



스위치 상태 모니터링

Install and maintain

NetApp
February 13, 2026

목차

스위치 상태 모니터링	1
스위치 상태 모니터 개요	1
스위치 상태 모니터링 구성	1
구성 개요	1
로그 수집 구성	1
스위치에 SNMPv3 구성(선택 사항)	8
스위치 상태 확인	26
건강 검진 개요	26
이더넷 스위치 모니터링 관리	26
이더넷 스위치 모니터링 확인	27
알림 문제 해결	28
로그 수집	29
로그 수집 개요	29
로그 수집 문제 해결	29

스위치 상태 모니터링

스위치 상태 모니터 개요

이더넷 스위치 상태 모니터(CSHM)는 클러스터 및 스토리지 네트워크 스위치의 작동 상태를 보장하고 디버깅 목적으로 스위치 로그를 수집하는 역할을 합니다.

스위치 상태 모니터링 구성

구성 개요

이더넷 스위치 상태 모니터(CSHM)는 클러스터 및 스토리지 네트워크 스위치의 작동 상태를 보장하고 디버깅 목적으로 스위치 로그를 수집하는 역할을 합니다.

- "로그 수집 구성"
- "SNMPv3 구성(선택 사항)"

로그 수집 구성

이더넷 스위치 상태 모니터(CSHM)는 클러스터 및 스토리지 네트워크 스위치의 작동 상태를 보장하고 디버깅 목적으로 스위치 로그를 수집하는 역할을 합니다. 이 절차에서는 AutoSupport 에서 수집하는 주기적 데이터의 매시간 수집을 활성화하고, 자세한 지원 로그를 요청하고, 수집을 설정하는 과정을 안내합니다.

참고: FIPS 모드를 활성화하는 경우 다음을 완료해야 합니다.



1. 공급업체의 지침을 사용하여 스위치에서 SSH 키를 다시 생성합니다.
2. ONTAP 에서 SSH 키를 재생성하려면 다음을 사용하세요. `debug system regenerate-systemshell-key-pair`
3. 다음을 사용하여 로그 수집 설정 루틴을 다시 실행하세요. `system switch ethernet log setup-password` 명령

시작하기 전에

- 사용자는 스위치에 액세스할 수 있어야 합니다. `show` 명령. 이러한 권한이 없는 경우 새 사용자를 만들고 해당 사용자에게 필요한 권한을 부여하세요.
- 스위치에 대해 스위치 상태 모니터링을 활성화해야 합니다. 이를 확인하려면 다음을 확인하세요. `Is Monitored:` 필드는 출력에서 `*true*`로 설정됩니다. `system switch ethernet show` 명령.
- Broadcom 및 Cisco 스위치를 사용한 로그 수집:
 - 로컬 사용자는 네트워크 관리자 권한이 있어야 합니다.
 - 로그 수집이 활성화된 각 클러스터 설정에 대해 스위치에 새 사용자를 만들어야 합니다. 이러한 스위치는 동일한 사용자에게 대해 여러 개의 SSH 키를 지원하지 않습니다. 추가 로그 수집 설정을 수행하면 해당 사용자의 기존 SSH 키가 덮어쓰여집니다.

- NVIDIA 스위치로 로그 수집을 지원하려면 로그 수집을 위한 `_user_`가 다음을 실행할 수 있어야 합니다. `cl-support` 비밀번호를 제공하지 않고도 명령을 실행할 수 있습니다. 이러한 사용을 허용하려면 다음 명령을 실행하세요.

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

단계

ONTAP 9.15.1 이상

1. 로그 수집을 설정하려면 각 스위치에 대해 다음 명령을 실행합니다. 로그 수집을 위해 스위치 이름, 사용자 이름, 비밀번호를 입력하라는 메시지가 표시됩니다.

