Wartungsverfahren für MetroCluster IP-Konfigurationen

ONTAP MetroCluster

NetApp
September 06, 2024

Inhalt

Wartungsverfahren für MetroCluster IP-Konfigurationen

Ändern Sie die Eigenschaften einer MetroCluster-IP-Schnittstelle

Ab ONTAP 9.10.1 können Sie die folgenden Eigenschaften einer MetroCluster IP-Schnittstelle ändern: IP-Adresse und -Maske sowie Gateway. Sie können jede beliebige Kombination von Parametern zum Aktualisieren verwenden.

Möglicherweise müssen Sie diese Eigenschaften aktualisieren, z. B. wenn eine doppelte IP-Adresse erkannt wird oder wenn ein Gateway aufgrund von Änderungen der Routerkonfiguration im Fall eines Layer 3-Netzwerks geändert werden muss.

Über diese Aufgabe

- Sie können jeweils nur eine Schnittstelle ändern. Es wird eine Verkehrsunterbrechung auf dieser Schnittstelle geben, bis die anderen Schnittstellen aktualisiert und Verbindungen wiederhergestellt sind.
- Verwenden Sie die `metrocluster configuration-settings interface modify` Befehl zum Ändern einer MetroCluster IP-Schnittstelleneigenschaft.

> Mit diesen Befehlen wird die Konfiguration auf einem bestimmten Node für einen bestimmten Port geändert. Um eine vollständige Netzwerkverbindung wiederherzustellen, sind ähnliche Befehle auf anderen Ports erforderlich. Auf ähnliche Weise müssen Netzwerk-Switches auch ihre Konfiguration aktualisieren. Wenn das Gateway beispielsweise aktualisiert wird, wird idealerweise auf beiden Knoten eines HA-Paares geändert, da sie identisch sind. Außerdem muss der mit diesen Nodes verbundene Switch auch sein Gateway aktualisieren.

- Mit den `metrocluster configuration-settings interface show`Befehlen , `metrocluster connection check`und `metrocluster connection show` können Sie überprüfen, ob alle Verbindungen in allen Schnittstellen funktionieren.

Ändern Sie die IP-Adresse, die Netmask und das Gateway

Führen Sie die folgenden Schritte aus, um die IP-Adresse, die Netzmaske und das Gateway einer MetroCluster IP-Schnittstelle zu ändern.

Schritte

1. Aktualisieren Sie die IP-Adresse, die Netmask und das Gateway für einen einzelnen Node und eine einzelne Schnittstelle: `metrocluster configuration-settings interface modify`

   Mit dem folgenden Befehl wird gezeigt, wie die IP-Adresse, die Netmask und das Gateway aktualisiert werden:

```
cluster_A::* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsi13:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsi14:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsi15:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsi16:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful
```

2. Überprüfen Sie, ob alle Verbindungen für alle Schnittstellen funktionieren: `metrocluster configuration-settings interface show`

   Mit dem folgenden Befehl wird gezeigt, wie Sie überprüfen können, ob alle Verbindungen für alle Schnittstellen funktionieren:

```
cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR              Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.12.201  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.200  255.255.255.0   192.168.20.1
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.12.101  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.101  255.255.255.0   192.168.20.1
completed
      cluster_B node_B_1
                 Home Port: e0a-10
                      192.168.11.151  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.150  255.255.255.0   192.168.21.1
completed
                node_B_2
                 Home Port: e0a-10
                      192.168.11.250  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.250  255.255.255.0   192.168.21.1
completed
8 entries were displayed.
```

3. Überprüfen Sie, ob alle Verbindungen funktionieren:

   `metrocluster configuration-settings connection show`

   Mit dem folgenden Befehl wird gezeigt, wie Sie überprüfen können, ob alle Verbindungen funktionieren:

```
cluster_A::*> metrocluster configuration-settings connection show
  (metrocluster configuration-settings connection show)
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A node_A_2
                  Home Port: e0a-10
                       192.168.10.200  192.168.10.101  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.250  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.151  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.20.100  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.250  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.150  DR Auxiliary
completed
                 node_A_1
                  Home Port: e0a-10
                       192.168.10.101  192.168.10.200  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.151  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.250  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.20.200  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.150  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.250  DR Auxiliary
completed
```

Wartung und Austausch von IP-Switches

Ersetzen Sie einen IP-Switch oder ändern Sie die Verwendung vorhandener MetroCluster IP-Switches

Möglicherweise müssen Sie einen ausgefallenen Switch ersetzen, einen Switch aktualisieren oder herunterstufen oder die Verwendung vorhandener MetroCluster IP-Switches ändern.

Über diese Aufgabe

Dieses Verfahren gilt, wenn Sie NetApp Validated Switches verwenden. Wenn Sie MetroCluster-konforme Switches verwenden, wenden Sie sich an den Switch-Anbieter.

