



Configurare il software

Cluster and storage switches

NetApp
April 25, 2024

Sommario

- Configurare il software 1
 - Preparazione all'installazione del software NX-OS e del file di configurazione di riferimento (RCF) 1
 - Installare il software NX-OS 8
 - Installazione del file di configurazione di riferimento (RCF)..... 18
 - Raccolta registro monitoraggio stato switch Ethernet 38
 - Configurare SNMPv3 40

Configurare il software

Preparazione all'installazione del software NX-OS e del file di configurazione di riferimento (RCF)

Prima di installare il software NX-OS e il file di configurazione di riferimento (RCF), seguire questa procedura.

Di cosa hai bisogno

- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Le guide appropriate per il software e l'aggiornamento, disponibili all'interno del sito ["Switch Cisco Nexus serie 9000"](#).

A proposito degli esempi

Gli esempi di questa procedura utilizzano due nodi. Questi nodi utilizzano due porte di interconnessione cluster da 10 GbE e0a e. e0b. Vedere ["Hardware Universe"](#) per verificare le porte cluster corrette sulle piattaforme.

Gli esempi di questa procedura utilizzano la seguente nomenclatura di switch e nodi:

- I nomi dei due switch Cisco sono `cs1` e. `cs2`.
- I nomi dei nodi sono `node1` e. `node2`.
- I nomi LIF del cluster sono `node1_clus1` e. `node1_clus2` per il `node1` e. `node2_clus1` e. `node2_clus2` per il `node2`.
- Il `cluster1: : *>` prompt indica il nome del cluster.

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 9000 Series Switches; i comandi ONTAP vengono utilizzati se non diversamente indicato. Gli output dei comandi possono variare a seconda delle diverse versioni di ONTAP.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (*>).

2. Se AutoSupport è attivato su questo cluster, eliminare la creazione automatica del caso richiamando un messaggio AutoSupport:

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

dove *x* è la durata della finestra di manutenzione in ore.



Il messaggio AutoSupport informa il supporto tecnico di questa attività di manutenzione in modo che la creazione automatica del caso venga soppressa durante la finestra di manutenzione.

Il seguente comando elimina la creazione automatica del caso per due ore:

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

3. Visualizza quante interfacce di interconnessione cluster sono configurate in ciascun nodo per ogni switch di interconnessione cluster: `network device-discovery show -protocol cdp`

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C92300YC				
	e0b	cs2	Eth1/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C92300YC				
	e0b	cs2	Eth1/1	N9K-
C92300YC				

4 entries were displayed.

4. Controllare lo stato amministrativo o operativo di ciascuna interfaccia del cluster.
- a. Visualizzare gli attributi della porta di rete: `network port show -ip space Cluster`

Mostra esempio

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

Node: node2

Health					Speed (Mbps)	
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: node1

Health					Speed (Mbps)	
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						

4 entries were displayed.

b. Visualizzare le informazioni sui LIF: `network interface show -vserver Cluster`

Mostra esempio

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

5. Ping delle LIF del cluster remoto:

```
cluster ping-cluster -node node-name
```

Mostra esempio

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      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. Verificare che il comando di auto-revert sia attivato su tutte le LIF del cluster:

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

Mostra esempio

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

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

7. Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor di stato dello switch del cluster per la raccolta dei file di log relativi allo switch utilizzando i comandi seguenti:

```
system cluster-switch log setup-password e. system cluster-switch log enable-collection
```