참고: 사용자 지정 프롬프트에 *y*로 응답하는 경우 사용자에게 다음에 설명된 대로 필요한 권한이 있는지 확인하십시오. [시작하기 전에](#).

```
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 5.11.1의 경우, 사용자 **cumulus***를 생성하고 다음 프롬프트에 *y*로 응답합니다. 로그 수집에 **admin**이 아닌 다른 사용자를 지정하시겠습니까? {y|n}: *y

1. 주기적 로그 수집 활성화:

```
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. 지원 로그 수집 요청:

```
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.

- 로그 수집의 모든 세부 정보(활성화, 상태 메시지, 이전 타임스탬프 및 주기적 수집 파일 이름, 요청 상태, 상태 메시지, 지원 수집의 이전 타임스탬프 및 파일 이름 포함)를 보려면 다음을 사용하세요.

```
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 및 이전 버전

1. 로그 수집을 설정하려면 각 스위치에 대해 다음 명령을 실행합니다. 로그 수집을 위해 스위치 이름, 사용자 이름, 비밀번호를 입력하라는 메시지가 표시됩니다.

참고: 답변하는 경우 y 사용자 사양 프롬프트에 따라 사용자에게 다음에 설명된 대로 필요한 권한이 있는지 확인하십시오.[시작하기 전에](#).

```
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 5.11.1의 경우, 사용자 **cumulus***를 생성하고 다음 프롬프트에 ***y***로 응답합니다. 로그 수집에 **admin**이 아닌 다른 사용자를 지정하시겠습니까? {y|n}: ***y**

1. 지원 로그 수집을 요청하고 주기적 수집을 활성화하려면 다음 명령을 실행하세요. 이렇게 하면 두 가지 유형의 로그 수집이 시작됩니다. 자세한 내용 Support 로그 및 시간별 수집 Periodic 데이터.

```
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.
```

10분간 기다린 후 로그 수집이 완료되었는지 확인하세요.

```
system switch ethernet log show
```



로그 수집 기능에서 오류 상태가 보고되는 경우(출력에서 확인 가능) `system switch ethernet log show`), 보다 "[로그 수집 문제 해결](#)" 자세한 내용은.

다음은 무엇인가요?

["SNMPv3 구성\(선택 사항\)"](#).

스위치에 **SNMPv3** 구성(선택 사항)

SNMP는 스위치를 모니터링하는 데 사용됩니다. SNMPv3에 의한 모니터링은 다음 절차에 따라 구성됩니다.

이더넷 스위치 상태 모니터(CSHM)는 SNMP를 활용하여 클러스터 및 스토리지 스위치의 상태와 성능을 모니터링합니다. 기본적으로 SNMPv2c는 참조 구성 파일(RCF)을 통해 자동으로 구성됩니다. SNMPv3는 인증, 암호화, 메시지 무결성과 같은 강력한 보안 기능을 도입하여 무단 접근을 방지하고 전송 중 데이터의 기밀성과 무결성을 보장하므로 SNMPv2보다 보안성이 더 높습니다.



- SNMPv3는 ONTAP 9.12.1 이상에서만 지원됩니다.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 및 이후 버전은 다음 두 가지 문제를 해결합니다.
 - "[Cisco 스위치의 ONTAP 상태 모니터링의 경우 모니터링을 위해 SNMPv3으로 전환한 후에도 SNMPv2 트래픽이 계속 표시될 수 있습니다.](#)"
 - "["SNMP 실패 발생 시 거짓 양성 스위치 팬 및 전원 경고"](#)

이 작업에 관하여

다음 명령은 **Broadcom**, * Cisco*, * NVIDIA* 스위치에서 SNMPv3 사용자 이름을 구성하는 데 사용됩니다.

브로드컴 스위치

Broadcom BES-53248 스위치에서 SNMPv3 사용자 이름 NETWORK-OPERATOR를 구성합니다.

- *인증 없음*의 경우:

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

- *MD5/SHA 인증*의 경우:

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

- *AES/DES 암호화를 사용한 MD5/SHA 인증*의 경우:

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

다음 명령은 ONTAP 측에서 SNMPv3 사용자 이름을 구성합니다.

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

다음 명령은 CSHM을 사용하여 SNMPv3 사용자 이름을 설정합니다.

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

단계

1. 스위치에서 SNMPv3 사용자를 설정하여 인증 및 암호화를 사용합니다.

