



Configurez le logiciel

Cluster and storage switches

NetApp
April 25, 2024

Sommaire

- Configurez le logiciel 1
 - Préparez l'installation du logiciel NX-OS et du fichier de configuration de référence 1
 - Installez le logiciel NX-OS 6
 - Installer le fichier RCF (Reference Configuration File). 13
 - Collecte du journal de surveillance de l'état du commutateur Ethernet 38
 - Configurer SNMPv3 41

Configurez le logiciel

Préparez l'installation du logiciel NX-OS et du fichier de configuration de référence

Avant d'installer le logiciel NX-OS et le fichier RCF (Reference Configuration File), suivez cette procédure.

À propos des exemples

Les exemples de cette procédure utilisent deux nœuds. Ces nœuds utilisent deux ports d'interconnexion de cluster 10GbE e0a et e0b.

Voir la "[Hardware Universe](#)" pour vérifier les ports de cluster appropriés sur vos plates-formes.



Les sorties de la commande peuvent varier en fonction des différentes versions d'ONTAP.

Les exemples de cette procédure utilisent la nomenclature des commutateurs et des nœuds suivante :

- Les noms des deux commutateurs Cisco sont `cs1` et `cs2`.
- Les noms de nœud sont `cluster1-01` et `cluster1-02`.
- Les noms LIF de cluster sont `cluster1-01_clus1` et `cluster1-01_clus2` pour `cluster1-01` et `cluster1-02_clus1` et `cluster1-02_clus2` pour `cluster 1-02`.
- Le `cluster1 : *>` l'invite indique le nom du cluster.

Description de la tâche

La procédure nécessite l'utilisation des commandes ONTAP et des commutateurs Cisco Nexus 3000 ; les commandes ONTAP sont utilisées sauf indication contraire.

Étapes

1. Si AutoSupport est activé sur ce cluster, supprimez la création automatique de dossiers en invoquant un message AutoSupport :

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

où x représente la durée de la fenêtre de maintenance en heures.



Le message AutoSupport informe le support technique de cette tâche de maintenance de sorte que la création automatique de dossier soit supprimée lors de la fenêtre de maintenance.

2. Définissez le niveau de privilège sur avancé, en entrant **y** lorsque vous êtes invité à continuer :

```
set -privilege advanced
```

L'invite avancée (***>**) s'affiche.

3. Afficher le nombre d'interfaces d'interconnexion de cluster configurées sur chaque nœud pour chaque commutateur d'interconnexion de cluster :

```
network device-discovery show -protocol cdp
```

Montrer l'exemple

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e0a	cs1	Eth1/2	N3K-
C3132Q-V	e0b	cs2	Eth1/2	N3K-
C3132Q-V				
cluster1-01/cdp	e0a	cs1	Eth1/1	N3K-
C3132Q-V	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

4. Vérifier le statut administratif ou opérationnel de chaque interface de cluster.

a. Afficher les attributs des ports réseau :

```
network port show -ipSPACE Cluster
```

Montrer l'exemple

```
cluster1::*> network port show -ipspace Cluster
```

```
Node: cluster1-02
```

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

```
Node: cluster1-01
```

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

b. Afficher les informations relatives aux LIFs :

```
network interface show -vserver Cluster
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver Cluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.49.125/16	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			

5. Exécutez une commande ping des LIFs de cluster distantes :

```
cluster ping-cluster -node local
```

Montrer l'exemple

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01      e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01      e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02      e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Vérifiez que le auto-revert La commande est activée sur l'ensemble des LIFs du cluster :

```
network interface show -vserver Cluster -fields auto-revert
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver Cluster -fields auto-revert
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

Et la suite ?

["Installez le logiciel NX-OS".](#)

Installez le logiciel NX-OS

Suivez cette procédure pour installer le logiciel NX-OS sur le commutateur de cluster Nexus 3132Q-V.

Examen des conditions requises

Ce dont vous avez besoin

- Sauvegarde actuelle de la configuration du commutateur.
- Cluster totalement opérationnel (aucune erreur dans les journaux ou problèmes similaires).

