



監控 **MetroCluster IP** 交換器的運作狀況

ONTAP MetroCluster

NetApp
February 13, 2026

目錄

監控 MetroCluster IP 交換器的運作狀況	1
了解 MetroCluster IP 設定中的交換器運作狀況監控	1
在 MetroCluster IP 設定中設定 CSHM 的重要注意事項	1
設定 SNMPv3 來監控 MetroCluster IP 交換器的運作狀況	1
在 MetroCluster IP 交換器上設定日誌收集	18
開始之前	19
步驟	19
管理 MetroCluster IP 設定中的乙太網路交換器監控	25
建立交換器項目，讓 ONTAP 能夠監控	25
停用監控，但不刪除交換器	26
移除不再需要的交換器	26
驗證 MetroCluster IP 設定中的乙太網路交換器監控	26
確認監控連接的乙太網路交換器	26
確認韌體和 RCF 版本為最新版本	27
確認管理網路連線	27

監控 MetroCluster IP 交換器的運作狀況

了解 MetroCluster IP 設定中的交換器運作狀況監控

乙太網路交換器健全狀況監視器（CSHM）負責確保叢集與儲存網路交換器的作業健全狀況、並收集交換器記錄以供偵錯之用。

在 MetroCluster IP 設定中設定 CSHM 的重要注意事項

本節包含在 Cisco、Broadcom 和 NVIDIA SN2100 交換器上設定 SNMPv3 和日誌收集的通用步驟。您必須按照 MetroCluster IP 設定中支援的交換器韌體版本的步驟進行操作。請參閱["Hardware Universe"](#)驗證支援的韌體版本。

在 MetroCluster 設定中，僅在本機叢集交換器上設定運作狀況監控。

對於使用 Broadcom 和 Cisco 交換器進行日誌收集，應在交換器上為每個啟用日誌收集的叢集建立一個新使用者。在 MetroCluster 配置中，這表示 MetroCluster 1、MetroCluster 2、MetroCluster 3 和 MetroCluster 4 都需要在交換器上設定單獨的使用者。這些交換器不支援同一位使用者的多個 SSH 金鑰。執行的任何其他記錄集合設定都會覆寫使用者先前存在的任何 SSH 金鑰。

在配置 CSHM 之前，您應該停用未使用的 ISL 以避免任何不必要的 ISL 警報。

設定 SNMPv3 來監控 MetroCluster IP 交換器的運作狀況

在 MetroCluster IP 組態中、您可以設定 SNMPv3 來監控 IP 交換器的健全狀況。

此程序顯示在交換器上設定 SNMPv3 的通用步驟。列出的某些交換器韌體版本可能不受 MetroCluster IP 配置支援。

您必須按照 MetroCluster IP 設定中支援的交換器韌體版本的步驟進行操作。請參閱["Hardware Universe"](#)驗證支援的韌體版本。

- 僅 ONTAP 9.12.1 及更新版本支援 SNMPv3 。
- ONTAP 9.13.1P12、9.14.1P9、9.15.1P5、9.16.1 及更高版本修正了以下兩個問題：
 - "對於 Cisco 交換器的 ONTAP 運作狀況監控，切換到 SNMPv3 進行監控後仍可能看到 SNMPv2 流量"
 - "SNMP 故障發生時誤報交換器風扇及電源警報"



關於這項工作

以下命令用於在 **Broadcom**、**Cisco** 和 ***NVidia** 交換機上配置 SNMPv3 用戶名：

Broadcom 交換器

在 Broadcom BS-53248 交換器上設定 SNMPv3 使用者名稱網路操作員。

- 若為 *無驗證*：

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

- 對於 *MD5/SHA 驗證*：

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

- 對於採用 AES/DES 加密的 *MD5/SHA 驗證*：

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

下列命令可在 ONTAP 端設定 SNMPv3 使用者名稱：

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

下列命令會使用 CSHM 建立 SNMPv3 使用者名稱：

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

步驟

1. 設定交換器上的v3使用者使用驗證和加密：

```
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 Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

2. 設定位在邊上的v3使用者ONTAP :

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. 設定 CSHM 以監控新的 SNMPv3 使用者 :

```
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: cshml!
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 輪詢期後，驗證乙太網路交換器的序號是否已填入。

```
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 交換器

在 Cisco 9336C-FX2 交換器上設定 SNMPv3 使用者名稱 SNMPv3 使用者：

- 若為 *無驗證*：

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

- 對於 *MD5/SHA 驗證*：

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

- 對於採用 AES/DES 加密的 *MD5/SHA 驗證*：

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

下列命令可在 ONTAP 端設定 SNMPv3 使用者名稱：

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

下列命令會使用 CSHM 建立 SNMPv3 使用者名稱：

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

步驟

1. 設定交換器上的v3使用者使用驗證和加密：

```
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. 設定位在邊上的v3使用者ONTAP :

```
security login create -user-or-group-name <username> -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1  
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true
```

```
cluster1::*> security login create -user-or-group-name <username>  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. 設定 CSHM 以監控新的 SNMPv3 使用者 :

