



## **Configure software**

### **Cluster and storage switches**

NetApp  
April 25, 2024

# Table of Contents

- Configure software ..... 1
  - Software install workflow for BES-53248 switches ..... 1
  - Install the EFOS software ..... 1
  - Install licenses for BES-53248 cluster switches..... 13
  - Install the Reference Configuration File (RCF) ..... 26
  - Enable SSH on BES-53248 cluster switches..... 56
  - Ethernet Switch Health Monitoring log collection..... 58
  - Configure SNMPv3 ..... 61

# Configure software

## Software install workflow for BES-53248 switches

To initially install and configure the software for a BES-53248 cluster switch, follow these steps:

1. [Install the EFOS software.](#)

Download and install the Ethernet Fabric OS (EFOS) software on the BES-53248 cluster switch.

2. [Install licenses for BES-53248 cluster switches.](#)

Optionally, add new ports by purchasing and installing more licenses. The switch base model is licensed for 16 10GbE or 25GbE ports and two 100GbE ports.

3. [Install the Reference Configuration File \(RCF\).](#)

Install or upgrade the RCF on the BES-53248 cluster switch, and then verify the ports for an additional license after the RCF is applied.

4. [Install the Cluster Switch Health Monitor \(CSHM\) configuration file.](#)

Install the applicable configuration file for cluster switch health monitoring.

5. [Enable SSH on BES-53248 cluster switches.](#)

If you use the Cluster Switch Health Monitor (CSHM) and log collection features, enable SSH on the switches.

6. [Enable the log collection feature.](#)

Use this feature to collect switch-related log files in ONTAP.

## Install the EFOS software

Follow these steps to install the Ethernet Fabric OS (EFOS) software on the BES-53248 cluster switch.

EFOS software includes a set of advanced networking features and protocols for developing Ethernet and IP infrastructure systems. This software architecture is suitable for any network organizational device using applications that require thorough packet inspection or separation.

### Prepare for installation

#### Before you begin

- Download the applicable Broadcom EFOS software for your cluster switches from the [Broadcom Ethernet Switch Support](#) site.
- Review the following notes regarding EFOS versions.

**Note the following:**

- When upgrading from EFOS 3.4.x.x to EFOS 3.7.x.x or later, the switch must be running EFOS 3.4.4.6 (or later 3.4.x.x release). If you are running a release prior to that, then upgrade the switch to EFOS 3.4.4.6 (or later 3.4.x.x release) first, then upgrade the switch to EFOS 3.7.x.x or later.
- The configuration for EFOS 3.4.x.x and 3.7.x.x or later are different. Changing the EFOS version from 3.4.x.x to 3.7.x.x or later, or vice versa, requires the switch to be reset to factory defaults and the RCF files for the corresponding EFOS version to be (re)applied. This procedure requires access through the serial console port.
- Beginning with EFOS version 3.7.x.x or later, a non-FIPS compliant and a FIPS compliant version is available. Different steps apply when moving from a non-FIPS compliant to a FIPS compliant version or vice versa. Changing EFOS from a non-FIPS compliant to a FIPS compliant version or vice versa will reset the switch to factory defaults. This procedure requires access through the serial console port.

Procedure	Current EFOS version	New EFOS version	High level steps
Steps to upgrade EFOS between two (non) FIPS compliant versions	3.4.x.x	3.4.x.x	Install the new EFOS image using <a href="#">Method 1: Install EFOS</a> . The configuration and license information is retained.
	3.4.4.6 (or later 3.4.x.x)	3.7.x.x or later non-FIPS compliant	Upgrade EFOS using <a href="#">Method 1: Install EFOS</a> . Reset the switch to factory defaults and apply the RCF file for EFOS 3.7.x.x or later.
	3.7.x.x or later non-FIPS compliant	3.4.4.6 (or later 3.4.x.x)	Downgrade EFOS using <a href="#">Method 1: Install EFOS</a> . Reset the switch to factory defaults and apply the RCF file for EFOS 3.4.x.x
		3.7.x.x or later non-FIPS compliant	Install the new EFOS image using <a href="#">Method 1: Install EFOS</a> . The configuration and license information is retained.
	3.7.x.x or later FIPS compliant	3.7.x.x or later FIPS compliant	Install the new EFOS image using <a href="#">Method 1: Install EFOS</a> . The configuration and license information is retained.