Documentation suggérée

- ["Commutateur Ethernet Cisco"](#). Consultez le tableau de compatibilité des commutateurs pour connaître les versions ONTAP et NX-OS prises en charge.
- ["Commutateurs Cisco Nexus 3000 Series"](#). Consultez les guides de mise à niveau et de logiciels appropriés disponibles sur le site Web de Cisco pour obtenir une documentation complète sur les procédures de mise à niveau et de mise à niveau vers une version antérieure du commutateur Cisco.

Installez le logiciel

Description de la tâche

La procédure nécessite l'utilisation des commandes ONTAP et des commutateurs Cisco Nexus 3000 ; les commandes ONTAP sont utilisées sauf indication contraire.

Veiller à terminer la procédure dans ["Préparez l'installation du logiciel NX-OS et du fichier de configuration de référence"](#), puis suivez les étapes ci-dessous.

Étapes

1. Connectez le commutateur de cluster au réseau de gestion.
2. Utilisez le `ping` Commande permettant de vérifier la connectivité au serveur hébergeant le logiciel NX-OS et le FCR.

Montrer l'exemple

```
cs2# ping 172.19.2.1 vrf management
Pinging 172.19.2.1 with 0 bytes of data:

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

3. Copiez le logiciel NX-OS sur le commutateur Nexus 3132Q-V à l'aide de l'un des protocoles de transfert suivants : FTP, TFTP, SFTP ou SCP. Pour plus d'informations sur les commandes Cisco, reportez-vous au guide approprié dans ["Guides de référence des commandes Cisco Nexus série 3000 NX-OS"](#).

Montrer l'exemple

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password: xxxxxxxx
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Vérifiez la version en cours d'exécution du logiciel NX-OS :

```
show version
```

Montrer l'exemple

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
  NXOS: version 9.3(3)
  BIOS compile time: 01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
  NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(3)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Installez l'image NX-OS.

L'installation du fichier image entraîne son chargement à chaque redémarrage du commutateur.

Montrer l'exemple

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Performing module support checks.
[] 100% -- SUCCESS

Notifying services about system upgrade.
[] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----  -
      1      yes          disruptive          reset          default
upgrade is not hitless

Images will be upgraded according to following table:
Module      Image      Running-Version(pri:alt)
New-Version      Upg-Required
-----  -
      1      nxos      9.3(3)
9.3(4)          yes
      1      bios      v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)  no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

```
cs2#
```

6. Vérifiez la nouvelle version du logiciel NX-OS après le redémarrage du commutateur :

```
show version
```

Montrer l'exemple

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
  NXOS: version 9.3(4)
  BIOS compile time: 05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(4)
Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s) :

cs2#
```

Et la suite ?

["Installer le fichier RCF \(Reference Configuration File\)".](#)

Installer le fichier RCF (Reference Configuration File)

Suivre cette procédure pour installer la FCR après avoir configuré pour la première fois le commutateur Nexus 3132Q-V. Vous pouvez également utiliser cette procédure pour mettre à niveau votre version RCF.

Examen des conditions requises

Ce dont vous avez besoin

- Sauvegarde actuelle de la configuration du commutateur.
- Cluster totalement opérationnel (aucune erreur dans les journaux ou problèmes similaires).
- Le fichier FCR (Reference Configuration File) actuel.
- Connexion de la console au commutateur, requise lors de l'installation du FCR.
- ["Commutateur Ethernet Cisco"](#). Consultez le tableau de compatibilité des commutateurs pour connaître les versions ONTAP et RCF prises en charge. Notez que la syntaxe de la commande peut être utilisée dans la FCR et dans les versions de NX-OS.
- ["Commutateurs Cisco Nexus 3000 Series"](#). Consultez les guides de mise à niveau et de logiciels appropriés disponibles sur le site Web de Cisco pour obtenir une documentation complète sur les procédures de mise à niveau et de mise à niveau vers une version antérieure du commutateur Cisco.

