スイッチの状態を監視する

Install and maintain

NetApp
February 13, 2026

目次

スイッチの状態を監視する

スイッチヘルスモニターの概要

イーサネット スイッチ ヘルス モニター (CSHM) は、クラスターおよびストレージ ネットワーク スイッチの動作の健全性を確認し、デバッグのためにスイッチ ログを収集する役割を担います。

スイッチのヘルスモニタリングを構成する

設定の概要

イーサネット スイッチ ヘルス モニター (CSHM) は、クラスターおよびストレージ ネットワーク スイッチの動作の健全性を確認し、デバッグのためにスイッチ ログを収集する役割を担います。

- "ログ収集を構成する"
- "SNMPv3 を構成する (オプション)"

ログ収集を構成する

イーサネット スイッチ ヘルス モニター (CSHM) は、クラスターおよびストレージ ネットワーク スイッチの動作の健全性を確認し、デバッグのためにスイッチ ログを収集する役割を担います。この手順では、収集の設定、詳細な サポート ログの要求、およびAutoSupportによって収集される 定期的 データの 1 時間ごとの収集の有効化のプロセスについて説明します。

注意: FIPS モードを有効にする場合は、次の手順を完了する必要があります。

1. ベンダーの指示に従ってスイッチ上の SSH キーを再生成します。
2. ONTAPでSSHキーを再生成するには `debug system regenerate-systemshell-key-pair`
3. ログ収集セットアップルーチンを再実行します。 `system switch ethernet log setup-password`指示

開始する前に

- ユーザーはスイッチにアクセスできる必要があります `show`コマンド。これらが利用できない場合は、新しいユーザーを作成し、そのユーザーに必要な権限を付与します。
- スイッチのヘルス モニタリングを有効にする必要があります。これを確かめるためには、 `Is Monitored:`フィールドが*true*に設定されている場合は、 `system switch ethernet show`指示。
- Broadcom およびCiscoスイッチによるログ収集の場合:
  - ローカル ユーザーにはネットワーク管理者権限が必要です。

- ログ収集が有効になっているクラスタ設定ごとに、スイッチ上に新しいユーザーを作成する必要があります。これらのスイッチは、同じユーザーに対して複数の SSH キーをサポートしません。追加のログ収集設定を実行すると、ユーザーの既存の SSH キーが上書きされます。

- NVIDIAスイッチによるログ収集をサポートするには、ログ収集の_ユーザー_に実行を許可する必要があります。 `cl-support`パスワードを入力しなくてもコマンドを実行できます。この使用を許可するには、次のコマンドを実行します。

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

手順

ONTAP 9.15.1以降

1. ログ収集を設定するには、スイッチごとに次のコマンドを実行します。ログ収集用のスイッチ名、ユーザー名、およびパスワードの入力を求められます。

   注意: ユーザー指定プロンプトに **y** と答える場合は、ユーザーが以下の必要な権限を持っていることを確認してください。[開始する前に] 。

```
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>
```

CL 5.11.1 の場合、ユーザー **cumulus** を作成し、次のプロンプトに **y** と応答します: ログ収集に admin 以外のユーザーを指定しますか? {y|n}: **y**

1. 定期的なログ収集を有効にする:

```
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. サポートログ収集をリクエスト:

```
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. 定期的な収集の有効化、ステータス メッセージ、前回のタイムスタンプとファイル名、サポート収集の要求ステータス、ステータス メッセージ、前回のタイムスタンプとファイル名など、ログ収集のすべての詳細を表示するには、以下を使用します。

```
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以前

1. ログ収集を設定するには、スイッチごとに次のコマンドを実行します。ログ収集用のスイッチ名、ユーザー名、およびパスワードの入力を求められます。

   注: 回答する場合 `y`ユーザー指定プロンプトが表示されたら、ユーザーが以下の必要な権限を持っていることを確認してください。[開始する前に] 。

```
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>
```

CL 5.11.1 の場合、ユーザー **cumulus** を作成し、次のプロンプトに **y** と応答します: ログ収集に admin 以外のユーザーを指定しますか? {y|n}: **y**

1. サポートログの収集を要求し、定期的な収集を有効にするには、次のコマンドを実行します。これにより、詳細なログ収集と、 `Support`ログと1時間ごとの収集 `Periodic`データ。