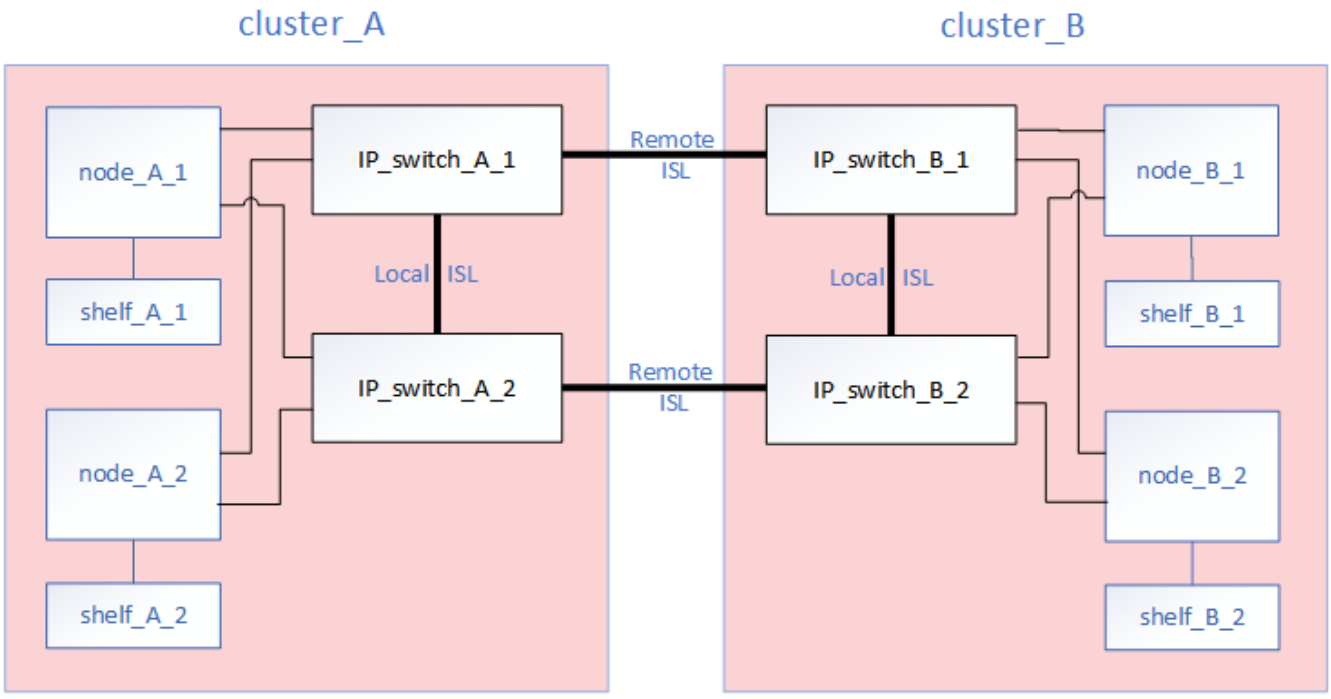
"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Dieses Verfahren unterstützt die folgenden Konvertierungen:

- Ändern des Switch-Anbieters, -Typs oder beider Typen. Der neue Switch kann mit dem alten Schalter identisch sein, wenn ein Switch ausgefallen ist, oder Sie können den Switch-Typ ändern (Upgrade oder Downgrade des Schalters).

  Um beispielsweise eine MetroCluster IP-Konfiguration von einer Konfiguration mit vier Nodes mit AFF A400 Controllern und BES-53248 Switches auf eine Konfiguration mit acht Nodes mit AFF A400 Controllern zu erweitern, müssen Sie die Switches auf einen unterstützten Typ für die Konfiguration ändern, da BES-53248 Switches in der neuen Konfiguration nicht unterstützt werden.

  Wenn Sie einen defekten Switch durch denselben Switch-Typ ersetzen möchten, tauschen Sie nur den ausgefallenen Switch aus. Wenn Sie einen Switch aktualisieren oder herunterstufen möchten, müssen Sie zwei Switches anpassen, die sich im gleichen Netzwerk befinden. Zwei Switches befinden sich im selben Netzwerk, wenn sie mit einer ISL (Inter-Switch Link) verbunden sind und sich nicht am selben Standort befinden. Netzwerk 1 umfasst z. B. IP_Switch_A_1 und IP_Switch_B_1, Netzwerk 2 enthält IP_Switch_A_2 und IP_Switch_B_2, wie in der folgenden Abbildung dargestellt:



Wenn Sie einen Switch ersetzen oder auf verschiedene Switches aktualisieren, können Sie die Switches vorkonfigurieren, indem Sie die Switch-Firmware und die RCF-Datei installieren.

- Konvertieren einer MetroCluster IP-Konfiguration in eine MetroCluster IP-Konfiguration mit MetroCluster-Switches für Shared Storage.

  Wenn Sie beispielsweise über eine regelmäßige MetroCluster IP-Konfiguration mit AFF A700 Controllern verfügen und die MetroCluster neu konfigurieren möchten, um NS224-Shelfs mit denselben Switches zu verbinden.

  - Wenn Sie Shelfs in einer MetroCluster IP-Konfiguration mithilfe von MetroCluster IP-Switches für gemeinsamen Speicher hinzufügen oder entfernen, führen Sie die Schritte in aus "Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von MetroCluster-Switches mit Shared-Storage"
  - Die MetroCluster IP-Konfiguration stellt möglicherweise bereits eine direkte Verbindung zu NS224-Shelfs oder zu dedizierten Storage-Switches her.

Arbeitsblatt zur Portnutzung

Im Folgenden finden Sie ein Beispiel-Arbeitsblatt zum Konvertieren einer MetroCluster IP-Konfiguration in eine Konfiguration mit gemeinsamem Speicher, bei der zwei NS224-Shelfs unter Verwendung der vorhandenen Switches verbunden werden.

Arbeitsblattdefinitionen:

- Vorhandene Konfiguration: Verkabelung der vorhandenen MetroCluster-Konfiguration.
- Neue Konfiguration mit NS224 Shelfs: Die Zielkonfiguration, bei der die Switches zwischen Storage und MetroCluster gemeinsam genutzt werden

Die hervorgehobenen Felder in diesem Arbeitsblatt geben Folgendes an:

- Grün: Sie müssen die Verkabelung nicht ändern.
- Gelb: Sie müssen Ports mit derselben oder einer anderen Konfiguration verschieben.
- Blau: Ports, die neue Verbindungen sind.

