MetroCluster IPスイッチの健全性を監視する

ONTAP MetroCluster

NetApp
February 13, 2026

目次

MetroCluster IPスイッチの健全性を監視する

MetroCluster IP構成におけるスイッチヘルスモニタリングについて学習します

イーサネットスイッチヘルスモニタ（CSHM）は、クラスタネットワークスイッチと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、デバッグ用にスイッチのログを収集します。

MetroCluster IP構成でCSHMを構成する際の重要な注意事項

このセクションでは、Cisco、Broadcom、NVIDIA SN2100スイッチでSNMPv3とログ収集を設定するための一般的な手順について説明します。MetroCluster構成でサポートされているスイッチファームウェアバージョンに応じた手順に従う必要があります。"Hardware Universe"サポートされているファームウェアのバージョンを確認します。

MetroCluster 構成では、ローカル クラスタ スイッチに対してのみヘルス モニタリングを構成します。

BroadcomおよびCiscoスイッチでログ収集を行う場合、ログ収集が有効になっているクラスタごとに、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。MetroCluster構成では、MetroCluster 1、MetroCluster 2 、MetroCluster 3、およびMetroCluster 4のそれぞれについて、スイッチ上に個別のユーザーを設定する必要があります。これらのスイッチは、同じユーザに対して複数の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、そのユーザの既存のSSHキーが上書きされます。

CSHM を設定する前に、不要な ISL アラートを回避するために、使用されていない ISL を無効にする必要があります。

MetroCluster IPスイッチの健全性を監視するためにSNMPv3を構成する

MetroCluster IP構成では、IPスイッチのヘルスを監視するようにSNMPv3を設定できます。

この手順は、スイッチ上で SNMPv3 を構成するための一般的な手順を示しています。記載されているスイッチファームウェアバージョンの一部は、MetroCluster IP構成ではサポートされない可能性があります。

MetroCluster IP構成でサポートされているスイッチファームウェアバージョンに応じた手順に従う必要があります。 "Hardware Universe"サポートされているファームウェアのバージョンを確認します。

- 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障害発生時にスイッチファンと電源の誤検知アラートを通知"

このタスクについて

Broadcom 、**Cisco** *、および NVIDIA *スイッチでSNMPv3ユーザ名を設定するには、次のコマンドを使用します。

Broadcomスイッチ

Broadcom BES-53248スイッチでSNMPv3ユーザ名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暗号化を使用した* 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でSNMPv3ユーザ名を確立します。

```
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ようにスイッチのSNMPv3ユーザを設定します。

```
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ユーザをセットアップします。

```
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ユーザで監視するようにCSHMを設定します。

```
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暗号化を使用した* 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でSNMPv3ユーザ名を確立します。

```
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ようにスイッチのSNMPv3ユーザを設定します。

```
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ユーザをセットアップします。

```
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ユーザで監視するようにCSHMを設定します。

```
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. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で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暗号化を使用した* 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でSNMPv3ユーザ名を確立します。

```
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ようにスイッチのSNMPv3ユーザを設定します。

```
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ユーザをセットアップします。

```
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ユーザで監視するようにCSHMを設定します。

```
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. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で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暗号化を使用した* 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でSNMPv3ユーザ名を確立します。

```
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ようにスイッチのSNMPv3ユーザを設定します。

```
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ユーザをセットアップします。

```
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ユーザで監視するようにCSHMを設定します。

```
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. 新しく作成したSNMPv3ユーザで照会するシリアル番号が、CSHMポーリング期間の完了後に前の手順で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
```

MetroCluster IPスイッチでログ収集を構成する

MetroCluster IP 構成では、デバッグの目的でスイッチ ログを収集するようにログ収集を設定できます。

BroadcomおよびCiscoスイッチでは、ログ収集を行うクラスタごとに新しいユーザーが必要です。例えば、MetroCluster 1、MetroCluster 2、MetroCluster 3、MetroCluster 4のそれぞれについて、スイッチ上で個別のユーザーを設定する必要があります。同一ユーザーに対して複数のSSHキーを設定することはサポートされていません。

このタスクについて

イーサネットスイッチヘルスモニタ（CSHM）は、クラスタネットワークスイッチと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、デバッグ用にスイッチのログを収集します。この手順では、収集を設定し、詳細な*サポート*ログを要求し、AutoSupportによって収集される*定期的*データの1時間ごとの収集を有効にするプロセスをガイドします。

注： FIPSモードを有効にする場合は、次の手順を実行する必要があります。

1. ベンダーの指示に従って、スイッチでSSHキーを再生成します。
2. を使用したONTAPでのSSHキーの再生成 `debug system regenerate-systemshell-key-pair`
3. `system switch ethernet log setup-password`コマンドを使用してログ収集セットアップルーチンを再実行します。

作業を開始する前に

- ユーザはスイッチコマンドにアクセスできる必要があります `show` 。これらが使用できない場合は、新しいユーザを作成し、必要な権限をユーザに付与します。
- スイッチのヘルスモニタが有効になっている必要があります。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スイッチを使用したログ収集の場合：
  - 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。
  - ログ収集を有効にして、クラスタセットアップごとにスイッチに新しいユーザ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、そのユーザの既存のSSHキーが上書きされます。
- NVIDIAスイッチを使用したログ収集をサポートするには、 `cl-support`パスワードを入力せずにコマンドを実行できる_user_forログ収集を許可する必要があります。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。 [作業を開始する前に] 。

