监控交换机运行状况

Cluster and storage switches

NetApp
August 09, 2024

目录

监控交换机运行状况

交换机运行状况监控器概述

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。

配置交换机运行状况监控

配置概述

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。

- "配置日志收集"
- "可选：配置SNMPv3"

配置日志收集

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端重新生成ssh密钥 `debug system regenerate-systemshell-key-pair`
> 3. 使用重新运行日志收集设置例程 `system switch ethernet log setup-password`

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。通过确保进行验证 `Is Monitored:` 字段在的输出中设置为*TRUE* `system switch ethernet show` 命令：
- 对于NVIDIA交换机、必须允许日志收集用户在不显示密码提示的情况下运行日志收集命令。要允许使用此命令、请运行以下命令： `echo '<username> ALL = NOPASSWD: /usr/cumulus/bin/cl-support, /usr/sbin/csmgrctl' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus`

步骤

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。

   ```
   system switch ethernet log setup-password
   ```

   ```
   cluster1::*> system switch ethernet log setup-password
   Enter the switch name: <return>
   The switch name entered is not recognized.
   Choose from the following list:
   cs1
   cs2

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs1
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs2

   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>
   ```

2. 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
```

ONTAP 9.151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。

```
system switch ethernet log setup-password
```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. 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.
```

3. 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.
```

4. 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.
```

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"

下一步是什么?

"配置SNMPv3 (可选)"(英文)

可选：为交换机配置SNMPv3

SNMP用于监控交换机。以太网交换机运行状况监控器(CSHM)利用SNMP监控集群和存储交换机的运行状况和性能。默认情况下、SNMPv2c是通过参考配置文件(Reference Configuration File、RCF)自动配置的。

SNMPv3比SNMPv2更安全、因为它引入了身份验证、加密和消息完整性等强大的安全功能、可防止未经授权的访问、并确保数据在传输期间的机密性和完整性。

> 仅ONTAP 9.12.1及更高版本支持SNMPv3。

按照以下步骤为支持CSHM的特定交换机配置SNMPv3。

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. 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: 10.228.136.24
                                  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交换机

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 - CLI 5.4

在运行CLI 5.4的NVIDIA SN2100交换机上配置SNMPv3用户名SNMPv3 _user：

- 对于*no authentication (无身份验证)*：

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

- 对于*MD5/SHA身份验证*：

```
net add 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*：

```
net add 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 4.4.3 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. 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 4.4.3 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

检查交换机运行状况

运行状况检查概述

运行状况监控器会主动监控集群中的某些严重情况，并在检测到故障或风险时发出警报。

要查看当前引发的以太网交换机运行状况监控器警报、请运行以下命令： `system health alert show -monitor ethernet-switch`

要查看可用的以太网交换机运行状况监控器警报、请运行以下命令： `system health alert definition show -monitor ethernet-switch`

对警报进行故障排除

如果在集群中检测到以太网交换机出现故障、风险或严重情况、则会发出警报。

如果出现引发的警报、则系统运行状况状态会报告集群的降级状态。发出的警报包括对降级的系统运行状况做出响应所需的信息。

要查看可用的以太网交换机运行状况监控器警报、请运行以下命令： `system health alert definition`

```
show -monitor ethernet-switch
```

有关警报的高级解决方案详细信息、请参见知识库文章 "《交换机运行状况监控器警报解决指南》" 。

收集日志

日志收集概述

设置日志收集后、您可以每小时收集AutoSupport收集的定期数据、并请求详细的支持日志。

有关详细信息、请参见 "配置日志收集" 。

对日志收集进行故障排除

如果遇到日志收集功能报告的以下任一错误状态(显示在命令输出中 `system switch ethernet log show`)、请尝试相应的调试步骤：

日志收集错误状态	分辨率
RSA密钥不存在	重新生成ONTAP SSH密钥。
切换密码错误	验证凭据、测试SSH连接并重新生成ONTAP SSH密钥。查看交换机文档或联系NetApp支持部门以获取相关说明。
对于**FIPS**，ECDSA密钥不存在	如果启用了FIPS模式、则需要在重试之前在交换机上生成ECDSA密钥。
已找到已有日志	删除交换机上先前的日志收集文件。
交换机转储日志错误	确保交换机用户具有日志收集权限。请参阅上述前提条件。

ⓘ 如果解决方案详细信息不起作用、请联系NetApp支持部门。

版权信息

商标信息