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.
   a. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt: **`system health alert show`**

2. Konfigurieren Sie den neuen Switch vor der Installation.

   Wenn Sie vorhandene Switches erneut verwenden, fahren Sie mit fort Schritt 4.

   > Wenn Sie die Switches aktualisieren oder verkleinern, müssen Sie alle Switches im Netzwerk konfigurieren.

   Befolgen Sie die Schritte im Abschnitt *Konfigurieren der IP-Switches* im "Installation und Konfiguration von MetroCluster IP"

   Stellen Sie sicher, dass Sie die korrekte RCF-Datei für den Schalter _A_1, _A_2, _B_1 oder _B_2 anwenden. Wenn der neue Switch mit dem alten Switch identisch ist, müssen Sie dieselbe RCF-Datei anwenden.

   Wenn Sie einen Switch aktualisieren oder herunterstufen, wenden Sie die neueste unterstützte RCF-Datei für den neuen Switch an.

3. Führen Sie den Befehl Port show aus, um Informationen zu den Netzwerkports anzuzeigen:

   `network port show`

   a. Ändern Sie alle Cluster-LIFs, um die automatische Zurücksetzung zu deaktivieren:

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. Trennen Sie die Verbindungen vom alten Switch.

   Sie trennen nur Verbindungen, die nicht denselben Port in der alten und neuen Konfiguration verwenden. Wenn Sie neue Switches verwenden, müssen Sie alle Verbindungen trennen.

   Entfernen Sie die Anschlüsse in der folgenden Reihenfolge:

   a. Trennen Sie die lokalen Cluster-Schnittstellen
   b. Trennen Sie die lokalen Cluster-ISLs
   c. Trennen Sie die MetroCluster IP-Schnittstellen
   d. Trennen Sie die MetroCluster-ISLs

      Im Beispiel [port_usage_worksheet]Die Schalter ändern sich nicht. Die MetroCluster-ISLs werden verschoben und müssen getrennt werden. Sie müssen die grün markierten Verbindungen auf dem Arbeitsblatt nicht trennen.

5. Wenn Sie neue Schalter verwenden, schalten Sie den alten Schalter aus, entfernen Sie die Kabel, und entfernen Sie den alten Schalter.

   Wenn Sie vorhandene Switches erneut verwenden, fahren Sie mit fort Schritt 6.

   Verkabeln Sie die neuen Switches mit Ausnahme der Verwaltungsschnittstelle (falls verwendet) nicht.

6. Konfigurieren Sie die vorhandenen Switches.

   Wenn Sie die Switches bereits vorkonfiguriert haben, können Sie diesen Schritt überspringen.

   Führen Sie zum Konfigurieren der vorhandenen Switches die Schritte zum Installieren und Aktualisieren der Firmware- und RCF-Dateien aus:

   - "Aktualisieren der Firmware auf MetroCluster IP Switches"
   - "Aktualisieren Sie RCF-Dateien auf MetroCluster IP-Switches"

7. Verkabeln Sie die Schalter.

   Sie können die Schritte im Abschnitt *verkabeln der IP-Switches* in befolgen "Installation und Konfiguration von MetroCluster IP".

   Verkabeln Sie die Schalter in der folgenden Reihenfolge (falls erforderlich):

   a. Verkabeln Sie die ISLs mit dem Remote-Standort.
   b. Verkabeln Sie die MetroCluster IP-Schnittstellen.
   c. Verkabeln Sie die lokalen Cluster-Schnittstellen.

- Die verwendeten Ports können von denen auf dem alten Switch abweichen, wenn der Switch-Typ anders ist. Wenn Sie die Switches aktualisieren oder verkleinern, müssen Sie die lokalen ISLs nicht * verkabeln. Verkabeln Sie die lokalen ISLs nur, wenn Sie die Switches im zweiten Netzwerk aktualisieren oder herunterstufen und beide Switches an einem Standort den gleichen Typ und die gleiche Verkabelung aufweisen.
- Wenn Sie Switch-A1 und Switch-B1 aktualisieren, müssen Sie die Schritte 1 bis 6 für Schalter A2 und Switch-B2 ausführen.

8. Schließen Sie die lokale Clusterverkabelung ab.
   a. Wenn die lokalen Cluster-Schnittstellen mit einem Switch verbunden sind:
      i. Verkabeln Sie die lokalen Cluster-ISLs.
   b. Wenn die lokalen Clusterschnittstellen **nicht** mit einem Switch verbunden sind:
      i. Verwenden Sie die "Migration zu einer NetApp Cluster-Umgebung mit Switch" Vorgehensweise zum Konvertieren eines Clusters ohne Switches in ein Cluster mit Switches. Verwenden Sie die in angegebenen Anschlüsse "Installation und Konfiguration von MetroCluster IP" Oder die RCF-Verkabelungsdateien, um die lokale Clusterschnittstelle zu verbinden.
9. Schalten Sie den Schalter ein oder schalten Sie den Schalter ein.

   Wenn der neue Schalter gleich ist, schalten Sie den neuen Schalter ein. Wenn Sie die Schalter aktualisieren oder verkleinern, schalten Sie beide Schalter ein. Die Konfiguration kann mit zwei verschiedenen Switches an jedem Standort betrieben werden, bis das zweite Netzwerk aktualisiert wird.
10. Wiederholen Sie die Schritte, um zu überprüfen, ob die MetroCluster-Konfiguration ordnungsgemäß ist Schritt 1.

    Wenn Sie die Switches im ersten Netzwerk aktualisieren oder verkleinern, werden möglicherweise einige Warnmeldungen im Zusammenhang mit dem lokalen Clustering angezeigt.