Steps to upgrade to/from a FIPS compliant EFOS version	Non-FIPS compliant	FIPS compliant	Installation of the EFOS image using <a href="#">Method 2: Upgrade EFOS using the ONIE OS installation</a> . The switch configuration and license information will be lost.
	FIPS compliant	Non-FIPS compliant	

To check if your version of EFOS is FIPS compliant or non-FIPS compliant, use the `show fips status` command. In the following examples, **IP\_switch\_a1** is using FIPS compliant EFOS and **IP\_switch\_a2** is using non-FIPS compliant EFOS.

- On switch IP\_switch\_a1:

```
IP_switch_a1 # *show fips status*
```

```
System running in FIPS mode
```

- On switch IP\_switch\_a2:

```
IP_switch_a2 # *show fips status*
```

```
                ^
% Invalid input detected at ``^` marker.
```

## Install the software

Use one of the following methods:

- [Method 1: Install EFOS](#). Use for most cases (see the table above).
- [Method 2: Upgrade EFOS using the ONIE OS installation](#). Use if one EFOS version is FIPS compliant and the other EFOS version is non-FIPS compliant.

### Method 1: Install EFOS

Perform the following steps to install or upgrade the EFOS software.

Note that after upgrading BES-53248 cluster switches from EFOS 3.3.x.x or 3.4.x.x to EFOS 3.7.0.4 or 3.8.0.2, Inter-Switch Links (ISLs) and port channel are marked in the **Down** state. See this KB article: [BES-53248 Cluster Switch NDU failed upgrade to EFOS 3.7.0.4 and later](#) for further details.

### Steps

1. Connect the BES-53248 cluster switch to the management network.
2. Use the `ping` command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

### Show example

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2)# ping 172.19.2.1  
Pinging 172.19.2.1 with 0 bytes of data:  
  
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

### 3. Back up the current active image on cs2:

```
show bootvar
```

## Show example

```
(cs2)# show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.3.3	Q.10.22.1	3.4.3.3	3.4.3.3

```
(cs2)# copy active backup
```

Copying active to backup

Management access will be blocked for the duration of the operation

Copy operation successful

```
(cs2)# show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.3.3	3.4.3.3	3.4.3.3	3.4.3.3

```
(cs2)#
```

## 4. Verify the running version of the EFOS software:

```
show version
```

## Show example

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,
3.4.3.3, Linux 4.4.117-ceeeb99d, 2016.05.00.05
Machine Type..... BES-53248A1
Machine Model..... BES-53248
Serial Number..... QTFCU38260014
Maintenance Level..... A
Manufacturer..... 0xbc00
Burned In MAC Address..... D8:C4:97:71:12:3D
Software Version..... 3.4.3.3
Operating System..... Linux 4.4.117-
ceeeb99d
Network Processing Device..... BCM56873_A0
CPLD Version..... 0xff040c03

Additional Packages..... BGP-4
..... QOS
..... Multicast
..... IPv6
..... Routing
..... Data Center
..... OpEN API
..... Prototype Open API
```

### 5. Download the image file to the switch.

Copying the image file to the active image means that when you reboot, that image establishes the running EFOS version. The previous image remains available as a backup.



Show example

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.4.4.6.stk active
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.4.4.6.stk
Data Type..... Code
Destination Filename..... active

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...

File transfer operation completed successfully.
```

6. Display the boot images for the active and backup configuration:

```
show bootvar
```

Show example

```
(cs2)# show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1         3.4.3.3      3.4.3.3      3.4.3.3             3.4.4.6
```

7. Reboot the switch:

```
reload
```

### Show example

```
(cs2)# reload
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully .
```

```
Configuration Saved!
```

```
System will now restart!
```