Installez le fichier

À propos des exemples

Les exemples de cette procédure utilisent la nomenclature des commutateurs et des nœuds suivante :

- Les noms des deux commutateurs Cisco sont `cs1` et `cs2`.
- Les noms de nœud sont `cluster1-01`, `cluster1-02`, `cluster1-03`, et `cluster1-04`.
- Les noms LIF de cluster sont `cluster1-01_clus1`, `cluster1-01_clus2`, `cluster1-02_clus1`, `cluster1-02_clus2`, `cluster1-03_clus1`, `cluster1-03_clus2`, `cluster1-04_clus1`, et

```
cluster1-04_clus2.
```

- Le `cluster1::*>` l'invite indique le nom du cluster.

Description de la tâche

La procédure nécessite l'utilisation des commandes ONTAP et des commutateurs Cisco Nexus 3000 ; les commandes ONTAP sont utilisées sauf indication contraire.

Aucune liaison inter-commutateurs (ISL) opérationnelle n'est nécessaire au cours de cette procédure. Ceci est de par sa conception, car les modifications de version des fichiers RCF peuvent affecter temporairement la connectivité ISL. Pour assurer un fonctionnement sans interruption du cluster, la procédure suivante migre toutes les LIFs du cluster vers le commutateur partenaire opérationnel tout en effectuant les étapes sur le commutateur cible.

Veiller à terminer la procédure dans ["Préparez l'installation du logiciel NX-OS et du fichier de configuration de référence"](#), puis suivez les étapes ci-dessous.

Étape 1 : vérifier l'état des ports

1. Afficher les ports de cluster sur chaque nœud connecté aux commutateurs du cluster :

```
network device-discovery show
```


Montrer l'exemple

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N3K-
C3132Q-V
          e0d    cs2                Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3132Q-V
          e0d    cs2                Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3132Q-V
          e0b    cs2                Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3132Q-V
          e0b    cs2                Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*>
```

2. Vérifiez le statut administratif et opérationnel de chaque port du cluster.

a. Vérifier que tous les ports du cluster sont défectueux :

```
network port show -ipospace Cluster
```

Montrer l'exemple

```
cluster1::*> network port show -ipspace 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					
e0d	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					
e0d	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. Vérifier que toutes les interfaces de cluster (LIFs) sont sur le port de home port :

```
network interface show -vserver Cluster
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver Cluster
```

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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	e0d 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	e0d 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			

```
cluster1::*>
```

c. Vérifiez que le cluster affiche les informations relatives aux deux commutateurs de cluster :

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Montrer l'exemple

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                       cluster-network     10.0.0.1
NX3132QV
    Serial Number: FOXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                        9.3(4)
    Version Source: CDP

cs2                                       cluster-network     10.0.0.2
NX3132QV
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                        9.3(4)
    Version Source: CDP

2 entries were displayed.
```



Pour ONTAP 9.8 et versions ultérieures, utilisez la commande `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Désactivez la fonction de restauration automatique sur les LIF du cluster.

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

Assurez-vous que la fonction de restauration automatique est désactivée après avoir exécuté cette commande.

4. Sur le commutateur de cluster cs2, arrêtez les ports connectés aux ports de cluster des nœuds.

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

5. Vérifiez que les ports de cluster ont migré vers les ports hébergés sur le commutateur de cluster cs1. Cette opération peut prendre quelques secondes.

```
network interface show -vserver Cluster
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver Cluster
```

Current Is	Logical	Status	Network	Current
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::*>
```

6. Vérifiez que le cluster fonctionne correctement :

```
cluster show
```

Montrer l'exemple

```
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
cluster1::*>
```

Étape 2 : configurer et vérifier la configuration

1. Si ce n'est pas déjà fait, enregistrez une copie de la configuration actuelle du commutateur en copiant la sortie de la commande suivante dans un fichier texte :

```
show running-config
```

2. Nettoyez la configuration du commutateur cs2 et effectuez une configuration de base.



Lors de la mise à jour ou de l'application d'une nouvelle FCR, vous devez effacer les paramètres du commutateur et effectuer une configuration de base. Vous devez être connecté au port série console du commutateur pour pouvoir le configurer à nouveau.