Mostra esempio

```
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>

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::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

Quali sono le prossime novità?

["Installare il software NX-OS".](#)

Installare il software NX-OS

Seguire questa procedura per installare il software NX-OS sullo switch Nexus 92300YC.

NX-OS è un sistema operativo di rete per la serie Nexus di switch Ethernet e la serie MDS di switch Fibre Channel (FC) storage area network forniti da Cisco Systems.

Verifica dei requisiti

Porte e connessioni di nodi supportate

- I collegamenti Inter-Switch (ISL) supportati per gli switch Nexus 92300YC sono le porte 1/65 e 1/66.
- Le connessioni dei nodi supportate per gli switch Nexus 92300YC sono le porte da 1/1 a 1/66.

Di cosa hai bisogno

- Software NetApp Cisco NX-OS applicabile per i tuoi switch dal sito di supporto NetApp, disponibile all'interno del sito ["mysupport.netapp.com"](https://mysupport.netapp.com)
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- ["Pagina switch Ethernet Cisco"](#). Consultare la tabella di compatibilità degli switch per le versioni supportate di ONTAP e NX-OS.

Installare il software

Gli esempi di questa procedura utilizzano due nodi, ma è possibile includere fino a 24 nodi in un cluster.

A proposito degli esempi

Gli esempi di questa procedura utilizzano la seguente nomenclatura di switch e nodi:

- I nomi degli switch Nexus 92300YC sono `cs1` e `cs2`.
- L'esempio utilizzato in questa procedura avvia l'aggiornamento sul secondo switch, `*cs2*`.
- I nomi LIF del cluster sono `node1_clus1` e `node1_clus2` per il `node1`, e `node2_clus1` e `node2_clus2` per il `node2`.
- Il nome IPspace è `Cluster`.
- Il `cluster1: :*>` prompt indica il nome del cluster.
- Le porte del cluster su ciascun nodo sono denominate `e0a` e `e0b`.

Vedere ["Hardware Universe"](#) per le porte cluster effettivamente supportate sulla piattaforma.

Fasi

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare `ping` Comando per verificare la connettività al server che ospita il software NX-OS e RCF.

Mostra esempio

Questo esempio verifica che lo switch possa raggiungere il server all'indirizzo IP 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. Copia il software NX-OS e le immagini EPLD sullo switch Nexus 92300YC.

Mostra esempio

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
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:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.2.2.img /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verificare la versione in esecuzione del software NX-OS:

```
show version
```

Mostra esempio

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, 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 05.31
  NXOS: version 9.2(1)
  BIOS compile time: 05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]

Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

  Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.2(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

5. Installare l'immagine NX-OS.

L'installazione del file immagine ne provoca il caricamento ogni volta che lo switch viene riavviato.

Mostra esempio

```
cs2# install all nxos bootflash:nxos.9.2.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.2.2.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	9.2(1)	
9.2(2)	yes		
1	bios	v05.31(05/17/2018):v05.28(01/18/2018)	
v05.33(09/08/2018)	yes		

```
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
```

```
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:  
Successfully deactivated virtual service 'guestshell+'
```

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

6. Verificare la nuova versione del software NX-OS dopo il riavvio dello switch:

```
show version
```



```
cs2# show version
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, 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 05.33
  NXOS: version 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
```

```
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

Reason: Reset due to upgrade

System version: 9.2(1)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

7. Aggiornare l'immagine EPLD e riavviare lo switch.

Mostra esempio

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	IO FPGA	Successful

1 SUP Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. Dopo il riavvio dello switch, accedere nuovamente e verificare che la nuova versione di EPLD sia stata caricata correttamente.

Mostra esempio

```
cs2# *show version module 1 epld*
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x19
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

Quali sono le prossime novità?

["Installare il file di configurazione di riferimento"](#)

Installazione del file di configurazione di riferimento (RCF)

È possibile installare RCF dopo aver configurato lo switch Nexus 92300YC per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

A proposito di questa attività

Gli esempi di questa procedura utilizzano la seguente nomenclatura di switch e nodi:

- I nomi dei due switch Cisco sono `cs1` e `cs2`.
- I nomi dei nodi sono `node1` e `node2`.
- I nomi LIF del cluster sono `node1_clus1`, `node1_clus2`, `node2_clus1`, e `node2_clus2`.
- Il `cluster1::*>` prompt indica il nome del cluster.



- La procedura richiede l'utilizzo di entrambi i comandi ONTAP e. "[Switch Cisco Nexus serie 9000](#)"; I comandi ONTAP vengono utilizzati se non diversamente indicato.
- Prima di eseguire questa procedura, assicurarsi di disporre di un backup corrente della configurazione dello switch.
- Durante questa procedura non è necessario alcun collegamento interswitch operativo (ISL). Ciò è dovuto alla progettazione, in quanto le modifiche alla versione di RCF possono influire temporaneamente sulla connettività ISL. Per garantire operazioni del cluster senza interruzioni, la seguente procedura esegue la migrazione di tutte le LIF del cluster allo switch del partner operativo durante l'esecuzione delle operazioni sullo switch di destinazione.