### 8. Log in again and verify the new version of the EFOS software:

```
show version
```

### Show example

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.4.4.6, Linux 4.4.211-28a6fe76, 2016.05.00.04  
Machine Type..... BES-53248A1,  
Machine Model..... BES-53248  
Serial Number..... QTFCU38260023  
Maintenance Level..... A  
Manufacturer..... 0xbc00  
Burned In MAC Address..... D8:C4:97:71:0F:40  
Software Version..... 3.4.4.6  
Operating System..... Linux 4.4.211-  
28a6fe76  
Network Processing Device..... BCM56873_A0  
CPLD Version..... 0xff040c03
```

```
Additional Packages..... BGP-4  
..... QOS  
..... Multicast  
..... IPv6  
..... Routing  
..... Data Center  
..... OpEN API  
..... Prototype Open API
```





```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configure the Ethernet interface and add the route using `ifconfig eth0 <ipAddress> netmask <netmask> up` and `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Verify that the server hosting the ONIE installation file is reachable:

ping

**Show example**

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Install the new switch software:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

### Show example

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

The software installs and then reboots the switch. Let the switch reboot normally into the new EFOS version.

#### 6. Verify that the new switch software is installed:

```
show bootvar
```

### Show example

```
(cs2)# show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
-----
unit    active      backup    current-active  next-active
-----
1       3.7.0.4        3.7.0.4    3.7.0.4         3.7.0.4
(cs2) #
```

#### 7. Complete the installation.

The switch will reboot with no configuration applied and reset to factory defaults.

### What's next?

[Install licenses for BES-53248 cluster switches.](#)

# Install licenses for BES-53248 cluster switches

The BES-53248 cluster switch base model is licensed for 16 10GbE or 25GbE ports and two 100GbE ports. You can add new ports by purchasing more licenses.

## Review available licenses

The following licenses are available for use on the BES-53248 cluster switch:

License type	License details	Supported firmware version
SW-BES-53248A2-8P-2P	Broadcom 8PT-10G25G + 2PT-40G100G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES-53248A2-8P-1025G	Broadcom 8 Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES53248A2-6P-40-100G	Broadcom 6 Port 40G100G License Key, X190005/R	EFOS 3.4.4.6 and later

## Legacy licenses

The following table lists the legacy licenses that were available for use on the BES-53248 cluster switch:

License type	License details	Supported firmware version
SW-BES-53248A1-G1-8P-LIC	Broadcom 8P 10-25,2P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES-53248A1-G1-16P-LIC	Broadcom 16P 10-25,4P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES-53248A1-G1-24P-LIC	Broadcom 24P 10-25,6P40-100 License Key, X190005/R	EFOS 3.4.3.3 and later
SW-BES54248-40-100G-LIC	Broadcom 6Port 40G100G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES53248-8P-10G25G-LIC	Broadcom 8Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later
SW-BES53248-16P-1025G-LIC	Broadcom 16Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later

License type	License details	Supported firmware version
SW-BES53248-24P-1025G-LIC	Broadcom 24Port 10G25G License Key, X190005/R	EFOS 3.4.4.6 and later



A license is not required for the base configuration.

## Install license files

Follow these steps to install licenses for BES-53248 cluster switches.

### Steps

1. Connect the cluster switch to the management network.
2. Use the `ping` command to verify connectivity to the server hosting EFOS, licenses, and the RCF file.

#### Show example

This example verifies that the switch is connected to the server at IP address 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Ping 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Check the current license usage on switch cs2:

```
show license
```

#### Show example

```
(cs2)# show license
Reboot needed..... No
Number of active licenses..... 0

License Index  License Type      Status
-----
No license file found.
```

4. Install the license file.

Repeat this step to load more licenses and to use different key index numbers.



### Show example

The following example uses SFTP to copy a license file to a key index 1.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... /var/lib/tftpboot/
Filename..... license.dat
Data Type..... license

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...