    Wenn Sie die Netzwerke aktualisieren oder herunterstufen, dann wiederholen Sie alle Schritte für das zweite Netzwerk.
11. Ändern Sie alle Cluster-LIFs, um die automatische Zurücksetzung erneut zu aktivieren:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. Verschieben Sie optional die NS224-Shelfs.

    Wenn Sie eine MetroCluster IP-Konfiguration neu konfigurieren, bei der keine NS224-Shelfs mit den MetroCluster IP-Switches verbunden werden, gehen Sie wie folgt vor, um die NS224-Shelfs hinzuzufügen oder zu verschieben:

    - "Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von MetroCluster-Switches mit Shared-Storage"
    - "Migrieren Sie von einem Cluster ohne Switches mit Direct-Attached Storage"
    - "Migrieren Sie mit der erneuten Nutzung der Storage-Switches von einer Konfiguration ohne Switches mit Switch-Attached Storage"

Online- oder Offline-Ports der MetroCluster IP-Schnittstelle

Wenn Sie Wartungsaufgaben durchführen, müssen Sie möglicherweise einen MetroCluster IP-Schnittstellenport offline oder online schalten.

Über diese Aufgabe

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

Sie können die folgenden Schritte durchführen, um einen MetroCluster-IP-Schnittstellen-Port online zu schalten oder in den Offline-Modus zu versetzen.

1. Legen Sie die Berechtigungsebene auf erweitert fest.

```
set -privilege advanced
```

Beispielausgabe

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. Versetzen Sie den Port der MetroCluster IP-Schnittstelle in den Offline-Modus.

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

   a. Überprüfen Sie, ob die MetroCluster-IP-Schnittstelle offline ist.

```
Cluster_A1::*> system ha interconnect port show
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  disabled  down              4          3
false
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

3. Versetzen Sie den MetroCluster IP-Schnittstellenport in den Online-Modus.

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. Überprüfen Sie, ob der Port der MetroCluster IP-Schnittstelle online ist.

```
Cluster_A1::*> system ha interconnect port show
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  linkup    active            5          3
true
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

Aktualisieren der Firmware auf MetroCluster IP Switches

Möglicherweise müssen Sie die Firmware auf einem MetroCluster IP Switch aktualisieren.

Über diese Aufgabe

Sie müssen diese Aufgabe nacheinander an jedem der Schalter wiederholen.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist:

      ```
      metrocluster show
      ```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind:

`metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

a. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Installieren Sie die Software auf dem ersten Switch.

> Sie müssen die Switch-Software auf den Switches in der folgenden Reihenfolge installieren: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

Befolgen Sie die Schritte zum Installieren der Switch-Software im entsprechenden Thema, je nachdem, ob der Switch-Typ Broadcom, Cisco oder NVIDIA ist:

- "Laden Sie die Broadcom-Switch-EFOS-Software herunter, und installieren Sie sie"
- "Laden Sie die Cisco Switch NX-OS-Software herunter, und installieren Sie sie"
- "Laden Sie die NVIDIA SN2100 Switch Cumulus Software herunter und installieren Sie sie"

3. Wiederholen Sie den vorherigen Schritt für jeden der Schalter.
4. Wiederholen Schritt 1 Um den Zustand der Konfiguration zu überprüfen.

Aktualisieren Sie RCF-Dateien auf MetroCluster IP-Switches

Möglicherweise müssen Sie eine RCF-Datei auf einem MetroCluster IP-Switch aktualisieren. Wenn beispielsweise die RCF-Dateiversion, die Sie auf den Switches ausführen, nicht von der ONTAP-Version, der Switch-Firmware-Version oder beiden unterstützt wird.

Stellen Sie sicher, dass die RCF-Datei unterstützt wird

Wenn Sie die ONTAP-Version oder die Switch-Firmware-Version ändern, sollten Sie überprüfen, ob eine RCF-

Datei vorhanden ist, die für diese Version unterstützt wird. Wenn Sie den RCF-Generator verwenden, wird für Sie die richtige RCF-Datei generiert.

Schritte

1. Verwenden Sie die folgenden Befehle der Schalter, um die Version der RCF-Datei zu überprüfen:

Von diesem Schalter…	Geben Sie diesen Befehl aus…
Broadcom-Switch	`(IP_switch_A_1) # show clibanner`
Cisco Switch	`IP_switch_A_1# show banner motd`

   Suchen Sie bei jedem Switch die Zeile in der Ausgabe, die die Version der RCF-Datei anzeigt. Die folgende Ausgabe ist beispielsweise von einem Cisco-Switch, der angibt, dass die RCF-Dateiversion „`v1.80`“ ist.

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Um zu überprüfen, welche Dateien für eine bestimmte ONTAP-Version, einen Switch und eine bestimmte Plattform unterstützt werden, verwenden Sie den RCfFileGenerator. Wenn Sie die RCF-Datei für die Konfiguration generieren können, die Sie haben oder auf die Sie aktualisieren möchten, wird sie unterstützt.
3. Um sicherzustellen, dass die Switch-Firmware unterstützt wird, lesen Sie bitte die folgenden Informationen:
   - "Hardware Universe"
   - "NetApp Interoperabilitätsmatrix"

RCF-Dateien aktualisieren

Wenn Sie neue Switch-Firmware installieren, müssen Sie die Switch-Firmware installieren, bevor Sie die RCF-Datei aktualisieren.

Über diese Aufgabe

- Dieses Verfahren unterbricht den Datenverkehr auf dem Switch, auf dem die RCF-Datei aktualisiert wird. Der Datenverkehr wird wieder aufgenommen, sobald die neue RCF-Datei angewendet wurde.
- Führen Sie die Schritte jeweils an einem Schalter in der folgenden Reihenfolge aus: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführung `metrocluster check show` Um die Ergebnisse anzuzeigen.