```
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: cshml!
                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. 驗證要與新建立的 SNMPv3 使用者查詢的序號、是否與 CSHM 輪詢期間結束後上一步所述相同。

```

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

在執行 CLI 5.4.0 的 NVIDIA SN2100 交換器上設定 SNMPv3 使用者名稱 SNMPv3_USER :

- 若為 *無驗證* :

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

- 對於 *MD5/SHA 驗證* :

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

- 對於採用 AES/DES 加密的 *MD5/SHA 驗證* :

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

下列命令可在 ONTAP 端設定 SNMPv3 使用者名稱：

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

下列命令會使用 CSHM 建立 SNMPv3 使用者名稱：

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

步驟

1. 設定交換器上的v3使用者使用驗證和加密：

```
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 laErrorMessage "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 cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syssservices 72
-rocommunity cshml! 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. 設定位在邊上的v3使用者ONTAP :

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. 設定 CSHM 以監控新的 SNMPv3 使用者 :

```
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: cshml!
                                     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. 驗證要與新建立的 SNMPv3 使用者查詢的序號、是否與 CSHM 輪詢期間結束後上一步所述相同。

```
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
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

在執行 CLI 5.11.0 的 NVIDIA SN2100 交換器上設定 SNMPv3 使用者名稱 SNMPv3_USER :

- 若為 *無驗證* :

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

- 對於 *MD5/SHA 驗證* :

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

- 對於採用 AES/DES 加密的 *MD5/SHA 驗證* :

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

下列命令可在 ONTAP 端設定 SNMPv3 使用者名稱：

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

下列命令會使用 CSHM 建立 SNMPv3 使用者名稱：

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

步驟

1. 設定交換器上的v3使用者使用驗證和加密：

```
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. 設定位在邊上的v3使用者ONTAP：

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. 設定 CSHM 以監控新的 SNMPv3 使用者：

```
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: cshml!
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. 驗證要與新建立的 SNMPv3 使用者查詢的序號、是否與 CSHM 輪詢期間結束後上一步所述相同。

```
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
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 交換器上設定日誌收集

在 MetroCluster IP 設定中，您可以設定日誌收集以收集交換器日誌以用於偵錯目的。



在 Broadcom 和 Cisco 交換器上，每個具有日誌收集功能的叢集都需要一個新使用者。例如，MetroCluster 1、MetroCluster 2、MetroCluster 3 和 MetroCluster 4 都需要在交換器上設定單獨的使用者。不支援同一用戶使用多個 SSH 金鑰。

關於這項工作

乙太網路交換器健全狀況監視器（CSHM）負責確保叢集與儲存網路交換器的作業健全狀況、並收集交換器記錄以供偵錯之用。本程序將引導您完成設定收集、要求詳細的 * 支援 * 記錄、以及啟用 AutoSupport 所收集 * 定期 * 資料的每小時收集。

- 注意：* 如果您啟用 FIPS 模式、則必須完成下列步驟：



1. 使用廠商指示在交換器上重新產生 SSH 金鑰。
2. 使用在 ONTAP 中重新產生 SSH 金鑰 `debug system regenerate-systemshell-key-pair`
3. 使用 `'system switch ethernet log setup-password'` 命令重新執行記錄收集設定例程序

開始之前

- 使用者必須能夠存取交換器 `show` 命令。如果這些權限不可用、請建立新使用者、並將必要的權限授予使用者。
- 必須為交換器啟用交換器健全狀況監控。透過確保 `Is Monitored:` 字段在輸出中設定為 `true` `system switch ethernet show` 命令。
- 對於 Broadcom 和 Cisco 交換器的記錄收集：
 - 本機使用者必須具有網路管理員權限。
 - 應在交換器上為啟用記錄收集的每個叢集設定建立新使用者。這些交換器不支援同一位使用者的多個 SSH 金鑰。執行的任何其他記錄集合設定都會覆寫使用者先前存在的任何 SSH 金鑰。
- 若要使用 NVIDIA 交換器來支援記錄收集、必須允許記錄收集的 `user` 執行 `cl-support` 命令、而無需提供密碼。若要允許這種使用方式、請執行命令：

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

步驟

ONTAP 9.15.1 及更新版本

1. 若要設定記錄收集、請針對每個交換器執行下列命令。系統會提示您輸入用於記錄收集的交換器名稱、使用者名稱和密碼。

注意：*如果對使用者規範提示回答 **y**，請確保使用者俱有必要的權限，如[\[開始之前\]](#)。

```
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>
```



對於 CL 5.11.1，建立使用者 **cumulus** 並對以下提示回答 **y**：您要指定管理員以外的使用者進行日誌收集嗎？{y|n}：**y**

1. 啟用定期日誌收集：