- a. Nettoyez la configuration :

Montrer l'exemple

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

- b. Redémarrer le commutateur :

Montrer l'exemple

```
(cs2)# reload

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

3. Copiez le RCF sur le bootflash du commutateur cs2 à l'aide de l'un des protocoles de transfert suivants : FTP, TFTP, SFTP ou SCP. Pour plus d'informations sur les commandes Cisco, reportez-vous au guide approprié dans le ["Référence des commandes Cisco Nexus série 3000 NX-OS"](#) guides.

Montrer l'exemple

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

4. Appliquez le RCF préalablement téléchargé sur le bootflash.

Pour plus d'informations sur les commandes Cisco, reportez-vous au guide approprié dans le ["Référence des commandes Cisco Nexus série 3000 NX-OS"](#) guides.

Montrer l'exemple

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

5. Examinez le résultat de la bannière du `show banner motd` commande. Vous devez lire et suivre les instructions sous **remarques importantes** pour assurer la configuration et le fonctionnement corrects du commutateur.

Montrer l'exemple

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3132Q-V
* Filename  : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : Nov-02-2020
* Version   : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports 7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```

* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*   - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*     NX-OS using a version later than 9.3(5).
*   - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*   - After the RCF is applied and switch rebooted, then proceed to
upgrade
*     NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*   after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*   hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*   hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*   hardware profile front portmode qsfp      (To reset to QSFP)
*
*****
*****

```

6. Vérifiez que le fichier RCF est la version la plus récente correcte :

```
show running-config
```

Lorsque vous vérifiez que la sortie est correcte, vérifiez que les informations suivantes sont correctes :

- La bannière RCF
- Les paramètres du nœud et du port
- Personnalisations

Le résultat varie en fonction de la configuration de votre site. Vérifiez les paramètres des ports et reportez-vous aux notes de version pour voir si des modifications spécifiques à la FCR que vous avez installée.



Pour savoir comment mettre en ligne les ports 10 GbE après une mise à niveau du RCF, consultez l'article de la base de connaissance ["Les ports 10GbE d'un commutateur de cluster Cisco 3132Q ne sont pas mis en ligne"](#).

7. Après avoir vérifié que les versions de RCF et les paramètres de commutateur sont corrects, copiez le fichier running-config dans le fichier startup-config.

Pour plus d'informations sur les commandes Cisco, reportez-vous au guide approprié dans le ["Référence des commandes Cisco Nexus série 3000 NX-OS"](#) guides.

Montrer l'exemple

```
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

8. Redémarrer le commutateur cs2. Vous pouvez ignorer les événements « cluster port down » signalés sur les nœuds pendant le redémarrage du commutateur.

Montrer l'exemple

```
cs2# reload  
This command will reboot the system. (y/n)? [n] y
```

9. Appliquer la même FCR et sauvegarder la configuration en cours d'exécution pendant une seconde fois.

Montrer l'exemple

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands  
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

10. Vérifier l'état de santé des ports du cluster sur le cluster.
 - a. Vérifier que les ports du cluster fonctionnent correctement sur tous les nœuds du cluster :

```
network port show -ip space Cluster
```

Montrer l'exemple

```
cluster1::*> network port show -ipspace 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					
e0d	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					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

b. Vérifiez l'état du commutateur depuis le cluster.

```
network device-discovery show -protocol cdp
```

Montrer l'exemple

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
cluster1-01/cdp	e0a	cs1	Ethernet1/7
N3K-C3132Q-V	e0d	cs2	Ethernet1/7
cluster01-2/cdp	e0a	cs1	Ethernet1/8
N3K-C3132Q-V	e0d	cs2	Ethernet1/8
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1
N3K-C3132Q-V	e0b	cs2	Ethernet1/1/1
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2
N3K-C3132Q-V	e0b	cs2	Ethernet1/1/2

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

Switch	Type	Address
Model		
cs1	cluster-network	10.233.205.90
N3K-C3132Q-V		
Serial Number: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(4)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91

```

N3K-C3132Q-V
  Serial Number: FOXXXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  9.3(4)
  Version Source: CDP

2 entries were displayed.