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id 38
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

Befolgen Sie die Schritte für Ihren Switch-Anbieter:

- "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
- "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
- "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"

3. Laden Sie je nach Switch-Anbieter die IP RCF-Datei herunter, und installieren Sie sie.
   - "Laden Sie die Broadcom IP RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die Cisco IP RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die NVIDIA IP RCF-Dateien herunter, und installieren Sie sie"

> Wenn Sie über eine freigegebene L2- oder L3-Netzwerkkonfiguration verfügen, müssen Sie möglicherweise die ISL-Ports an den Zwischen-/Kunden-Switches anpassen. Der Switchport-Modus kann von „Access“ auf „Trunk“ geändert werden. Fahren Sie nur mit dem Upgrade des zweiten Switch-Paares (A_2, B_2) fort, wenn die Netzwerkverbindung zwischen den Switches A_1 und B_1 voll funktionsfähig ist und das Netzwerk ordnungsgemäß ist.

Aktualisieren Sie RCF-Dateien auf Cisco IP-Switches mithilfe von CleanUpFiles

Möglicherweise müssen Sie eine RCF-Datei auf einem Cisco IP-Switch aktualisieren. Beispielsweise ist für ein ONTAP Upgrade oder ein Switch-Firmware-Upgrade eine neue RCF-Datei erforderlich.

Über diese Aufgabe

- Ab der Version 1.4a von RcfFileGenerator gibt es eine neue Option, die Switch-Konfiguration auf Cisco IP-Switches zu ändern (Upgrade, Downgrade oder Ersetzen), ohne dass eine 'Schreiblöschung' durchgeführt werden muss.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.
- Der Cisco 9336C-FX2 Switch verfügt über zwei verschiedene Switch-Speichertypen, die im RCF unterschiedlich benannt sind. Verwenden Sie die folgende Tabelle, um den richtigen Cisco 9336C-FX2-Speichertyp für Ihre Konfiguration zu ermitteln:

Wenn Sie den folgenden Speicher verbinden…	Wählen Sie den Cisco 9336C-FX2-Speichertyp…	Beispiel für RCF-Dateibanner/MOTD
• Direkt verbundene SAS-Shelfs • Direkt verbundene NVMe-Shelfs • NVMe-Shelfs, die mit dedizierten Storage-Switches verbunden sind	9336C-FX2 – nur Direct Storage	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• Direkt verbundene SAS-Shelfs • Mit den MetroCluster IP-Switches verbundene NVMe Shelfs ⓘ Es ist mindestens ein Ethernet-angeschlossenes NVMe-Shelf erforderlich	9336C-FX2 – SAS- und Ethernet-Speicher	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

Bevor Sie beginnen

Sie können diese Methode verwenden, wenn Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Es wird die Standard-RCF-Konfiguration angewendet.
- Der "RCfFileGenerator" Muss in der Lage sein, dieselbe RCF-Datei zu erstellen, die angewendet wird, und zwar mit derselben Version und Konfiguration (Plattformen, VLANs).
- Die angewandte RCF-Datei wurde von NetApp nicht für eine spezielle Konfiguration zur Verfügung gestellt.
- Die RCF-Datei wurde vor der Anwendung nicht geändert.
- Die Schritte zum Zurücksetzen des Switches auf die Werkseinstellungen wurden vor dem Anwenden der

aktuellen RCF-Datei befolgt.

- Nach der Anwendung des RCF wurden an der Switch(Port)-Konfiguration keine Änderungen vorgenommen.

Wenn Sie diese Anforderungen nicht erfüllen, können Sie die CleanUpFiles, die beim Erstellen der RCF-Dateien erstellt wurden, nicht verwenden. Sie können jedoch die Funktion nutzen, um generische CleanUpFiles zu erstellen — die Bereinigung mit dieser Methode ist aus der Ausgabe von abgeleitet `show running-config` Und ist die Best Practice.

> Sie müssen die Switches in folgender Reihenfolge aktualisieren: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. Oder Sie können die Schalter Switch_A_1 und Switch_B_1 gleichzeitig aktualisieren, gefolgt von den Schaltern Switch_A_2 und Switch_B_2.

Schritte

1. Legen Sie die aktuelle RCF-Dateiversion fest, welche Ports und VLANs verwendet werden:
   `IP_switch_A_1# show banner motd`

> Sie müssen diese Informationen von allen vier Switches erhalten und die folgende Informationstabelle ausfüllen.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*