```
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. ONTAP 측에서 SNMPv3 사용자를 설정합니다.

```
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. 새로운 SNMPv3 사용자로 모니터링하도록 CSHM을 구성합니다.

```
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. CSHM 폴링 기간을 기다린 후 이더넷 스위치의 일련 번호가 채워졌는지 확인하세요.

```
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 스위치

Cisco 9336C-FX2 스위치에서 SNMPv3 사용자 이름 SNMPv3_USER를 구성합니다.

- *인증 없음*의 경우:

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

- *MD5/SHA 인증*의 경우:

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

- *AES/DES 암호화를 사용한 MD5/SHA 인증*의 경우:

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

다음 명령은 ONTAP 측에서 SNMPv3 사용자 이름을 구성합니다.

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

다음 명령은 CSHM을 사용하여 SNMPv3 사용자 이름을 설정합니다.

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

단계

1. 스위치에서 SNMPv3 사용자를 설정하여 인증 및 암호화를 사용합니다.

```
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 측에서 SNMPv3 사용자를 설정합니다.

```
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. 새로운 SNMPv3 사용자로 모니터링하도록 CSHM을 구성합니다.

```
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. CSHM 폴링 기간이 완료된 후 새로 생성된 SNMPv3 사용자에게 쿼리할 일련 번호가 이전 단계에서 자세히 설명한 것과 동일한지 확인합니다.

```

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 5.4.0을 실행하는 NVIDIA SN2100 스위치에서 SNMPv3 사용자 이름 SNMPv3_USER를 구성합니다.

- *인증 없음*의 경우:

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

- *MD5/SHA 인증*의 경우:

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

- *AES/DES 암호화를 사용한 MD5/SHA 인증*의 경우:

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

다음 명령은 ONTAP 측에서 SNMPv3 사용자 이름을 구성합니다.

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

다음 명령은 CSHM을 사용하여 SNMPv3 사용자 이름을 설정합니다.

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

단계

1. 스위치에서 SNMPv3 사용자를 설정하여 인증 및 암호화를 사용합니다.

```
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. ONTAP 측에서 SNMPv3 사용자를 설정합니다.

```
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. 새로운 SNMPv3 사용자로 모니터링하도록 CSHM을 구성합니다.

```
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. CSHM 폴링 기간이 완료된 후 새로 생성된 SNMPv3 사용자에게 쿼리할 일련 번호가 이전 단계에서 자세히 설명한 것과 동일한지 확인합니다.

```
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

CLI 5.11.0을 실행하는 NVIDIA SN2100 스위치에서 SNMPv3 사용자 이름 SNMPv3_USER를 구성합니다.

- *인증 없음*의 경우:

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

- *MD5/SHA 인증*의 경우:

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

- *AES/DES 암호화를 사용한 MD5/SHA 인증*의 경우:

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

다음 명령은 ONTAP 측에서 SNMPv3 사용자 이름을 구성합니다.

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

다음 명령은 CSHM을 사용하여 SNMPv3 사용자 이름을 설정합니다.

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

단계

1. 스위치에서 SNMPv3 사용자를 설정하여 인증 및 암호화를 사용합니다.

```
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 측에서 SNMPv3 사용자를 설정합니다.

```
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. 새로운 SNMPv3 사용자로 모니터링하도록 CSHM을 구성합니다.

```
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. CSHM 폴링 기간이 완료된 후 새로 생성된 SNMPv3 사용자에게 쿼리할 일련 번호가 이전 단계에서 자세히 설명한 것과 동일한지 확인합니다.

```
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

```

스위치 상태 확인

건강 검진 개요

상태 모니터는 클러스터의 특정한 중요 상태를 사전에 모니터링하고 오류나 위험을 감지하면 경고를 발생시킵니다.