License Key transfer operation completed successfully. System reboot
is required.
```

5. Display all current license information and note the license status before switch cs2 is rebooted:

```
show license
```

### Show example

```
(cs2)# show license

Reboot needed..... Yes
Number of active licenses..... 0

License Index  License Type      Status
-----
1              Port              License valid but not applied
```

6. Display all licensed ports:

```
show port all | exclude Detach
```

The ports from the additional license files are not displayed until after the switch is rebooted.

Show example



```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----	-----	-----	-----	-----	-----	-----	-----
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/55		Disable	Auto		Down	Enable	
Enable long							
0/56		Disable	Auto		Down	Enable	
Enable long							

7. Reboot the switch:

```
reload
```

**Show example**

```
(cs2)# reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!
Are you sure you would like to reset the system? (y/n) y
```

8. Check that the new license is active and note that the license has been applied:

```
show license
```

**Show example**

```
(cs2)# show license

Reboot needed..... No
Number of installed licenses..... 1
Total Downlink Ports enabled..... 16
Total Uplink Ports enabled..... 8

License Index  License Type                Status
-----
-----
1              Port                      License applied
```

9. Check that all new ports are available:

```
show port all | exclude Detach
```

## Show example

```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----		-----	-----	-----	-----	-----	
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/49		Disable	100G Full		Down	Enable	
Enable long							
0/50		Disable	100G Full		Down	Enable	
Enable long							

0/51	Disable	100G	Full	Down	Enable
Enable long					
0/52	Disable	100G	Full	Down	Enable
Enable long					
0/53	Disable	100G	Full	Down	Enable
Enable long					
0/54	Disable	100G	Full	Down	Enable
Enable long					
0/55	Disable	100G	Full	Down	Enable
Enable long					
0/56	Disable	100G	Full	Down	Enable
Enable long					



When installing additional licenses, you must configure the new interfaces manually. Do not re-apply an RCF to an existing working production switch.

## Troubleshoot install issues

Where problems arise when installing a license, run the following debug commands before running the `copy` command again.

Debug commands to use: `debug transfer` and `debug license`

### Show example

```
(cs2)# debug transfer
Debug transfer output is enabled.
(cs2)# debug license
Enabled capability licensing debugging.
```

When you run the `copy` command with the `debug transfer` and `debug license` options enabled, the log output is returned.

## Show example

```
transfer.c(3083):Transfer process  key or certificate file type = 43
transfer.c(3229):Transfer process  key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
LICENSING :
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
    },
    "description": "",
    "ports": "0+6"
  }
}.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Model BES-53248
matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Applying license file
1.
```

Check for the following in the debug output:

- Check that the Serial number matches: Serial number QTFCU38290012 matched.
- Check that the switch Model matches: Model BES-53248 matched.
- Check that the specified license index was not used previously. Where a license index is already used, the following error is returned: License file /mnt/download//license.dat.1 already exists.
- A port license is not a feature license. Therefore, the following statement is expected: Feature not found in license file with index = 1.

Use the copy command to back up port licenses to the server:



```
(cs2) # copy nvram:license-key 1  
scp://<UserName>@<IP_address>/saved_license_1.dat
```



If you need to downgrade the switch software from version 3.4.4.6, the licenses are removed. This is expected behavior.

You must install an appropriate older license before reverting to an older version of the software.

## Activate newly licensed ports

To activate newly licensed ports, you need to edit the latest version of the RCF and uncomment the applicable port details.

The default license activates ports 0/1 to 0/16 and 0/55 to 0/56 while the newly licensed ports will be between ports 0/17 to 0/54 depending on the type and number of licenses available. For example, to activate the SW-BES54248-40-100G-LIC license, you must uncomment the following section in the RCF:

## Show example