#
IP_switch_A_1#
```

In dieser Ausgabe müssen Sie die in den folgenden beiden Tabellen aufgeführten Informationen erfassen.

Allgemeine Informationen	MetroCluster	Daten
RCF-Dateiversion		1.81
Switch-Typ		NX9336
Netzwerktypologie		L2-Netzwerke, direkte ISL
Storage-Typ		SAS-Storage
Plattformen	1	AFF A400
	2	FAS9000

VLAN-Informationen	Netzwerk	MetroCluster-Konfiguration	Switchports	Standort A	Standort B
VLAN lokaler Cluster	Netzwerk 1	1	1, 2	111	222
		2	3, 4	151	251
	Netzwerk 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN-MetroCluster	Netzwerk 1	1	9, 10	119	119
		2	11, 12	159	159
	Netzwerk 2	1	9, 10	219	219
		2	11, 12	259	259

2. [[Create-RCF-files-and-CleanUpFiles-or-create-generic-CleanUp Files] Erstellen Sie die RCF-Dateien und CleanUpFiles oder erstellen Sie allgemeine CleanUpFiles für die aktuelle Konfiguration.

   Wenn Ihre Konfiguration die in den Voraussetzungen beschriebenen Anforderungen erfüllt, wählen Sie **Option 1**. Wenn Ihre Konfiguration die in den Voraussetzungen beschriebenen Anforderungen nicht erfüllt, wählen Sie **Option 2**.

Option 1: Erstellen Sie die RCF-Dateien und CleanUpFiles

Gehen Sie folgendermaßen vor, wenn die Konfiguration den Anforderungen entspricht.

Schritte

a. Verwenden Sie den RCfFileGenerator 1.4a (oder höher), um die RCF-Dateien mit den Informationen zu erstellen, die Sie in Schritt 1 abgerufen haben. Die neue Version des RcfFileGenerators erstellt einen zusätzlichen Satz von CleanUpFiles, mit denen Sie einige Konfigurationen zurücksetzen und den Switch vorbereiten können, um eine neue RCF-Konfiguration anzuwenden.

b. Vergleichen Sie das Banner motd mit den derzeit verwendeten RCF-Dateien. Die Plattformtypen, der Switch-Typ, die Port- und die VLAN-Nutzung müssen identisch sein.

Sie müssen die CleanUpFiles aus derselben Version wie die RCF-Datei und für die exakt gleiche Konfiguration verwenden. Die Verwendung von CleanUpFile funktioniert nicht und erfordert möglicherweise ein vollständiges Zurücksetzen des Switches.

Die ONTAP-Version, für die die RCF-Datei erstellt wurde, ist nicht relevant. Es ist nur die RCF-Dateiversion wichtig.

Die RCF-Datei (auch die gleiche Version ist) könnte weniger oder mehr Plattformen auflisten. Stellen Sie sicher, dass Ihre Plattform aufgeführt ist.

Option 2: Erstellen Sie allgemeine CleanUpFiles

Gehen Sie folgendermaßen vor, wenn die Konfiguration nicht alle Anforderungen erfüllt.

Schritte

a. Abrufen der Ausgabe von `show running-config` Von jedem Schalter.

b. Öffnen Sie das RcfFileGenerator-Tool und klicken Sie unten im Fenster auf 'Generic CleanUpFiles erstellen'

c. Kopieren Sie die Ausgabe, die Sie in Schritt 1 von „One“-Schalter in das obere Fenster abgerufen haben. Sie können die Standardausgabe entfernen oder belassen.

d. Klicken Sie auf „CUF-Dateien erstellen“.

e. Kopieren Sie die Ausgabe aus dem unteren Fenster in eine Textdatei (diese Datei ist die CleanUpFile).

f. Wiederholen Sie die Schritte c, d und e für alle Schalter in der Konfiguration.

Am Ende dieses Verfahrens sollten Sie vier Textdateien haben, eine für jeden Switch. Sie können diese Dateien auf die gleiche Weise wie die CleanUpFiles verwenden, die Sie mit Option 1 erstellen können.

3. Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration. Erstellen Sie diese Dateien auf die gleiche Weise, wie Sie die Dateien im vorherigen Schritt erstellt haben, außer wählen Sie die entsprechende ONTAP und RCF-Dateiversion.

Nach Abschluss dieses Schritts sollten Sie zwei Sätze RCF-Dateien haben, die jeweils aus zwölf Dateien

bestehen.

4. Laden Sie die Dateien auf den Bootflash herunter.

   a. Laden Sie die CleanUpFiles herunter, die Sie in erstellt haben Erstellen Sie die RCF-Dateien und CleanUpFiles oder erstellen Sie allgemeine CleanUpFiles für die aktuelle Konfiguration

      Diese CleanUpFile ist für die aktuelle RCF-Datei, die angewendet wird und **NICHT** für die neue RCF, auf die Sie aktualisieren möchten.

      Beispiel CleanUpFile für Switch-A1: `Cleanup_NX9336_v1.81_Switch-A1.txt`

   b. Laden Sie die neuen RCF-Dateien herunter, die Sie in erstellt haben Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration.

      Beispiel für RCF-Datei für Switch-A1: `NX9336_v1.90_Switch-A1.txt`

   c. Laden Sie die CleanUpFiles herunter, die Sie in erstellt haben Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration. Dieser Schritt ist optional — Sie können die Datei in Zukunft verwenden, um die Switch-Konfiguration zu aktualisieren. Es stimmt mit der aktuell verwendeten Konfiguration überein.

      Beispiel CleanUpFile für Switch-A1: `Cleanup_NX9336_v1.90_Switch-A1.txt`

      Sie müssen die CleanUpFile für die korrekte (passende) RCF-Version verwenden. Wenn Sie eine CleanUpFile für eine andere RCF-Version oder eine andere Konfiguration verwenden, funktioniert die Bereinigung der Konfiguration möglicherweise nicht richtig.

      Im folgenden Beispiel werden die drei Dateien auf den Bootflash kopiert:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

   +

      Sie werden aufgefordert, Virtual Routing und Forwarding (VRF) anzugeben.

5. Übernehmen Sie die CleanUpFile- oder die allgemeine CleanUpFile-Datei.

   Einige der Konfigurationen werden zurückgesetzt und die Switchports gehen „offline“.

a. Vergewissern Sie sich, dass keine ausstehenden Änderungen an der Startkonfiguration vorliegen: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Wenn Sie die Systemausgabe sehen, speichern Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

> Die Systemausgabe zeigt an, dass die Startkonfiguration und die laufende Konfiguration unterschiedlich und ausstehende Änderungen sind. Wenn Sie die ausstehenden Änderungen nicht speichern, können Sie den Switch nicht erneut laden.

a. Anwenden der CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

> Das Skript kann eine Weile dauern, bis es zur Switch-Eingabeaufforderung zurückkehrt. Es wird keine Ausgabe erwartet.

7. Zeigen Sie die laufende Konfiguration an, um zu überprüfen, ob die Konfiguration gelöscht wurde: `show running-config`

   Die aktuelle Konfiguration sollte Folgendes zeigen:

   - Es sind keine Klassenkarten und IP-Zugriffslisten konfiguriert
   - Es wurden keine Richtlinienzuordnungen konfiguriert
   - Es sind keine Service-Richtlinien konfiguriert
   - Es werden keine Port-Profile konfiguriert
   - Alle Ethernet-Schnittstellen (außer mgmt0 die keine Konfiguration zeigen sollten, und nur VLAN 1 sollte konfiguriert sein).

     Wenn Sie feststellen, dass eines der oben genannten Elemente konfiguriert ist, können Sie möglicherweise keine neue RCF-Dateikonfiguration anwenden. Sie können jedoch auf die vorherige Konfiguration zurücksetzen, indem Sie den Switch *neu laden, ohne die laufende Konfiguration in die Startkonfiguration zu speichern. Der Switch verfügt über die vorherige Konfiguration.

8. Wenden Sie die RCF-Datei an und stellen Sie sicher, dass die Ports online sind.

   a. Wenden Sie die RCF-Dateien an.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

Beim Anwenden der Konfiguration werden einige Warnmeldungen angezeigt. Fehlermeldungen werden in der Regel nicht erwartet. Wenn Sie jedoch mit SSH angemeldet sind, wird möglicherweise die folgende Fehlermeldung angezeigt: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. Überprüfen Sie nach der Anwendung der Konfiguration, ob die Cluster- und MetroCluster-Ports mit einem der folgenden Befehle online geschaltet werden: `show interface brief`, `show cdp neighbors`, Oder `show lldp neighbors`

Wenn Sie das VLAN für den lokalen Cluster geändert haben und Sie den ersten Switch am Standort aktualisiert haben, wird der Zustand der Cluster-Zustandsüberwachung möglicherweise nicht als „stabil“ angegeben, da die VLANs der alten und der neuen Konfigurationen nicht übereinstimmen. Nach der Aktualisierung des zweiten Schalters sollte der Status wieder in den Status „gesund“ zurückkehren.

Wenn die Konfiguration nicht korrekt angewendet wird oder Sie die Konfiguration nicht beibehalten möchten, können Sie die vorherige Konfiguration wiederherstellen, indem Sie den Switch wieder laden **ohne** die laufende Konfiguration in die Startkonfiguration zu speichern. Der Switch verfügt über die vorherige Konfiguration.

9. Speichern Sie die Konfiguration, und laden Sie den Schalter neu.

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Umbenennen eines Cisco IP-Switches

Möglicherweise müssen Sie einen Cisco IP-Switch umbenennen, um während der Konfiguration eine konsistente Benennung zu ermöglichen.

Über diese Aufgabe

- In den Beispielen in dieser Aufgabe wird der Switch-Name von geändert `myswitch` Bis `IP_switch_A_1`.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   Im folgenden Beispiel wird die Eingabeaufforderung für den Konfigurationsmodus angezeigt. In beiden Eingabeaufforderungen wird der Switch-Name von angezeigt `myswitch`.