현재 발생한 이더넷 스위치 상태 모니터 알림을 보려면 다음 명령을 실행하세요. `system health alert show -monitor ethernet-switch`

사용 가능한 이더넷 스위치 상태 모니터 알림을 보려면 다음 명령을 실행하세요. `system health alert definition show -monitor ethernet-switch`

이더넷 스위치 모니터링 관리

대부분의 경우 이더넷 스위치는 ONTAP 에서 자동으로 검색되고 CSHM에서 모니터링됩니다. 스위치에 적용된 RCF(참조 구성 파일)는 무엇보다도 Cisco Discovery Protocol(CDP) 및/또는 Link Layer Discovery Protocol(LLDP)을 활성화합니다. 하지만 검색되지 않은 스위치를 수동으로 추가하거나 더 이상 사용하지 않는 스위치를 제거해야 할 수도 있습니다. 유지 관리

등의 목적으로 스위치를 구성 상태로 유지하면서 활성 모니터링을 중지할 수도 있습니다.

ONTAP 모니터링할 수 있도록 스위치 항목을 만듭니다.

사용하다 `system switch ethernet create` 지정된 이더넷 스위치에 대한 모니터링을 수동으로 구성하고 활성화하는 명령입니다. ONTAP 스위치를 자동으로 추가하지 않거나, 이전에 스위치를 제거했다가 다시 추가하려는 경우 이 기능이 유용합니다.

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

일반적인 예로는 IP 주소가 1.2.3.4이고 SNMPv2c 자격 증명이 *cshml!*로 설정된 [DeviceName]이라는 스위치를 추가하는 것입니다. 사용 `-type storage-network` 대신에 `-type cluster-network` 스토리지 스위치를 구성하는 경우.

스위치를 삭제하지 않고 모니터링을 비활성화합니다.

특정 스위치에 대한 모니터링을 일시 중지하거나 중지하지만 향후 모니터링을 위해 계속 유지하려는 경우 해당 스위치를 수정하십시오. `is-monitoring-enabled-admin` 삭제하는 대신 매개변수를 삭제하세요.

예를 들어:

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

이를 통해 새로운 알림이나 재검색을 생성하지 않고도 스위치 세부 정보와 구성을 보존할 수 있습니다.

더 이상 필요하지 않은 스위치를 제거하세요

사용 `system switch ethernet delete` 연결이 끊어졌거나 더 이상 필요하지 않은 스위치를 삭제하려면:

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

기본적으로 이 명령은 ONTAP 현재 CDP 또는 LLDP를 통해 스위치를 감지하지 못하는 경우에만 성공합니다. 검색된 스위치를 제거하려면 다음을 사용하세요. `-force` 매개변수:

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

언제 `-force` 이 사용되면 ONTAP 다시 감지하면 스위치가 자동으로 다시 추가될 수 있습니다.

이더넷 스위치 모니터링 확인

이더넷 스위치 상태 모니터(CSHM)는 발견된 스위치를 자동으로 모니터링하려고 시도합니다.

그러나 스위치가 올바르게 구성되지 않은 경우 모니터링이 자동으로 이루어지지 않을 수 있습니다. 스위치를 모니터링하기 위해 상태 모니터가 올바르게 구성되었는지 확인해야 합니다.

연결된 이더넷 스위치 모니터링 확인

연결된 이더넷 스위치가 모니터링되고 있는지 확인하려면 다음을 실행하세요.

```
system switch ethernet show
```

만약 Model 열에는 **OTHER** 또는 IS Monitored 필드에 **false***가 표시되면 **ONTAP** 스위치를 모니터링할 수 없습니다. ***OTHER** 값은 일반적으로 ONTAP 해당 스위치의 상태 모니터링을 지원하지 않음을 나타냅니다.