Fasi

1. Visualizzare le porte del cluster su ciascun nodo collegato agli switch del cluster: `network device-discovery show`

Mostra esempio

```
cluster1::*> *network device-discovery show*
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface
Platform
-----
node1/cdp
C92300YC   e0a     cs1                      Ethernet1/1/1    N9K-
C92300YC   e0b     cs2                      Ethernet1/1/1    N9K-
node2/cdp
C92300YC   e0a     cs1                      Ethernet1/1/2    N9K-
C92300YC   e0b     cs2                      Ethernet1/1/2    N9K-
cluster1::*>
```

2. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
 - a. Verificare che tutte le porte del cluster siano funzionanti: `network port show -ipspace Cluster`

Mostra esempio

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

Node: node1

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node2

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
healthy false
cluster1::*>
```

- b. Verificare che tutte le interfacce del cluster (LIF) siano sulla porta home: `network interface show -vserver Cluster`

Mostra esempio

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

Current      Logical      Status      Network
Vserver      Current Is
Port         Interface   Admin/Oper  Address/Mask  Node
-----
Cluster
e0c          node1_clus1  up/up      169.254.3.4/23  node1
e0d          node1_clus2  up/up      169.254.3.5/23  node1
e0c          node2_clus1  up/up      169.254.3.8/23  node2
e0d          node2_clus2  up/up      169.254.3.9/23  node2
cluster1::*>
```

- c. Verificare che il cluster visualizzi le informazioni per entrambi gli switch del cluster: `system cluster-switch show -is-monitoring-enabled-operational true`

Mostra esempio

```
cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                                Type                                Address
Model                                -----
-----
cs1                                  cluster-network                    10.233.205.92
N9K-C92300YC
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                9.3(4)
    Version Source: CDP

cs2                                  cluster-network                    10.233.205.93
N9K-C92300YC
    Serial Number: FOXXXXXXXXGD
    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.
```

3. Disattiva l'autorevert sulle LIF del cluster.

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

4. Sullo switch del cluster cs2, spegnere le porte collegate alle porte del cluster dei nodi.

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Verificare che le porte del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi. `network interface show -vserver Cluster`

Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
      Logical      Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      node1_clus1      up/up      169.254.3.4/23      node1
e0c      true
      node1_clus2      up/up      169.254.3.5/23      node1
e0c      false
      node2_clus1      up/up      169.254.3.8/23      node2
e0c      true
      node2_clus2      up/up      169.254.3.9/23      node2
e0c      false
cluster1::*>
```

6. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

```
cluster1::*> *cluster show*
Node      Health      Eligibility      Epsilon
-----
node1      true      true      false
node2      true      true      false
cluster1::*>
```

7. Se non è già stato fatto, salvare una copia della configurazione corrente dello switch copiando l'output del seguente comando in un file di testo:

```
show running-config
```

8. Pulire la configurazione sullo switch cs2 ed eseguire una configurazione di base.



Quando si aggiorna o si applica un nuovo RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. Per configurare nuovamente lo switch, è necessario essere collegati alla porta della console seriale dello switch.

a. Pulire la configurazione:

Mostra esempio

```
(cs2)# write erase
```

Warning: This command will erase the startup-configuration.

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

b. Riavviare lo switch:

Mostra esempio

```
(cs2)# reload
```

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

9. Copiare l'RCF nella flash di avvio dello switch cs2 utilizzando uno dei seguenti protocolli di trasferimento: FTP, TFTP, SFTP o SCP. Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Switch Cisco Nexus serie 9000" guide](#).

Questo esempio mostra l'utilizzo di TFTP per copiare un RCF nella flash di avvio sullo switch cs2:

```
cs2# copy tftp: bootflash: vrf management
```

Enter source filename: **/code/Nexus_92300YC_RCF_v1.0.2.txt**

Enter hostname for the tftp 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:

tftp> **progress**

Progress meter enabled

tftp> **get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin**
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00

tftp> **exit**

Copy complete, now saving to disk (please wait)...

Copy complete.

10. Applicare l'RCF precedentemente scaricato al bootflash.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Switch Cisco Nexus serie 9000" guide](#).

Questo esempio mostra il file RCF Nexus_92300YC_RCF_v1.0.2.txt in fase di installazione sullo switch cs2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands
```

```
Disabling ssh: as its enabled right now:
```

```
generating ecdsa key(521 bits).....
```

```
generated ecdsa key
```

```
Enabling ssh: as it has been disabled
```

```
this command enables edge port type (portfast) by default on all  
interfaces. You
```

```
should now disable edge port type (portfast) explicitly on switched  
ports leading to hubs,
```

```
switches and bridges as they may create temporary bridging loops.
```

```
Edge port type (portfast) should only be enabled on ports connected to a  
single
```

```
host. Connecting hubs, concentrators, switches, bridges, etc... to  
this
```

```
interface when edge port type (portfast) is enabled, can cause  
temporary bridging loops.
```

```
Use with CAUTION
```

```
Edge Port Type (Portfast) has been configured on Ethernet1/1 but will  
only
```

```
have effect when the interface is in a non-trunking mode.
```

```
...
```

```
Copy complete, now saving to disk (please wait)...
```

```
Copy complete.
```