```
myswitch# configure terminal
myswitch(config)#
```

2. Umbenennung des Switches:

   `switchname new-switch-name`

   Wenn Sie beide Switches in der Fabric umbenennen, verwenden Sie auf jedem Switch den gleichen Befehl.

   Die CLI-Eingabeaufforderung wird geändert, um den neuen Namen wiederzugeben:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Konfigurationsmodus beenden:

   `exit`

   Die Eingabeaufforderung für den Schalter auf oberster Ebene wird angezeigt:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Kopieren der aktuellen Konfiguration in die Startkonfigurationsdatei:

   `copy running-config startup-config`

5. Vergewissern Sie sich, dass die Änderung des Switch-Namens von der ONTAP-Cluster-Eingabeaufforderung aus sichtbar ist.

   Beachten Sie, dass der neue Switch-Name und der alte Switch-Name angezeigt werden (`myswitch`) Erscheint nicht.

   a. Rufen Sie den erweiterten Berechtigungsmodus auf, und drücken Sie **`y`** Wenn Sie dazu aufgefordert werden:
      `set -privilege advanced`

   b. Anzeige der angeschlossenen Geräte:
      `network device-discovery show`

   c. Zurück zum Admin-Berechtigungsmodus:
      `set -privilege admin`

      Das folgende Beispiel zeigt, dass der Schalter mit dem neuen Namen angezeigt wird. `IP_switch_A_1`:

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Unterbrechungsfreies Hinzufügen, Entfernen oder Ändern von ISL-Ports auf Cisco IP-Switches

Möglicherweise müssen Sie ISL-Ports bei Cisco IP-Switches hinzufügen, entfernen oder ändern. Sie können dedizierte ISL-Ports in gemeinsame ISL-Ports konvertieren oder die Geschwindigkeit von ISL-Ports auf einem Cisco IP-Switch ändern.

Über diese Aufgabe

Wenn Sie dedizierte ISL-Ports in gemeinsam genutzte ISL-Ports konvertieren, stellen Sie sicher, dass die neuen Ports den entsprechen "Voraussetzungen für gemeinsam genutzte ISL-Ports".

Um die ISL-Konnektivität sicherzustellen, müssen Sie alle Schritte auf beiden Switches ausführen.

Im folgenden Verfahren wird vorausgesetzt, dass Sie eine 10-GB-ISL, die am Switch-Port eth1/24/1 angeschlossen ist, durch zwei 100-GB-ISLs ersetzen, die mit den Switch-Ports 17 und 18 verbunden sind.

> Wenn Sie einen Cisco 9336C-FX2-Switch in einer gemeinsam genutzten Konfiguration verwenden, die NS224-Shelfs verbindet, erfordert das Ändern der ISLs möglicherweise eine neue RCF-Datei. Sie benötigen keine neue RCF-Datei, wenn Ihre aktuelle und neue ISL-Geschwindigkeit 40 Gbit/s und 100 Gbit/s beträgt. Für alle anderen Änderungen an der ISL-Geschwindigkeit ist eine neue RCF-Datei erforderlich. Wenn Sie beispielsweise die ISL-Geschwindigkeit von 40 Gbit/s auf 100 Gbit/s ändern, ist keine neue RCF-Datei erforderlich, aber wenn Sie die ISL-Geschwindigkeit von 10 Gbit/s auf 40 Gbit/s ändern, ist eine neue RCF-Datei erforderlich.

Bevor Sie beginnen

Weitere Informationen finden Sie im Abschnitt **Schalter** des "NetApp Hardware Universe" Überprüfen der unterstützten Transceiver.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Deaktivieren Sie die ISL-Ports der ISLs auf beiden Switches in der Fabric, die Sie ändern möchten.

   > Die aktuellen ISL-Ports müssen nur deaktiviert werden, wenn sie zu einem anderen Port verschoben werden oder sich die Geschwindigkeit der ISL ändert. Wenn Sie einen ISL-Port mit derselben Geschwindigkeit wie die vorhandenen ISLs hinzufügen, fahren Sie mit Schritt 3 fort.

   Sie müssen nur einen Konfigurationsbefehl für jede Zeile eingeben und Strg-Z drücken, nachdem Sie alle Befehle eingegeben haben, wie im folgenden Beispiel dargestellt:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#
```