그만큼 IS Monitored 필드는 지정된 이유로 *false*로 설정됩니다. Reason 필드.



스위치가 명령 출력에 나열되지 않으면 ONTAP 해당 스위치를 발견하지 못했을 가능성이 높습니다. 스위치 케이블이 올바르게 연결되었는지 확인하세요. 필요한 경우 스위치를 수동으로 추가할 수 있습니다. 보다"[이더넷 스위치 모니터링 관리](#)" 자세한 내용은.

펌웨어 및 RCF 버전이 최신인지 확인하세요

스위치가 최신 지원 펌웨어를 실행하고 있는지, 호환 가능한 참조 구성 파일(RCF)이 적용되었는지 확인하세요. 자세한 내용은 다음에서 확인할 수 있습니다.<https://mysupport.netapp.com/site/downloads/>"NetApp 지원 다운로드 페이지"시.

기본적으로 상태 모니터는 모니터링을 위해 커뮤니티 문자열 *cshm1!*과 함께 SNMPv2c를 사용하지만 SNMPv3도 구성할 수 있습니다.

기본 SNMPv2c 커뮤니티 문자열을 변경해야 하는 경우, 원하는 SNMPv2c 커뮤니티 문자열이 스위치에 구성되어 있는지 확인하세요.

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



보다"[선택 사항: SNMPv3 구성](#)" SNMPv3를 사용하도록 구성하는 방법에 대한 자세한 내용은 다음을 참조하세요.

관리 네트워크 연결 확인

스위치의 관리 포트가 관리 네트워크에 연결되어 있는지 확인하세요.

ONTAP SNMP 쿼리를 수행하고 로그를 수집하려면 올바른 관리 포트 연결이 필요합니다.

알림 문제 해결

클러스터의 이더넷 스위치에서 오류, 위험 또는 중요 조건이 감지되면 경고가 발생합니다.

경고가 발생하면 시스템 상태는 클러스터의 성능이 저하된 상태로 보고됩니다. 발생한 경고에는 저하된 시스템 상태에

대응하는 데 필요한 정보가 포함되어 있습니다.

사용 가능한 이더넷 스위치 상태 모니터 알림을 보려면 다음 명령을 실행하세요. `system health alert definition show -monitor ethernet-switch`

지식 기반 문서를 참조하세요 "[스위치 상태 모니터 경고 해결 가이드](#)" 알림에 대한 고급 해결 세부 정보를 확인하세요.

로그 수집

로그 수집 개요

로그 수집을 설정하면 AutoSupport 에서 수집하는 주기적 데이터의 매시간 수집을 활성화하고 자세한 지원 로그를 요청할 수 있습니다.

보다 "[로그 수집 구성](#)" 자세한 내용은.

로그 수집 문제 해결

로그 수집 기능에서 보고된 다음 오류 상태 중 하나가 발생하는 경우(출력에서 확인 가능) `system switch ethernet log show` 명령), 해당 디버그 단계를 시도하세요.

로그 수집 오류 상태	해결
RSA 키가 없습니다	ONTAP SSH 키를 다시 생성합니다.
비밀번호 변경 오류	자격 증명을 확인하고, SSH 연결을 테스트하고, ONTAP SSH 키를 다시 생성합니다. 스위치 설명서를 검토하거나 NetApp 지원팀에 문의하여 지침을 받으세요.
FIPS 에는 ECDSA 키가 없습니다	FIPS 모드가 활성화된 경우 다시 시도하기 전에 스위치에서 ECDSA 키를 생성해야 합니다.
기존 로그 발견	스위치에서 이전 로그 수집 파일을 제거합니다.
스위치 덤프 로그 오류	스위치 사용자에게 로그 수집 권한이 있는지 확인하세요. 위의 전제 조건을 참조하세요.



해결 방법이 작동하지 않으면 NetApp 지원팀에 문의하세요.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.