: a detalhada `Support` registros e uma coleta horária de `Periodic` dados.

```
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 verifique se a coleta de logs foi concluída:

```
system switch ethernet log show
```

Se algum status de erro for relatado pelo recurso de coleta de logs (visível na saída de `system switch ethernet log show`), ver"Solução de problemas na coleta de logs" Para obter mais detalhes.

O que vem a seguir?

"Configurar SNMPv3 (Opcional)".

Configure o SNMPv3 para o seu switch (Opcional)

O SNMP é usado para monitorar os switches. O monitoramento por SNMPv3 é configurado seguindo este procedimento.

O Ethernet Switch Health Monitor (CSHM) utiliza SNMP para monitorar a integridade e o desempenho de switches de cluster e de armazenamento. Por padrão, o SNMPv2c é configurado automaticamente através do Arquivo de Configuração de Referência (RCF). O SNMPv3 é mais seguro que o SNMPv2 porque introduz recursos de segurança robustos, como autenticação, criptografia e integridade de mensagens, que protegem contra acesso não autorizado e garantem a confidencialidade e integridade dos dados durante a transmissão.

- O SNMPv3 só é compatível com o ONTAP 9.12.1 e versões posteriores.
- O ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 e versões posteriores corrigem esses dois problemas:
  - "Para monitoramento de integridade do ONTAP em switches Cisco , o tráfego SNMPv2 ainda pode ser observado após a migração para o SNMPv3."
  - "Alertas falsos positivos de ventoinha e energia do switch quando ocorrem falhas SNMP."

Sobre esta tarefa

Os seguintes comandos são usados para configurar um nome de usuário SNMPv3 em switches **Broadcom**, * Cisco* e * NVIDIA*:

switches Broadcom

Configure um nome de usuário SNMPv3 NETWORK-OPERATOR em switches Broadcom BES-53248.

- Para **nenhuma autenticação**:

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

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

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

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 Priv
                                     Meth Meth    Remote Engine ID
---------------- ------------------ ---- ------
-------------------------
<username>        network-admin      MD5  AES128
8000113d03d8c497710bee
```

2. Configure o usuário SNMPv3 no lado do 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: cshm1!
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Após aguardar o período de consulta do CSHM, verifique se o número de série está preenchido para o switch Ethernet.

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

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

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

switches Cisco

Configure um nome de usuário SNMPv3, SNMPv3_USER, nos switches Cisco 9336C-FX2:

- Para **nenhuma autenticação**:

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

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

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

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 do 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: cshm1!
                                   Model Number: N9K-C9336C-FX2
                                 Switch Network: cluster-network
                               Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                     Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Verifique se o número de série a ser consultado com o usuário SNMPv3 recém-criado é o mesmo detalhado na etapa anterior, após a conclusão do período de pesquisa 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 um nome de usuário SNMPv3, SNMPv3_USER, em switches NVIDIA SN2100 executando a CLI 5.4.0:

- Para **nenhuma autenticação**:

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

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

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

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 laErrMessage "laTable" laErrorFlag != 0
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```
 pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
 pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! 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 o usuário SNMPv3 no lado do 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: cshm1!
                                 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 detalhado na etapa anterior, após a conclusão do período de pesquisa 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 um nome de usuário SNMPv3, SNMPv3_USER, em switches NVIDIA SN2100 executando a CLI 5.11.0:

- Para **nenhuma autenticação**:

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

- Para autenticação **MD5/SHA**:

```
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 comando a seguir configura um nome de usuário SNMPv3 no lado do ONTAP :

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

O comando a seguir estabelece o nome de usuário SNMPv3 com o 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 do 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: cshm1!
                                 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 detalhado na etapa anterior, após a conclusão do período de pesquisa 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
```

Verifique o estado do interruptor.

Visão geral do check-up de saúde

Os monitores de integridade monitoram proativamente determinadas condições críticas em seu cluster e emitem alertas caso detectem uma falha ou risco.

Para visualizar os alertas de monitoramento de integridade do switch Ethernet atualmente em execução, execute o comando: `system health alert show -monitor ethernet-switch`

Para visualizar os alertas disponíveis do monitor de integridade do switch Ethernet, execute o comando: `system health alert definition show -monitor ethernet-switch`

Gerenciar o monitoramento de switches Ethernet

Na maioria dos casos, os switches Ethernet são descobertos automaticamente pelo ONTAP e monitorados pelo CSHM. O arquivo de configuração de referência (RCF) aplicado ao switch, entre outras coisas, habilita o Cisco Discovery Protocol (CDP) e/ou o Link Layer Discovery Protocol (LLDP). No entanto, pode ser necessário adicionar manualmente um interruptor que não foi detectado ou remover um interruptor que não

está mais em uso. Você também pode interromper o monitoramento ativo, mantendo o switch na configuração, por exemplo, durante a manutenção.

