监控 **MetroCluster IP** 交换机的运行状况

ONTAP MetroCluster

NetApp
February 13, 2026

目录

监控 MetroCluster IP 交换机的运行状况

了解 MetroCluster IP 配置中的交换机运行状况监控

以太网交换机运行状况监控器(CSHM)负责确保集群和存储网络交换机的运行状况、并收集交换机日志以进行调试。

在 MetroCluster IP 配置中配置 CSHM 的重要注意事项

本节包含在 Cisco、Broadcom 和 NVIDIA SN2100 交换机上配置 SNMPv3 和日志收集的通用步骤。您必须遵循 MetroCluster IP 配置支持的交换机固件版本的步骤。请参阅"Hardware Universe"验证支持的固件版本。

在 MetroCluster 配置中，仅在本地集群交换机上配置运行状况监控。

对于使用 Broadcom 和 Cisco 交换机收集日志的情况，应在交换机上为每个启用了日志收集功能的集群创建一个新用户。在 MetroCluster 配置中，这意味着 MetroCluster 1、MetroCluster 2、MetroCluster 3 和 MetroCluster 4 都需要在交换机上配置单独的用户。这些交换机不支持同一用户使用多个SSH密钥。执行的任何其他日志收集设置都会覆盖用户的任何已有SSH密钥。

在配置 CSHM 之前，您应该禁用未使用的 ISL 以避免任何不必要的 ISL 警报。

配置 SNMPv3 来监控MetroCluster IP 交换机的运行状况

在MetroCluster IP配置中、您可以将SNMPv3配置为监控IP交换机的运行状况。

此过程显示在交换机上配置 SNMPv3 的通用步骤。列出的某些交换机固件版本可能不受 MetroCluster IP 配置支持。

您必须按照 MetroCluster IP 配置支持的交换机固件版本的步骤操作。请参阅"Hardware Universe"验证支持的固件版本。

- 仅ONTAP 9.12.1及更高版本支持SNMPv3。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 及更高版本修复了以下两个问题：
  - "对于 Cisco 交换机的 ONTAP 运行状况监控，切换到 SNMPv3 进行监控后仍可能看到 SNMPv2 流量"
  - "SNMP 故障发生时误报交换机风扇和电源警报"

关于此任务

以下命令用于在*Broadcom*、*Cisco*和*NVIDIA*交换机上配置SNMPv3用户名：

Broadcom交换机

在Broadcom BES-53248交换机上配置SNMPv3用户名network-operator。

- 对于*no authentication (无身份验证)*：

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

- 对于*MD5/SHA身份验证*：

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

- 对于采用AES/DES加密的*MD5/SHA身份验证*：

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

以下命令在ONTAP端配置SNMPv3用户名：

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

以下命令将使用CSHM建立SNMPv3用户名：

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

步骤

1. 在交换机上设置SNMPv3用户以使用身份验证和加密：

```
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. 在ONTAP 端设置SNMPv3用户：

```
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. 将CSHM配置为使用新SNMPv3用户进行监控：

```
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. 等待 CSHM 轮询期后，验证以太网交换机的序列号是否已填充。

```
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
```

Cisco switches

在Cisco 9334c-966交换机上配置SNMPv3用户名SNMPv3 _user：

- 对于*no authentication (无身份验证)*：

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

- 对于*MD5/SHA身份验证*：

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

- 对于采用AES/DES加密的*MD5/SHA身份验证*：

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

以下命令在ONTAP端配置SNMPv3用户名：

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

以下命令将使用CSHM建立SNMPv3用户名：

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

步骤

1. 在交换机上设置SNMPv3用户以使用身份验证和加密：

```
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. 在ONTAP 端设置SNMPv3用户：

```
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. 将CSHM配置为使用新SNMPv3用户进行监控：

```
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. 确认要使用新创建的SNMPv3用户查询的序列号与CSHM轮询周期完成后上一步中详述的序列号相同。

```
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

在运行 CLI 5.4.0 的 NVIDIA SN2100 交换机上配置 SNMPv3 用户名 SNMPv3_USER：

- 对于*no authentication (无身份验证)*：

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

- 对于*MD5/SHA身份验证*：

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

- 对于采用AES/DES加密的*MD5/SHA身份验证*：

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

以下命令在ONTAP端配置SNMPv3用户名：

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

以下命令将使用CSHM建立SNMPv3用户名：

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

步骤

1. 在交换机上设置SNMPv3用户以使用身份验证和加密：