```
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. 要求支援記錄收集：

```
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. 若要檢視記錄收集的所有詳細資料、包括啟用、狀態訊息、定期收集的先前時間戳記和檔名、要求狀態、狀態訊息、以及支援集合的先前時間戳記和檔名、請使用下列項目：

```
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. 若要設定記錄收集、請針對每個交換器執行下列命令。系統會提示您輸入用於記錄收集的交換器名稱、使用者名稱和密碼。
 - 注意：* 如果回答 `y` 使用者規格提示，請確定使用者擁有中所述的必要權限[\[開始之前\]](#)。

```
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>
```



對於 CL 5.11.1，建立使用者 **cumulus** 並對以下提示回答 **y**：您要指定管理員以外的使用者進行日誌收集嗎？{y|n}：**y**

1. 若要要求支援日誌收集並啟用定期收集，請執行下列命令。這會同時啟動記錄收集的兩種類型：詳細 Support 記錄和每小時收集 Periodic 的資料。

```
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 分鐘、然後檢查記錄收集是否完成：

```
system switch ethernet log show
```



如果記錄收集功能報告任何錯誤狀態（在的輸出中可見 `system switch ethernet log show`）、請參閱 ["疑難排解記錄收集"](#) 以取得進一步詳細資料。

管理 MetroCluster IP 設定中的乙太網路交換器監控

在大多數情況下，ONTAP 會自動探索乙太網路交換器，並由 CSHM 監控。套用至交換器的參考組態檔（RCF），除其他外，可啟用 Cisco 探索傳輸協定（CDP）和 / 或連結層探索傳輸協定（LLDP）。不過，您可能需要手動新增未發現的交換器，或移除不再使用的交換器。您也可以停止主動監控，同時將交換器保留在組態中，例如在維護期間。

建立交換器項目，讓 ONTAP 能夠監控

關於這項工作

使用 `system switch ethernet create` 命令手動設定及啟用指定乙太網路交換器的監控。如果 ONTAP 未自動新增交換器，或您先前已移除交換器並想要重新新增交換器，這項功能就很實用。

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

典型的例子是新增一個名為 [DeviceName] 的交換器，IP 位址為 1.2.3.4，而 SNMPv2c 認證設定為 **cshm1!**。

如果您正在設定儲存交換器，請改 `-type cluster-network`用`-type storage-network`。`

停用監控，但不刪除交換器

如果您想要暫停或停止監控某個交換器，但仍保留它以供未來監控，請修改其 ``is-monitoring-enabled-admin`` 參數而非刪除它。

例如：

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

這可讓您保留交換器的詳細資料和組態，而無需產生新警示或重新探索。

移除不再需要的交換器

用於 ``system switch ethernet delete`` 刪除已中斷連線或不再需要的交換器：

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

根據預設，只有在 ONTAP 目前未透過 CDP 或 LLDP 偵測到交換器時，此命令才會成功。若要移除探索到的交換器，請使用 ``-force`` 參數：

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

``-force`` 使用時，如果 ONTAP 再次偵測到交換器，可能會自動重新新增交換器。

驗證 MetroCluster IP 設定中的乙太網路交換器監控

乙太網路交換器健全狀況監視器（CSHM）會自動嘗試監控其探索到的交換器；不過，如果交換器未正確設定，則可能不會自動進行監控。您應該確認健全狀況監視器已正確設定、以監控交換器。

確認監控連接的乙太網路交換器

關於這項工作

若要確認正在監控連接的乙太網路交換器，請執行：

```
system switch ethernet show
```

如果 Model 欄顯示 * 其他 *，或欄位顯示 * 錯誤 * ``IS Monitored``，則 ONTAP 無法監控交換器。值

* 其他 * 通常表示 ONTAP 不支援該交換器進行健全狀況監控。

此 IS Monitored 欄位會因欄位中指定的理由而設為 * 錯誤 * Reason。



如果命令輸出中未列出交換機，則ONTAP可能尚未發現它。確認交換器的接線正確。如果需要，您可以手動新增交換器。請參閱["管理乙太網路交換器的監控"](#)了解更多詳情。

確認韌體和 RCF 版本為最新版本

請確定交換器執行的是最新支援的韌體，而且已套用相容的參考組態檔案（RCF）。如需詳細資訊[https://mysupport.netapp.com/site/downloads\["NetApp支援下載頁面"\]](https://mysupport.netapp.com/site/downloads[)、請參閱。

根據預設，健全狀況監視器會使用 SNMPv2c 搭配社群字串 **csbm1!** 進行監控，但也可以設定 SNMPv3。

如果您需要變更預設的 SNMPv2c 社群字串，請確定交換器上已設定所需的 SNMPv2c 社群字串。

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



如需設定要使用的 SNMPv3 的詳細資訊，請參閱["選用：設定 SNMPv3"](#)。

確認管理網路連線

確認交換器的管理連接埠已連線至管理網路。

ONTAP 執行 SNMP 查詢和記錄收集時，需要正確的管理連接埠連線。

相關資訊

- ["疑難排解警示"](#)

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。