```



Pour ONTAP 9.8 et versions ultérieures, utilisez la commande `system switch ethernet show -is-monitoring-enabled-operational true`.

Vous pouvez observer les valeurs de sortie suivantes sur la console des commutateurs cs1 en fonction de la version RCF précédemment chargée sur le commutateur :



```

2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.

```

+



Les nœuds de cluster peuvent prendre jusqu'à 5 minutes pour qu'ils fonctionnent correctement.

11. Sur le commutateur de cluster cs1, arrêtez les ports connectés aux ports de cluster des nœuds.

Montrer l'exemple

```

cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown

```

12. Vérifier que les LIFs de cluster ont migré vers les ports hébergés sur le commutateur cs2. Cette opération peut prendre quelques secondes.

```
network interface show -vserver Cluster
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver 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	e0d	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	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	e0b	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

13. Vérifiez que le cluster fonctionne correctement :

```
cluster show
```

Montrer l'exemple

```
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 entries were displayed.  
cluster1::*>
```


14. Répétez les étapes 1 à 10 de l'interrupteur cs1.
15. Activez la fonction de revert automatique sur les LIFs du cluster.

Montrer l'exemple

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

16. Redémarrer le commutateur cs1. Vous pouvez ainsi déclencher des LIF de cluster afin de rétablir leur port de départ. Vous pouvez ignorer les événements « cluster port down » signalés sur les nœuds pendant le redémarrage du commutateur.

```
cs1# reload  
This command will reboot the system. (y/n)? [n] y
```

Étape 3 : vérifier la configuration

1. Vérifier que les ports de commutateurs connectés aux ports du cluster sont bien connectés.

```
show interface brief | grep up
```

Montrer l'exemple

```
cs1# show interface brief | grep up  
.  
.  
Eth1/1/1      1      eth  access up      none  
10G(D) --  
Eth1/1/2      1      eth  access up      none  
10G(D) --  
Eth1/7        1      eth  trunk  up      none  
100G(D) --  
Eth1/8        1      eth  trunk  up      none  
100G(D) --  
.  
.
```

2. Vérifier que l'ISL entre cs1 et cs2 est fonctionnel :

```
show port-channel summary
```

Montrer l'exemple

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
  Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

3. Vérifier que les LIFs du cluster ont rétabli leur port de base :

```
network interface show -vserver Cluster
```

Montrer l'exemple

```
cluster1::*> network interface show -vserver 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	e0d	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	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	e0b	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

4. Vérifiez que le cluster fonctionne correctement :

```
cluster show
```

Montrer l'exemple

```
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

```
cluster1::*>
```

5. Exécutez une commande ping sur les interfaces de cluster distantes pour vérifier la connectivité :

```
cluster ping-cluster -node local
```

Montrer l'exemple

```
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 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
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. Pour ONTAP 9.8 et versions ultérieures, activez la fonction de collecte des journaux du moniteur d'intégrité

des commutateurs Ethernet pour collecter les fichiers journaux relatifs aux commutateurs à l'aide des commandes :

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

```
system switch ethernet log enable-collection
```

a. Entrez : `system switch ethernet log setup-password`

Montrer l'exemple

```
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
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

b. Entrez : `system switch ethernet log enable-collection`

Montrer l'exemple

```
cluster1::*> system switch ethernet log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Si l'une de ces commandes renvoie une erreur, contactez le support NetApp.

7. Pour ONTAP les versions 9.5P16, 9.6P12 et 9.7P10 et versions ultérieures des correctifs, activez la fonction de collecte des journaux du moniteur d'intégrité des commutateurs Ethernet pour collecter les fichiers journaux liés aux commutateurs à l'aide des commandes suivantes :

```
system cluster-switch log setup-password et
```

```
system cluster-switch log enable-collection
```