```
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. サポートログ収集のリクエスト：

```
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. イネーブルメント、ステータスメッセージ、前回のタイムスタンプと定期収集のファイル名、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サポート収集のファイル名など、ログ収集のすべての詳細を表示するには、次のコマンドを使用します。

```
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、ユーザ名、およびパスワードの入力を求められます。

   *注：*ユーザー指定プロンプトに応答する場合は `y`、で説明されているように、ユーザーに必要な権限があることを確認してください[作業を開始する前に]。

   ```
   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、詳細なログと1時間ごとのデータ収集の両方のタイプのログ収集が開始されます。 `Support 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.
```

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（の出力に表示され `system switch ethernet log show`ます）、詳細については、を参照してください "ログ収集のトラブルシューティング" 。

MetroCluster IP構成における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構成ファイル（RCF）では、特にCisco検出プロトコル（CDP）やリンク層検出プロトコル（LLDP）が有効になります。ただし、検出されなかった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しなければならない場合があります。また、メンテナンス中など、スイッチを構成内に残したまま、アクティブな監視を停止することもできます。

ONTAPで監視できるようにスイッチエントリを作成します。

このタスクについて

指定したイーサネットスイッチの監視を手動で設定してイネーブルにするには、コマンドを使用し `system switch ethernet create`ます。これは、ONTAPでスイッチが自動的に追加されない場合、または以前にスイッチを削除してから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、IPアドレスが1.2.3.4、SNMPv2cクレデンシャルが*cshm1!*に設定された[DeviceName]という名前のスイッチを追加します。ストレージスイッチを設定する場合は、の代わりにを `-type cluster-network`使用し `-type storage-network`ます。

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、今後の監視用に残しておく場合は、パラメータを削除するのではなく変更します `is-monitoring-enabled-admim`。

例：

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

これにより、新しいアラートを生成したり再検出したりすることなく、スイッチの詳細と設定を保持できます。

不要になったスイッチを削除

切断されたスイッチまたは不要になったスイッチを削除する場合に使用し `system switch ethernet delete`ます。

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

デフォルトでは、このコマンドが成功するのは、ONTAPがCDPまたはLLDPを介して現在スイッチを検出していない場合だけです。検出されたスイッチを削除するには、パラメータを使用し `-force`ます。

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

を使用している場合、 `-force`ONTAPがスイッチを再度検出すると、スイッチが自動的に再追加されることがあります。

MetroCluster IP構成における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（CSHM）は、検出したスイッチの監視を自動的に試みます。ただし、スイッチが正しく設定されていないと、監視が自動的に行われないことがあります。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。

接続されているイーサネットスイッチの監視を確認する

このタスクについて

接続された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
```

列に「* other 」と表示されているか、 **`IS Monitored`** フィールドに「 **false** 」と表示されている場合 **`Model`** 、 **ONTAP** はスイッチを監視できません。通常、値 other *は、ONTAPがヘルスモニタでそのスイッチをサポートしていないことを示します。

`IS Monitored`フィールドに指定された理由により、フィールドは`* false *`に設定されます`Reason`。

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によって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。。 "イーサネットスイッチの監視を管理します。"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する

スイッチがサポートされている最新のファームウェアを実行しており、互換性があるリファレンス構成ファイル（RCF）が適用されていることを確認してください。詳細については、を参照してhttps://mysupport.netapp.com/site/downloads["ネットアップサポートのダウンロードページ"^]ください。

デフォルトでは、ヘルスモニタはコミュニティストリング* cshm1！*を含むSNMPv2cを監視に使用しますが、SNMPv3も設定できます。

デフォルトのSNMPv2cコミュニティストリングを変更する必要がある場合は、スイッチに適切なSNMPv2cコミュニティストリングが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!
```

SNMPv3を使用するための設定の詳細については、を参照してください"オプション：SNMPv3を設定する"。

管理ネットワーク接続の確認

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ことを確認します。

ONTAPでSNMPクエリとログ収集を実行するには、適切な管理ポート接続が必要です。

関連情報

- "アラートのトラブルシューティング"

著作権に関する情報

商標に関する情報