```
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. 在ONTAP 端设置SNMPv3用户：

```
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. 将CSHM配置为使用新SNMPv3用户进行监控：

```
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. 确认要使用新创建的SNMPv3用户查询的序列号与CSHM轮询周期完成后上一步中详述的序列号相同。

```
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

在运行 CLI 5.11.0 的 NVIDIA SN2100 交换机上配置 SNMPv3 用户名 SNMPv3_USER：

- 对于*no authentication (无身份验证)*：

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

- 对于*MD5/SHA身份验证*：

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

- 对于采用AES/DES加密的*MD5/SHA身份验证*：

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

以下命令在ONTAP端配置SNMPv3用户名：

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

以下命令将使用CSHM建立SNMPv3用户名：

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

步骤

1. 在交换机上设置SNMPv3用户以使用身份验证和加密：

```
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. 在ONTAP 端设置SNMPv3用户：

```
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. 将CSHM配置为使用新SNMPv3用户进行监控：

```
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. 确认要使用新创建的SNMPv3用户查询的序列号与CSHM轮询周期完成后上一步中详述的序列号相同。

```
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
```

在 MetroCluster IP 交换机上配置日志收集

在 MetroCluster IP 配置中，您可以配置日志收集以收集交换机日志以用于调试目的。

在 Broadcom 和 Cisco 交换机上，每个具有日志收集功能的集群都需要一个新用户。例如，MetroCluster 1、MetroCluster 2、MetroCluster 3 和 MetroCluster 4 均需要在交换机上配置单独的用户。不支持为同一用户配置多个 SSH 密钥。

关于此任务

以太网交换机运行状况监控器(CSHM)负责确保集群和存储网络交换机的运行状况、并收集交换机日志以进行调试。此过程将指导您完成设置收集、请求详细的*Support*日志以及启用每小时收集AutoSupport收集的*定期*数据的过程。

*注：*如果启用FIPS模式，则必须完成以下操作：

1. 按照供应商说明在交换机上重新生成SSH密钥。
2. 使用在ONTAP中重新生成SSH密钥 `debug system regenerate-systemshell-key-pair`
3. 使用 `system switch ethernet log setup-password`命令重新运行日志收集设置例程

开始之前

- 用户必须能够访问交换机 `show` 命令。如果这些权限不可用、请创建一个新用户并向该用户授予必要的权限。
- 必须为交换机启用交换机运行状况监控。通过确保 `Is Monitored:`字段在输出中设置为 **true** `system switch ethernet show`命令。
- 要使用Broadcom和Cisco交换机收集日志、请执行以下操作：
  - 本地用户必须具有网络管理员权限。
  - 应在交换机上为启用了日志收集的每个集群设置创建一个新用户。这些交换机不支持同一用户使用多个SSH密钥。执行的任何其他日志收集设置都会覆盖用户的任何已有SSH密钥。
- 要使用NVIDIA交换机收集支持日志、必须允许用于收集日志的_user_运行 `cl-support`命令、而无需提供密码。要允许使用此命令、请运行以下命令：

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

步骤

ONTAP 9.15.1 及更高版本

1. 要设置日志收集、请对每个交换机运行以下命令。系统会提示您输入交换机名称、用户名和密码以收集日志。

   注意：*如果对用户规范提示回答 ***y**，请确保用户具有必要的权限，如[开始之前] 。

```
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>
```

对于 CL 5.11.1，创建用户 **cumulus** 并对以下提示回复 **y**：Would you like to specify a user other than admin for log collection? {y|n}: **y**

1. 启用定期日志收集：

```
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. 请求支持日志收集：

```
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. 要查看日志收集的所有详细信息、包括启用、状态消息、定期收集的先前时间戳和文件名、请求状态、状态消息以及支持收集的先前时间戳和文件名、请使用以下命令：

```
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及更早版本

1. 要设置日志收集、请对每个交换机运行以下命令。系统会提示您输入交换机名称、用户名和密码以收集日志。

   *注：*如果回答 `y`用户规范提示，请确保用户具有中所述的必要权限[开始之前]。