- a. Entrez : `system cluster-switch log setup-password`

Montrer l'exemple

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

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

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

b. Entrez: `system cluster-switch log enable-collection`

Montrer l'exemple

```
cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Si l'une de ces commandes renvoie une erreur, contactez le support NetApp.

Collecte du journal de surveillance de l'état du commutateur Ethernet

Vous pouvez utiliser la fonction de collecte de journaux pour collecter des fichiers journaux liés aux commutateurs dans ONTAP.

Le moniteur d'état des commutateurs Ethernet (CSHM) est chargé de garantir l'intégrité opérationnelle des commutateurs du réseau Cluster et Storage et de collecter les journaux des commutateurs à des fins de débogage. Cette procédure vous guide tout au long du processus de configuration et de démarrage de la collecte de journaux **support** détaillés à partir du commutateur et démarre une collecte horaire de données **périodiques** collectées par AutoSupport.

Avant de commencer

- Vérifiez que vous avez configuré votre environnement à l'aide du commutateur de cluster Cisco 3132Q-V CLI.
- La surveillance de l'état du commutateur doit être activée pour le commutateur. Vérifiez ceci en vous assurant que le `Is Monitored`: le champ est défini sur **true** dans la sortie du `system switch ethernet show` commande.

Étapes

1. Créez un mot de passe pour la fonction de collecte du journal du moniteur d'intégrité du commutateur Ethernet :

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


Montrer l'exemple

```
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. Pour démarrer la collecte des journaux, exécutez la commande suivante, en remplaçant le PÉRIPHÉRIQUE par le commutateur utilisé dans la commande précédente. Ceci lance les deux types de collecte de journaux : les journaux détaillés **support** et une collecte horaire de données **périodiques**.

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

Montrer l'exemple

```
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.
```

Attendez 10 minutes, puis vérifiez que la collecte des journaux se termine :

```
system switch ethernet log show
```



Si l'une de ces commandes renvoie une erreur ou si la collecte des journaux ne se termine pas, contactez le support NetApp.

Dépannage

Si vous rencontrez l'un des États d'erreur suivants signalés par la fonction de collecte de journaux (visible dans la sortie de `system switch ethernet log show`), essayez les étapes de débogage correspondantes :

Etat d'erreur de collecte de journaux	Résolution
Clés RSA non présentes	Régénérer les clés SSH ONTAP. Contactez le support NetApp.
erreur de mot de passe de commutateur	Vérifiez les identifiants, testez la connectivité SSH et régénérez les clés SSH ONTAP. Consultez la documentation du commutateur ou contactez le support NetApp pour obtenir des instructions.
Clés ECDSA non présentes pour FIPS	Si le mode FIPS est activé, les clés ECDSA doivent être générées sur le commutateur avant de réessayer.
journal préexistant trouvé	Supprimez le fichier de collecte de journaux précédent sur le commutateur.

Configurer SNMPv3

Suivez cette procédure pour configurer SNMPv3, qui prend en charge la surveillance de l'état du commutateur Ethernet (CSHM).

Description de la tâche

Les commandes suivantes permettent de configurer un nom d'utilisateur SNMPv3 sur les commutateurs Cisco 3132Q-V :

- Pour **pas d'authentification** : `snmp-server user SNMPv3_USER NoAuth`
- Pour l'authentification **MD5/SHA** : `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Pour l'authentification **MD5/SHA avec cryptage AES/DES** : `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

La commande suivante configure un nom d'utilisateur SNMPv3 côté ONTAP : `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication -method usm -remote-switch-ipaddress ADDRESS`

La commande suivante établit le nom d'utilisateur SNMPv3 avec CSHM : `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Étapes

1. Configurez l'utilisateur SNMPv3 sur le commutateur pour utiliser l'authentification et le cryptage :

```
show snmp user
```

Montrer l'exemple

```
(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. Configurez l'utilisateur SNMPv3 sur le côté ONTAP :

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

Montrer l'exemple

```
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. Configurez CSHM pour qu'il surveille avec le nouvel utilisateur SNMPv3 :

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

Montrer l'exemple

```
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: N3K-C3132Q-V
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. Vérifiez que le numéro de série à interroger avec l'utilisateur SNMPv3 nouvellement créé est le même que celui décrit à l'étape précédente après la fin de la période d'interrogation CSHM.

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

Montrer l'exemple

```
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: N3K-C3132Q-V
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::*>
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.