11. Verificare sullo switch che l'RCF sia stato Unito correttamente:

```
show running-config
```

```

cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJlRtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1 - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*

```



Quando si applica RCF per la prima volta, il messaggio **ERROR: Failed to write VSH comands** (ERRORE: Impossibile scrivere i comandi VSH) è previsto e può essere ignorato.

1. verificare che il file RCF sia la versione più recente corretta: `show running-config`

Quando si controlla l'output per verificare che l'RCF sia corretto, assicurarsi che le seguenti informazioni siano corrette:

- Il banner RCF
- Le impostazioni di nodo e porta
- Personalizzazioni

L'output varia in base alla configurazione del sito. Controllare le impostazioni della porta e fare riferimento alle note di rilascio per eventuali modifiche specifiche all'RCF installato.

2. Dopo aver verificato che le versioni RCF e le impostazioni dello switch siano corrette, copiare il file running-config nel file startup-config.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Switch Cisco Nexus serie 9000"](#) guide.

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

3. Riavviare lo switch cs2. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

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

4. Verificare lo stato delle porte del cluster sul cluster.

- a. Verificare che le porte e0d siano in buone condizioni su tutti i nodi del cluster: `network port show -ipspac Cluster`

Mostra esempio

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

Node: node1

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					

Node: node2

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					

- b. Verificare lo stato dello switch dal cluster (potrebbe non essere visualizzato lo switch cs2, poiché le LIF non sono presenti su e0d).

Mostra esempio



```

cluster1::*> *network device-discovery show -protocol cdp*
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/cdp
          e0a    cs1                      Ethernet1/1
N9K-C92300YC
          e0b    cs2                      Ethernet1/1
N9K-C92300YC
node2/cdp
          e0a    cs1                      Ethernet1/2
N9K-C92300YC
          e0b    cs2                      Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch          Type          Address
Model
-----
cs1              cluster-network  10.233.205.90
N9K-C92300YC
    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
N9K-C92300YC
    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.

```


A seconda della versione RCF precedentemente caricata sullo switch, è possibile osservare i seguenti output sulla console dello switch cs1



```
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.
```

5. Sullo switch del cluster cs1, spegnere le porte collegate alle porte del cluster dei nodi.

Nell'esempio seguente viene utilizzato l'output dell'esempio di interfaccia del passo 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

6. Verificare che le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi. `network interface show -vserver Cluster`

Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
      Logical      Status      Network      Current
Current Is
Vserver  Interface      Admin/Oper Address/Mask      Node
Port    Home
-----
Cluster
e0d      node1_clus1      up/up      169.254.3.4/23      node1
false
e0d      node1_clus2      up/up      169.254.3.5/23      node1
true
e0d      node2_clus1      up/up      169.254.3.8/23      node2
false
e0d      node2_clus2      up/up      169.254.3.9/23      node2
true
cluster1::*>
```

7. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-----
node1          true    true         false
node2          true    true         false
cluster1::*>
```

8. Ripetere i passaggi da 7 a 14 sullo switch cs1.
9. Abilitare il ripristino automatico sulle LIF del cluster.

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

10. Riavviare lo switch cs1. Questa operazione consente di attivare le LIF del cluster per ripristinare le porte home. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

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

11. Verificare che le porte dello switch collegate alle porte del cluster siano in funzione.

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1      eth  access up    none
10G(D) --
Ethernet1/2      1      eth  access up    none
10G(D) --
Ethernet1/3      1      eth  trunk  up    none
100G(D) --
Ethernet1/4      1      eth  trunk  up    none
100G(D) --
.
.
```

12. Verificare che l'ISL tra cs1 e cs2 funzioni correttamente: `show port-channel summary`

Mostra esempio