```
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>
```

对于 CL 5.11.1，创建用户 **cumulus** 并对以下提示回复 **y**：Would you like to specify a user other than admin for log collection? {y|n}: **y**

1. 要请求支持日志收集并启用定期收集，请运行以下命令。此时将开始两种类型的日志收集：详细 `Support` 日志和每小时数据收集 `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.
```

等待10分钟、然后检查日志收集是否完成：

```
system switch ethernet log show
```

如果日志收集功能报告了任何错误状态(在的输出中可见 `system switch ethernet log show`)，请参见以了解更多详细信息。 "对日志收集进行故障排除"

管理 MetroCluster IP 配置中的以太网交换机监控

在大多数情况下、以太网交换机会由ONTAP自动发现并由CSHM进行监控。应用于交换机的参考配置文件(Reference Configuration File、RCF)等功能可启用Cisco发现协议(CDP)和/或链路层发现协议(Link Layer Discovery Protocol、LDP)。但是、您可能需要手动添加未发现的交换机或删除不再使用的交换机。您还可以在将交换机保留在配置中的同时停止活动监控、例如在维护期间。

创建一个交换机条目、以便ONTAP可以对其进行监控

关于此任务

使用 `system switch ethernet create`命令为指定的以太网交换机手动配置和启用监控。如果ONTAP未自动添加交换机、或者您之前删除了交换机并希望重新添加它、则此功能非常有用。

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type
cluster-network
```

典型的示例是添加一个名为[DeviceName]的交换机、IP地址为1.2.3.4、SNMPv2c凭据设置为* cshm1！*。如果要配置存储交换机、请使用、 `-type storage-network`而不是 `-type cluster-network`。

禁用监控而不删除交换机

如果要暂停或停止监控某个交换机、但仍保留该交换机以供将来监控、请修改其参数、而不是将其 `is-monitoring-enabled-admim`删除。

例如：

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

这样、您就可以保留交换机详细信息和配置、而无需生成新警报或重新发现。

删除不再需要的交换机

`system switch ethernet delete`用于删除已断开连接或不再需要的交换机：

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

默认情况下、只有当ONTAP当前未通过CDP或LDP检测到交换机时、此命令才会成功。要删除已发现的交换机、请使用 `-force`参数：

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

使用时 `-force`、如果ONTAP再次检测到该交换机、则可能会自动重新添加该交换机。

验证 MetroCluster IP 配置中的以太网交换机监控

以太网交换机运行状况监控器(CSHM)会自动尝试监控其发现的交换机；但是、如果交换机配置不正确、则可能无法自动进行监控。您应验证是否已正确配置运行状况监控器以监控交换机。

确认监控已连接的以太网交换机

关于此任务

要确认已连接的以太网交换机正在受监控、请运行：

```
system switch ethernet show
```

如果 `Model`列显示*OTA*或 `IS Monitored`字段显示*false*，则ONTAP无法监控交换机。值*其他*通常表示ONTAP不支持使用该交换机进行运行状况监控。

由于在字段中指定的原因，此 `IS Monitored`字段将设置为*false* `Reason`。

如果命令输出中未列出交换机，则ONTAP可能尚未发现它。确认交换机的接线正确。如果需要，您可以手动添加交换机。请参阅"管理以太网交换机的监控"了解更多详情。

确认固件和RC框架 版本为最新

确保交换机运行的是受支持的最新固件、并且已应用兼容的参考配置文件(RCF)。有关详细信息，请参见https://mysupport.netapp.com/site/downloads["NetApp支持下载页面"^]。

默认情况下、运行状况监控器使用带有社区字符串* cshm1！*的SNMPv2c进行监控、但也可以配置SNMPv3。

如果需要更改默认SNMPv2c社区字符串、请确保已在交换机上配置所需的SNMPv2c社区字符串。

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

有关配置SNMPv3以供使用的详细信息、请参见"可选：配置SNMPv3"。

确认管理网络连接

验证交换机的管理端口是否已连接到管理网络。

要使ONTAP执行SNMP查询和日志收集、需要正确的管理端口连接。

相关信息

- "对警报进行故障排除"