Crie uma entrada de interruptor para que o ONTAP possa monitorá-la.

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

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -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 **cshm1!**. Usar `-type storage-network` em vez de `-type cluster-network` Se você estiver configurando um switch de armazenamento.

Desative o monitoramento sem excluir o interruptor.

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

Por exemplo:

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

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

Remova um interruptor que você não precisa mais.

Usar `system switch ethernet delete` Para excluir um interruptor que foi desconectado ou não é mais necessário:

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

Por padrão, este comando só terá sucesso se o ONTAP não detectar o switch por meio de CDP ou LLDP. Para remover um interruptor detectado, use o `-force` parâmetro:

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

Quando `-force` Se o ONTAP o detectar novamente, ele poderá ser adicionado novamente de forma automática.

Verifique o monitoramento dos switches Ethernet.

O monitor de integridade do switch Ethernet (CSHM) tenta monitorar automaticamente os switches que detecta; no entanto, o monitoramento pode não ocorrer 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.

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

```
system switch ethernet show
```

Se o `Model` A coluna exibe **OUTRO** ou o `IS Monitored` Se o campo exibir **false**, o ONTAP não poderá monitorar o switch. Um valor de **OUTRO** normalmente indica que o ONTAP não suporta essa opção para monitoramento de integridade.

O `IS Monitored` O campo está definido como **falso** pelo motivo especificado no `Reason` campo.

> Se um switch não estiver listado na saída do comando, é provável que o ONTAP ainda não o tenha detectado. Confirme se o interruptor está conectado corretamente. Se necessário, você pode adicionar o interruptor manualmente. Ver"Gerenciar o monitoramento de switches Ethernet" Para obter mais detalhes.

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

Certifique-se de que o switch esteja executando o firmware mais recente compatível e que um arquivo de configuração de referência (RCF) compatível tenha sido aplicado. Mais informações estão disponíveis emhttps://mysupport.netapp.com/site/downloads["Página de downloads de suporte da NetApp"^] .

Por padrão, o monitor de integridade usa SNMPv2c com a string de comunidade **cshm1!** para monitoramento, mas o SNMPv3 também pode ser configurado.

Se precisar alterar a string de comunidade SNMPv2c padrão, certifique-se de que a string de comunidade SNMPv2c desejada esteja configurada no switch.

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

> Ver"Opcional: Configurar SNMPv3" Para obter detalhes sobre como configurar o SNMPv3 para uso.

Confirme a conexão da rede de gerenciamento.

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

Para que o ONTAP execute consultas SNMP e colete logs, é necessária uma conexão correta à porta de

gerenciamento.

Solucionar problemas de alertas

Os alertas são gerados se uma falha, risco ou condição crítica for detectada em um switch Ethernet do seu cluster.

Caso sejam acionados alertas, o status de integridade do sistema será relatado como degradado para o cluster. Os alertas gerados incluem as informações necessárias para que você possa responder à degradação da integridade do sistema.

Para visualizar os alertas disponíveis do monitor de integridade do switch Ethernet, execute o comando: `system health alert definition show -monitor ethernet-switch`

Consulte o artigo da Base de Conhecimento. "Guia de Resolução de Alertas do Monitor de Saúde do Switch" Para obter detalhes avançados sobre a resolução de alertas.

Coleta de registros

Visão geral da coleta de logs

Com a coleta de logs configurada, você pode habilitar a coleta horária de dados periódicos que são coletados pelo AutoSupport e solicitar logs de suporte detalhados.

Ver"Configurar coleta de logs" Para obter mais detalhes.

Solução de problemas na coleta de logs

Se você encontrar algum dos seguintes códigos de erro relatados pelo recurso de coleta de logs (visíveis na saída do `system switch ethernet log show` comando), tente as etapas de depuração correspondentes:

Status de erro na coleta de logs	Resolução
Chaves RSA não presentes	Regenerar as chaves SSH do ONTAP .
Erro na senha do switch	Verificar credenciais, testar a conectividade SSH e regenerar as chaves SSH do ONTAP . Consulte a documentação do switch ou entre em contato com o suporte da NetApp para obter instruções.
Chaves ECDSA não presentes para FIPS	Se o modo FIPS estiver ativado, as chaves ECDSA precisam ser geradas no switch antes de tentar novamente.
Registro pré-existente encontrado	Remova o arquivo de coleta de logs anterior no switch.

Erro no log de despejo do switch	Certifique-se de que o usuário do switch tenha permissões de coleta de logs. Consulte os pré-requisitos acima.

Se as instruções de resolução não funcionarem, entre em contato com o suporte da NetApp .

Informações sobre direitos autorais

Informações sobre marcas comerciais