```
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      Eth1/65 (P)  Eth1/66 (P)
cs1#
```

13. Verificare che le LIF del cluster siano tornate alla porta home: `network interface show -vserver Cluster`

Mostra esempio

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

          Logical      Status      Network      Current
Current Is
Vserver   Interface    Admin/Oper  Address/Mask  Node
Port      Home
-----
-----
Cluster
          node1_clus1  up/up      169.254.3.4/23  node1
e0d       true
          node1_clus2  up/up      169.254.3.5/23  node1
e0d       true
          node2_clus1  up/up      169.254.3.8/23  node2
e0d       true
          node2_clus2  up/up      169.254.3.9/23  node2
e0d       true
cluster1::*>
```

14. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

```
cluster1::*> *cluster show*
Node           Health Eligibility  Epsilon
-----
node1          true   true       false
node2          true   true       false
```

15. Eseguire il ping delle interfacce del cluster remoto per verificare la connettività: `cluster ping-cluster -node local`

Mostra esempio

```
cluster1::*> *cluster ping-cluster -node local*
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 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)
```

Per ONTAP 9.8 e versioni successive

Per ONTAP 9.8 e versioni successive, attivare la funzione di raccolta dei log del monitor dello stato dello switch del cluster per la raccolta dei file di log relativi allo switch, utilizzando i comandi seguenti: `system switch ethernet log setup-password` e `system switch ethernet log enable-collection`

Inserire: `system switch ethernet log setup-password`

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

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

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

```
Enter the switch name: cs1
```

```
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>
```

Seguito da: `system switch ethernet log enable-collection`

```
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::*>
```

Per ONTAP 9.4 e versioni successive

Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor di stato dello switch del cluster per la raccolta dei file di log relativi allo switch utilizzando i comandi seguenti:

```
system cluster-switch log setup-password e.system cluster-switch log enable-collection
```

Inserire: `system cluster-switch log setup-password`

```
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>
```

Seguito da: `system cluster-switch log enable-collection`

```
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::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

Raccolta registro monitoraggio stato switch Ethernet

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug. Questa procedura guida l'utente attraverso il processo di impostazione e avvio della raccolta di registri **supporto** dettagliati dal centralino e avvia una raccolta oraria di dati **periodici** raccolti da AutoSupport.

Fasi

1. Per impostare la raccolta di log, eseguire il comando seguente per ogni switch. Viene richiesto di immettere il nome dello switch, il nome utente e la password per la raccolta del registro.

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

Mostra esempio

```
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. Per avviare la raccolta dei log, eseguire il comando seguente, sostituendo DEVICE con lo switch utilizzato nel comando precedente. Questo avvia entrambi i tipi di raccolta di log: I log dettagliati **Support** e una

raccolta oraria di dati **Periodic**.

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

Mostra esempio

```
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.
```

Attendere 10 minuti, quindi verificare che la raccolta dei log sia completa:

```
system switch ethernet log show
```



Se uno di questi comandi restituisce un errore o se la raccolta dei log non viene completata, contattare il supporto NetApp.

Risolvere i problemi

Se si verifica uno dei seguenti stati di errore segnalati dalla funzione di raccolta registri (visibile nell'output di `system switch ethernet log show`), provare i passi di debug corrispondenti:

Stato errore raccolta log	Risoluzione
Chiavi RSA non presenti	Rigenerare le chiavi SSH ONTAP. Contattare l'assistenza NetApp.
errore password cambio	Verificare le credenziali, verificare la connettività SSH e rigenerare le chiavi SSH ONTAP. Consultare la documentazione dello switch o contattare il supporto NetApp per le istruzioni.
Chiavi ECDSA non presenti per FIPS	Se la modalità FIPS è attivata, le chiavi ECDSA devono essere generate sullo switch prima di riprovare.

trovato log preesistente	Rimuovere il file di raccolta del registro precedente sullo switch.
errore registro dump switch	Assicurarsi che l'utente dello switch disponga delle autorizzazioni per la raccolta dei registri. Fare riferimento ai prerequisiti riportati sopra.

Configurare SNMPv3

Seguire questa procedura per configurare SNMPv3, che supporta il monitoraggio dello stato dello switch Ethernet (CSHM).

A proposito di questa attività

I seguenti comandi configurano un nome utente SNMPv3 sugli switch Cisco 92300YC:

- Per **nessuna autenticazione**: `snmp-server user SNMPv3_USER NoAuth`
- Per l'autenticazione **MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Per l'autenticazione **MD5/SHA con crittografia AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
show snmp user
```

Mostra esempio

```
(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. Impostare l'utente SNMPv3 sul lato ONTAP:

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

Mostra esempio

```
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. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

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

Mostra esempio

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C92300YC
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. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

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

Mostra esempio

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C92300YC
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::*>
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.