```
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.
```

10 分待ってから、ログ収集が完了したことを確認します。

```
system switch ethernet log show
```

ログ収集機能によってエラーステータスが報告された場合（ `system switch ethernet log show` ）、 見る"ログ収集のトラブルシューティング"詳細については、こちらをご覧ください。

次の手順

"SNMPv3 を構成する (オプション)"。

スイッチの**SNMPv3**を設定する（オプション）

スイッチを監視するために SNMP が使用されます。 SNMPv3 による監視は、次の手順に従って設定します。

イーサネット スイッチ ヘルス モニター (CSHM) は、SNMP を使用して、クラスターおよびストレージ スイッチのヘルスとパフォーマンスを監視します。デフォルトでは、SNMPv2c はリファレンス構成ファイル (RCF) を通じて自動的に構成されます。 SNMPv3 は、認証、暗号化、メッセージの整合性などの強力なセキュリティ機能を導入し、不正アクセスから保護し、送信中のデータの機密性と整合性を保証するため、SNMPv2 よりも安全です。

- SNMPv3 はONTAP 9.12.1 以降でのみサポートされます。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 以降のバージョンでは、次の 2 つの問題が修正されています。
  - "CiscoスイッチのONTAPヘルスモニタリングでは、モニタリングをSNMPv3に切り替えた後でもSNMPv2トラフィックが引き続き表示されることがあります。"
  - "SNMP障害発生時の誤検知スイッチファンおよび電源アラート"

タスク概要

次のコマンドは、**Broadcom**、* Cisco*、および * NVIDIA* スイッチで SNMPv3 ユーザー名を設定するために使用されます。

Broadcomスイッチ

Broadcom BES-53248 スイッチで SNMPv3 ユーザー名 NETWORK-OPERATOR を設定します。

- *認証なし*の場合:

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

- *MD5/SHA認証*の場合:

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

- **AES/DES** 暗号化による **MD5/SHA** 認証 の場合:

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

次のコマンドは、 ONTAP側で SNMPv3 ユーザー名を設定します。

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

次のコマンドは、CSHM を使用して SNMPv3 ユーザー名を確立します。

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

手順

1. 認証と暗号化を使用するために、スイッチ上の SNMPv3 ユーザーを設定します。

```
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. ONTAP側で SNMPv3 ユーザーを設定します。

```
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. 新しい SNMPv3 ユーザーで監視するように CSHM を構成します。

```
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. CSHM ポーリング期間を待った後、イーサネット スイッチのシリアル番号が入力されていることを確認します。

```
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スイッチ

Cisco 9336C-FX2 スイッチで SNMPv3 ユーザー名 SNMPv3_USER を設定します。

- *認証なし*の場合:

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

- *MD5/SHA認証*の場合:

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

- **AES/DES** 暗号化による **MD5/SHA** 認証 の場合:

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

次のコマンドは、 ONTAP側で SNMPv3 ユーザー名を設定します。

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

次のコマンドは、CSHM を使用して SNMPv3 ユーザー名を確立します。

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

手順

1. 認証と暗号化を使用するために、スイッチ上の SNMPv3 ユーザーを設定します。

```
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. ONTAP側で SNMPv3 ユーザーを設定します。

```
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. 新しい SNMPv3 ユーザーで監視するように CSHM を構成します。

```
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. CSHM ポーリング期間が完了した後、新しく作成された SNMPv3 ユーザーで照会されるシリアル番号が前の手順で詳細に説明したものと同じであることを確認します。

```
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

CLI 5.4.0 を実行しているNVIDIA SN2100 スイッチで SNMPv3 ユーザー名 SNMPv3_USER を設定します。

- *認証なし*の場合:

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

- *MD5/SHA認証*の場合:

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

- **AES/DES** 暗号化による **MD5/SHA** 認証 の場合:

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

次のコマンドは、 ONTAP側で SNMPv3 ユーザー名を設定します。

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

次のコマンドは、CSHM を使用して SNMPv3 ユーザー名を確立します。

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

手順

1. 認証と暗号化を使用するために、スイッチ上の SNMPv3 ユーザーを設定します。