```
.
.
!
! 2-port or 6-port 40/100GbE node port license block
!
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
.
.
```



For high-speed ports between 0/49 to 0/54 inclusive, uncomment each port but only uncomment one **speed** line in the RCF for each of these ports, either: **speed 100G full-duplex** or **speed 40G full-duplex** as shown in the example. For low-speed ports between 0/17 to 0/48 inclusive, uncomment the entire 8-port section when an appropriate license has been activated.

### What's next?

[Install the Reference Configuration File \(RCF\).](#)

## Install the Reference Configuration File (RCF)

You can install the Reference Configuration File (RCF) after configuring the BES-53248 cluster switch and after applying the new licenses.

If you are upgrading an RCF from an older version, you must reset the Broadcom switch settings and perform basic configuration to re-apply the RCF. You must perform this operation every time you want to upgrade or change an RCF. See the [KB article](#) for details.

## Review requirements

### Before you begin

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- The current RCF file, available from the [Broadcom Cluster Switches](#) page.
- A boot configuration in the RCF that reflects the desired boot images, required if you are installing only EFOS and keeping your current RCF version. If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- A console connection to the switch, required when installing the RCF from a factory-default state. This requirement is optional if you have used the Knowledge Base article [How to clear configuration on a Broadcom interconnect switch while retaining remote connectivity](#) to clear the configuration, beforehand.

### Suggested documentation

- Consult the switch compatibility table for the supported ONTAP and RCF versions. See the [EFOS Software download](#) page. Note that there can be command dependencies between the command syntax in the RCF and that found in versions of EFOS.
- Refer to the appropriate software and upgrade guides available on the [Broadcom](#) site for complete documentation on the BES-53248 switch upgrade and downgrade procedures.

## Install the configuration file

### About the examples

The examples in this procedure use the following switch and node nomenclature:

- The names of the two BES-53248 switches are cs1 and cs2.
- The node names are cluster1-01, cluster1-02, cluster1-03, and cluster1-04.
- The cluster LIF names are cluster1-01\_clus1, cluster1-01\_clus2, cluster1-02\_clus1, cluster1-02\_clus2, cluster1-03\_clus1, cluster1-03\_clus2, cluster1-04\_clus1, and cluster1-04\_clus2.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The examples in this procedure use four nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b. See the [Hardware Universe](#) to verify the correct cluster ports on your platforms.



The command outputs might vary depending on different releases of ONTAP.

### About this task

The procedure requires the use of both ONTAP commands and Broadcom switch commands; ONTAP commands are used unless otherwise indicated.

No operational inter-switch link (ISL) is needed during this procedure. This is by design because RCF version changes can affect ISL connectivity temporarily. To ensure non-disruptive cluster operations, the following procedure migrates all the cluster LIFs to the operational partner switch while performing the steps on the target switch.



Before installing a new switch software version and RCFs, use the [KB: How to clear configuration on a Broadcom interconnect switch while retaining remote connectivity](#). If you must erase the switch settings completely, then you will need to perform the basic configuration again. You must be connected to the switch using the serial console, since a complete configuration erasure resets the configuration of the management network.

## Step 1: Prepare for the installation

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

where x is the duration of the maintenance window in hours.



The AutoSupport message notifies technical support of this maintenance task so that automatic case creation is suppressed during the maintenance window.

The following command suppresses automatic case creation for two hours:

```
cluster1::*> system node autosupport invoke -node \* -type all -message  
MAINT=2h
```

2. Change the privilege level to advanced, entering y when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (\*>) appears.

3. Display the cluster ports on each node that are connected to the cluster switches: `network device-discovery show`

#### Show example

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
              e0a    cs1                      0/2          BES-
53248
              e0b    cs2                      0/2          BES-
53248
cluster1-02/cdp
              e0a    cs1                      0/1          BES-
53248
              e0b    cs2                      0/1          BES-
53248
cluster1-03/cdp
              e0a    cs1                      0/4          BES-
53248
              e0b    cs2                      0/4          BES-
53248
cluster1-04/cdp
              e0a    cs1                      0/3          BES-
53248
              e0b    cs2                      0/3          BES-
53248
cluster1::*>
```

4. Check the administrative and operational status of each cluster port.
  - a. Verify that all the cluster ports are up with a healthy status: `network port show -role cluster`

## Show example

```
cluster1::*> network port show -role cluster
```

```
Node: cluster1-01
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
8 entries were displayed.
```

```
Node: cluster1-03
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

cluster1::\*>

- b. Verify that all the cluster interfaces (LIFs) are on the home port: `network interface show -role cluster`



### Show example