```
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. ONTAP側で SNMPv3 ユーザーを設定します。

```
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. 新しい SNMPv3 ユーザーで監視するように CSHM を構成します。

```
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. CSHM ポーリング期間が完了した後、新しく作成された SNMPv3 ユーザーで照会されるシリアル番号が前の手順で詳細に説明したものと同じであることを確認します。

```
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

CLI 5.11.0 を実行しているNVIDIA SN2100 スイッチで SNMPv3 ユーザー名 SNMPv3_USER を設定します。

- *認証なし*の場合:

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

- *MD5/SHA認証*の場合:

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

- **AES/DES** 暗号化による **MD5/SHA** 認証 の場合:

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

次のコマンドは、 ONTAP側で SNMPv3 ユーザー名を設定します。

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

次のコマンドは、CSHM を使用して SNMPv3 ユーザー名を確立します。

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

手順

1. 認証と暗号化を使用するために、スイッチ上の SNMPv3 ユーザーを設定します。

```
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. ONTAP側で SNMPv3 ユーザーを設定します。

```
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. 新しい SNMPv3 ユーザーで監視するように CSHM を構成します。

```
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. CSHM ポーリング期間が完了した後、新しく作成された SNMPv3 ユーザーで照会されるシリアル番号が前の手順で詳細に説明したものと同じであることを確認します。

```
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
```

スイッチの状態を確認する

ヘルスチェックの概要

ヘルスモニタは、クラスタ内の特定のクリティカルな状態をプロアクティブに監視します。

現在発生しているイーサネット スイッチ ヘルス モニターのアラートを表示するには、次のコマンドを実行します。 `system health alert show -monitor ethernet-switch`

利用可能なイーサネット スイッチ ヘルス モニターのアラートを表示するには、次のコマンドを実行します。 `system health alert definition show -monitor ethernet-switch`

イーサネットスイッチの監視を管理する

ほとんどの場合、イーサネット スイッチはONTAPによって自動的に検出され、CSHMによって監視されます。スイッチに適用されるリファレンス コンフィギュレーション ファイル (RCF) により、 Cisco Discovery Protocol (CDP) や Link Layer Discovery Protocol (LLDP) などが有効になります。ただし、検出されないスイッチを手動で追加したり、使

用されなくなったスイッチを削除したりする必要がある場合があります。メンテナンス時など、スイッチを設定内に保持したままアクティブ モニタリングを停止することもできます。

ONTAPが監視できるようにスイッチエントリを作成します

使用 `system switch ethernet create`指定されたイーサネット スイッチの監視を手動で構成し、有効にするコマンド。これは、 ONTAP がスイッチを自動的に追加しない場合、または以前にスイッチを削除して再度追加する場合に役立ちます。

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

典型的な例としては、[DeviceName] という名前のスイッチを追加し、IP アドレスを 1.2.3.4 にし、SNMPv2c 資格情報を **cshm1!** に設定します。使用 `-type storage-network`の代わりに `-type cluster-network`ストレージスイッチを構成する場合。

スイッチを削除せずに監視を無効にする

特定のスイッチの監視を一時停止または停止したいが、将来の監視のために保持したい場合は、そのスイッチの `is-monitoring-enabled-admim`パラメータを削除するのではなく、そのまま残します。

例えば：

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

これにより、新しいアラートや再検出を生成せずに、スイッチの詳細と構成を保持できます。

不要になったスイッチを削除する

使用 `system switch ethernet delete`切断されたスイッチや不要になったスイッチを削除するには:

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

デフォルトでは、このコマンドは、 ONTAP が現在 CDP または LLDP を介してスイッチを検出していない場合にのみ成功します。検出されたスイッチを削除するには、 `-force`パラメータ:

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

いつ `-force`が使用されている場合、 ONTAP が再度検出すると、スイッチが自動的に再追加される可能性があります。

イーサネットスイッチの監視を確認する

イーサネット スイッチ ヘルス モニター (CSHM) は、検出したスイッチを自動的に監視しようとしますが、スイッチが正しく構成されていない場合は、監視が自動的に行われない可能性があります。ヘルスモニタが使用中のスイッチを監視するように適切に設定されていることを確認してください。

接続されたイーサネットスイッチの監視を確認する

接続されているイーサネット スイッチが監視されていることを確認するには、次のコマンドを実行します。

```
system switch ethernet show
```

もし `Model`列に*OTHER*または `IS Monitored`フィールドに「**false**」と表示されている場合、 ONTAP はスイッチを監視できません。通常、**OTHER** の値は、 ONTAP がそのスイッチのヘルス モニタリングをサポートしていないことを示します。

その `IS Monitored`フィールドは、指定された理由により*false*に設定されています。 `Reason`分野。

> コマンド出力にスイッチがリストされていない場合は、 ONTAPそのスイッチが検出されていない可能性があります。スイッチのケーブルが正しく接続されていることを確認します。必要に応じて、スイッチを手動で追加できます。見る"イーサネットスイッチの監視を管理する"詳細については、こちらをご覧ください。

ファームウェアと**RCF**のバージョンが最新であることを確認します

スイッチが最新のサポートされているファームウェアを実行していること、および互換性のある参照構成ファイル (RCF) が適用されていることを確認します。詳細は以下をご覧ください。https://mysupport.netapp.com/site/downloads["NetAppサポート ダウンロード ページ"^] 。

デフォルトでは、ヘルス モニターは監視にコミュニティ文字列 **cshm1!** を持つ SNMPv2c を使用しますが、SNMPv3 も設定できます。

デフォルトの SNMPv2c コミュニティ文字列を変更する必要がある場合は、必要な SNMPv2c コミュニティ文字列がスイッチに設定されていることを確認してください。

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

> 見る"オプション: SNMPv3 を構成する"SNMPv3 を使用するための設定の詳細については、こちらをご覧ください。

管理ネットワーク接続を確認する

スイッチの管理ポートが管理ネットワークに接続されているかを確認します。

ONTAPが SNMP クエリとログ収集を実行するには、正しい管理ポート接続が必要です。

アラートのトラブルシューティング

クラスター内のイーサネット スイッチで障害、リスク、または重大な状態が検出されると、アラートが生成されます。

アラートが発生した場合、システムのヘルス ステータスではクラスターの劣化ステータスが報告されます。発生したアラートには、システム状態の低下に対応するために必要な情報が含まれます。

利用可能なイーサネット スイッチ ヘルス モニターのアラートを表示するには、次のコマンドを実行します。
`system health alert definition show -monitor ethernet-switch`

ナレッジベースの記事を参照 "スイッチヘルスモニターアラート解決ガイド"アラートの詳細な解決方法については、こちらをご覧ください。

ログ収集

ログ収集の概要

ログ収集を設定すると、 AutoSupportによって収集される定期的なデータの 1 時間ごとの収集を有効にし、詳細なサポート ログを要求することができます。

見る"ログ収集を構成する"詳細については、こちらをご覧ください。

ログ収集のトラブルシューティング

ログ収集機能によって報告される以下のエラーステータス（ `system switch ethernet log show`コマンド) の場合は、対応するデバッグ手順を試してください。

ログ収集エラーステータス	解決
RSAキーが存在しません	ONTAP SSH キーを再生成します。
スイッチパスワードエラー	資格情報を確認し、SSH 接続をテストし、 ONTAP SSH キーを再生成します。スイッチのドキュメントを確認するか、 NetAppサポートに問い合わせて手順を確認してください。
FIPS では **ECDSA** キーは存在しません	FIPS モードが有効になっている場合は、再試行する前にスイッチで ECDSA キーを生成する必要があります。
既存のログが見つかりました	スイッチ上の以前のログ収集ファイルを削除します。
スイッチダンプログエラー	スイッチ ユーザーにログ収集権限があることを確認します。上記の前提条件を参照してください。

解決の詳細が機能しない場合は、 NetAppサポートにお問い合わせください。

著作権に関する情報

商標に関する情報