```
cluster1::*> network interface show -role cluster
```

	Logical	Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
-----				
Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

5. Verify that the cluster displays information for both cluster switches.

### ONTAP 9.8 and later

Beginning with ONTAP 9.8, use the command: `system switch ethernet show -is-monitoring-enabled-  
-enabled-operational true`

```
cluster1::*> system switch ethernet show -is-monitoring-enabled  
-operational true
```

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

### ONTAP 9.7 and earlier

For ONTAP 9.7 and earlier, use the command: `system cluster-switch show -is-monitoring  
-enabled-operational true`

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
```

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

## 6. Disable auto-revert on the cluster LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

## Step 2: Configure ports

1. On cluster switch cs2, shut down the ports connected to the cluster ports of the nodes.

```
(cs2) (Config) # interface 0/1-0/16
(cs2) (Interface 0/1-0/16) # shutdown
```

2. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.

```
network interface show -role cluster
```

### Show example

```
cluster1::*> network interface show -role cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
-----				
Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a	false		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0a	false		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0a	false		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0a	false		

```
cluster1::*>
```

3. Verify that the cluster is healthy: `cluster show`

### Show example

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

4. If you have not already done so, save the current switch configuration by copying the output of the following command to a log file: `show running-config`

5. Clean the configuration on switch cs2 and perform a basic setup.



When updating or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch using the serial console to erase switch settings.

a. SSH into the switch.

Only proceed when all the cluster LIFs have been removed from the ports on the switch and the switch is prepared to have the configuration cleared.

b. Enter privilege mode:

```
(cs2)> enable
```

```
(cs2) #
```

c. Copy and paste the following commands to remove the previous RCF configuration (depending on the previous RCF version used, some commands might generate an error if a particular setting is not present):

### Show example

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no class-map CLUSTER
no class-map HA
no class-map RDMA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
```

- d. Save the running configuration to the startup configuration:

#### Show example

```
(cs2)# write memory
```

```
This operation may take a few minutes.  
Management interfaces will not be available during this time.
```

```
Are you sure you want to save? (y/n) y
```

```
Config file 'startup-config' created successfully .
```

```
Configuration Saved!
```

e. Perform a reboot of the switch:

#### Show example

```
(cs2)# reload
```

```
Are you sure you would like to reset the system? (y/n) y
```

- f. Log in to the switch again using SSH to complete the RCF installation.
6. If additional port licenses have been installed on the switch, you must modify the RCF to configure the additional licensed ports. See [Activate newly licensed ports](#) for details.
  7. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP.

This example shows SFTP being used to copy an RCF to the bootflash on switch cs2:

### Show example

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt
nvram:script BES-53248_RCF_v1.9-Cluster-HA.scr
Remote Password:**
Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... BES-53248_RCF_v1.9-Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... BES-53248_RCF_v1.9-Cluster-HA.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...
File transfer operation completed successfully.
```

8. Verify that the script was downloaded and saved to the file name you gave it:

```
script list
```

### Show example

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

1 configuration script(s) found.

9. Apply the script to the switch:

```
script apply
```



### Show example

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

10. Examine the banner output from the `show clibanner` command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

## Show example

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename   : BES-53248-RCF-v1.9-Cluster.txt
```

```
Date       : 10-26-2022
```

```
Version    : v1.9
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

```
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms  
of port
```

```
speed:
```

```
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-  
40, 41-44,  
45-48
```

```
The port speed should be the same (10GbE or 25GbE) across all ports  
in a 4-port
```

```
group
```

```
- If additional licenses are purchased, follow the 'Additional Node  
Ports
```

```
activated with Licenses' section for instructions
```

```
- If SSH is active, it will have to be re-enabled manually after  
'erase
```

```
startup-config'
```

```
command has been executed and the switch rebooted
```

11. On the switch, verify that the additional licensed ports appear after the RCF is applied:

```
show port all | exclude Detach
```

## Show example

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					
-----						
0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

12. Verify on the switch that your changes have been made:

```
show running-config
```

```
(cs2)# show running-config
```

13. Save the running configuration so that it becomes the startup configuration when you reboot the switch:

```
write memory
```

**Show example**

```
(cs2)# write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

14. Reboot the switch and verify that the running configuration is correct:

```
reload
```

### Show example

```
(cs2)# reload
```

```
Are you sure you would like to reset the system? (y/n) y
```

```
System will now restart!
```

15. On cluster switch cs2, bring up the ports connected to the cluster ports of the nodes.

```
(cs2) (Config)# interface 0/1-0/16
```

```
(cs2) (Interface 0/1-0/16)# no shutdown
```

16. Verify the ports on switch cs2: `show interfaces status all | exclude Detach`

## Show example

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

17. Verify the health of cluster ports on the cluster.

- Verify that e0b ports are up and healthy across all nodes in the cluster: `network port show -role cluster`

## Show example

```
cluster1::*> network port show -role cluster
```

```
Node: cluster1-01
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

```
Node: cluster1-03
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

b. Verify the switch health from the cluster.



## Show example

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
-----			
-----			
cluster1-01/cdp	e0a	cs1	0/2
BES-53248	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp	e0a	cs1	0/1
BES-53248	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp	e0a	cs1	0/4
BES-53248	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp	e0a	cs1	0/3
BES-53248	e0b	cs2	0/2
BES-53248			

## ONTAP 9.8 and later

Beginning with ONTAP 9.8, use the command: `system switch ethernet show -is-monitoring-enabled-  
-enabled-operational true`

```
cluster1::*> system switch ethernet show -is-monitoring-enabled  
-operational true
```

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

## ONTAP 9.7 and earlier

For ONTAP 9.7 and earlier, use the command: `system cluster-switch show -is-monitoring  
-enabled-operational true`

```

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                Type                                Address                                Model
-----
cs1                                   cluster-network                    10.228.143.200                       BES-
53248
    Serial Number: QTWCU22510008
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP

cs2                                   cluster-network                    10.228.143.202                       BES-
53248
    Serial Number: QTWCU22510009
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP
cluster1::*>

```

18. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes.

The following example uses the interface example output:

```

(cs1)# configure
(cs1) (Config)# interface 0/1-0/16
(cs1) (Interface 0/1-0/16)# shutdown

```

19. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds.  
`network interface show -role cluster`

### Show example

```
cluster1::*> network interface show -role cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
-----				
Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	false		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

20. Verify that the cluster is healthy: cluster show

### Show example

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

21. Repeat steps 4 to 14 on switch cs1.

22. Enable auto-revert on the cluster LIFs: cluster1::\*> network interface modify -vserver

```
Cluster -lif * -auto-revert true
```

23. Reboot switch cs1. You do this to trigger the cluster LIFs to revert to their home ports. You can ignore the “cluster ports down” events reported on the nodes while the switch reboots.

#### Show example

```
(cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved! System will now restart!
```

### Step 3: Verify the configuration

1. On switch cs1, verify that the switch ports connected to the cluster ports are **up**.

## Show example

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Verify that the ISL between switches cs1 and cs2 is functional: show port-channel 1/1

Show example

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----
0/55      actor/long      Auto      True
          partner/long
0/56      actor/long      Auto      True
          partner/long
```

3. Verify that the cluster LIFs have reverted to their home port: `network interface show -role cluster`

### Show example

```
cluster1::*> network interface show -role cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
-----				
Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

4. Verify that the cluster is healthy: `cluster show`

### Show example

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

5. Ping the remote cluster interfaces to verify connectivity: `cluster ping-cluster -node local`



## Show example

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

### 6. Change the privilege level back to admin:

```
set -privilege admin
```

### 7. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

### What's next?

[Install the CSHM configuration file.](#)

## Enable SSH on BES-53248 cluster switches

If you are using the Cluster Switch Health Monitor (CSHM) and log collection features, you must generate the SSH keys and then enable SSH on the cluster switches.

### Steps

1. Verify that SSH is disabled:

```
show ip ssh
```

#### Show example

```
(switch)# show ip ssh
```

SSH Configuration

```
Administrative Mode: ..... Disabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Disabled
SCP server Administrative Mode: ..... Disabled
```

2. Generate the SSH keys:

```
crypto key generate
```

### Show example

```
(switch)# config

(switch) (Config)# crypto key generate rsa

Do you want to overwrite the existing RSA keys? (y/n): y

(switch) (Config)# crypto key generate dsa

Do you want to overwrite the existing DSA keys? (y/n): y

(switch) (Config)# crypto key generate ecdsa 521

Do you want to overwrite the existing ECDSA keys? (y/n): y

(switch) (Config)# aaa authorization commands "noCmdAuthList" none
(switch) (Config)# exit
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
(switch)# write mem

This operation may take a few minutes.
Management interfaces will not be available during this time.
Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```



Make sure that SSH is disabled before modifying the keys otherwise a warning is reported on the switch.

#### 3. Reboot the switch:

```
reload
```

#### 4. Verify that SSH is enabled:

```
show ip ssh
```

### Show example

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: ..... Enabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Enabled
SCP server Administrative Mode: ..... Enabled
```

### What's next?

[Enable log collection.](#)

## Ethernet Switch Health Monitoring log collection

The Ethernet switch health monitor (CSHM) is responsible for ensuring the operational health of Cluster and Storage network switches and collecting switch logs for debugging purposes. This procedure guides you through the process of setting up and starting the collection of detailed **Support** logs from the switch and starts an hourly collection of **Periodic** data that is collected by AutoSupport.

### Before you begin

- To enable the log collection feature, you must be running ONTAP version 9.12.1 or later and EFOS 3.8.0.2 or later.
- Switch health monitoring must be enabled for the switch. Verify this by ensuring the `Is Monitored:` field is set to **true** in the output of the `system switch ethernet show` command.

### Steps

1. To set up log collection, run the following command for each switch. You are prompted to enter the switch name, username, and password for log collection.

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

## Show example

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

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

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

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

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

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

2. To start log collection, run the following command, replacing **DEVICE** with the switch used in the previous command. This starts both types of log collection: the detailed **Support** logs and an hourly collection of **Periodic** data.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

## Show example

```
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.
```

Wait for 10 minutes and then check that the log collection completes:

```
system switch ethernet log show
```



If any of these commands return an error or if the log collection does not complete, contact NetApp support.

## Troubleshooting

If you encounter any of the following error statuses reported by the log collection feature (visible in the output of `system switch ethernet log show`), try the corresponding debug steps:

Log collection error status	Resolution
<b>RSA keys not present</b>	Regenerate ONTAP SSH keys. Contact NetApp support.
<b>switch password error</b>	Verify credentials, test SSH connectivity, and regenerate ONTAP SSH keys. Review switch documentation or contact NetApp support for instructions.
<b>ECDSA keys not present for FIPS</b>	If FIPS mode is enabled, ECDSA keys need to be generated on the switch before retrying.
<b>pre-existing log found</b>	Remove the previous log collection file on the switch.

**switch dump log error**

Ensure the switch user has log collection permissions. Refer to the prerequisites above.

## Configure SNMPv3

Follow this procedure to configure SNMPv3, which supports Ethernet switch health monitoring (CSHM).

### About this task

The following commands configure an SNMPv3 username on Broadcom BES-53248 switches:

- For **no authentication**: `snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth`
- For **MD5/SHA authentication**: `snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]`
- For **MD5/SHA authentication with AES/DES encryption**: `snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-md5|auth-sha] [priv-aes128|priv-des]`

The following command configures an SNMPv3 username on the ONTAP side: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication -method usm -remote-switch-ipaddress ADDRESS`

The following command establishes the SNMPv3 username with CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

### Steps

1. Set up the SNMPv3 user on the switch to use authentication and encryption:

```
show snmp status
```

### Show example

```
(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. Set up the SNMPv3 user on the ONTAP side:

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

### Show example

```
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. Configure CSHM to monitor with the new SNMPv3 user:

```
system switch ethernet show-all -device "sw1" -instance
```



### Show example

```
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. Verify that the serial number to be queried with the newly created SNMPv3 user is the same as detailed in the previous step after the CSHM polling period has completed.

```
system switch ethernet polling-interval show
```

## Show example

```
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
```

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.