2. Entfernen Sie die vorhandenen Kabel und Transceiver.
3. Ändern Sie den ISL-Port nach Bedarf.

> Wenn Sie Cisco 9336C-FX2-Switches in einer gemeinsam genutzten Konfiguration verwenden, die NS224-Shelfs verbindet, und Sie die RCF-Datei aktualisieren und die neue Konfiguration für die neuen ISL-Ports anwenden müssen, befolgen Sie die Schritte unter "Aktualisieren Sie die RCF-Dateien auf MetroCluster IP-Switches."

Option	Schritt
So ändern Sie die Geschwindigkeit eines ISL-Ports:	Verkabeln Sie die neuen ISLs entsprechend ihrer Geschwindigkeit an die entsprechenden Ports. Sie müssen sicherstellen, dass diese ISL-Ports für Ihren Switch in der *MetroCluster IP Installation and Configuration* aufgeführt sind.
ISL hinzufügen…	Fügen Sie QFSPs in die Ports ein, die Sie als ISL-Ports hinzufügen. Stellen Sie sicher, dass sie in der *MetroCluster IP-Installation und -Konfiguration* aufgeführt sind und verkabeln Sie sie entsprechend.

4. Aktivieren Sie alle ISL-Ports (falls nicht aktiviert) auf beiden Switches in der Fabric und beginnen Sie mit dem folgenden Befehl:

```
switch_A_1# conf t
```

Sie müssen nur einen Konfigurationsbefehl pro Zeile eingeben und Strg-Z drücken, nachdem Sie alle Befehle eingegeben haben:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Überprüfen Sie, ob die ISLs und Port-Kanäle für die ISLs zwischen beiden Switches eingerichtet sind:

   ```
   switch_A_1# show int brief
   ```

   Die ISL-Schnittstellen in der Befehlsausgabe sollten wie im folgenden Beispiel gezeigt werden:

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. Wiederholen Sie das Verfahren für Stoff 2.

Identifizierung des Storage in einer MetroCluster IP-Konfiguration

Wenn Sie ein Laufwerk- oder Shelf-Modul ersetzen müssen, müssen Sie zunächst den Standort identifizieren.

Identifizierung lokaler und Remote-Shelfs

Wenn Sie Shelf-Informationen von einem MetroCluster-Standort aus anzeigen, befinden sich alle Remote-Laufwerke auf 0 m, dem virtuellen iSCSI-Host-Adapter. Das bedeutet, dass über die MetroCluster IP Schnittstellen auf die Laufwerke zugegriffen wird. Alle anderen Laufwerke sind lokal.

Nachdem Sie erkannt haben, ob ein Shelf Remote ist (auf 0m), können Sie das Laufwerk oder Shelf nach der Seriennummer oder, abhängig von den Shelf-ID-Zuordnungen in Ihrer Konfiguration, nach Shelf-ID identifizieren.

Bei MetroCluster IP-Konfigurationen mit ONTAP 9.4 muss die Shelf-ID nicht zwischen den MetroCluster Standorten eindeutig sein. Hierzu zählen sowohl interne als auch externe Shelfs. Die Seriennummer ist konsistent, wenn sie von einem beliebigen Node auf einem MetroCluster Standort aus angezeigt wird.

Shelf-IDs sollten innerhalb der Disaster Recovery-Gruppe (DR) eindeutig sein, außer im internen Shelf.

Wenn das Laufwerk- oder Shelf-Modul identifiziert wurde, können Sie die Komponente durch das entsprechende Verfahren ersetzen.

"Aufrechterhaltung der Festplatten-Shelfs DS460C DS224C und DS212C"

Beispiel einer Ausgabe von sysconfig -a

Im folgenden Beispiel wird das verwendet `sysconfig -a` Befehl zum Anzeigen der Geräte auf einem Knoten in der MetroCluster IP-Konfiguration. Dieser Node ist mit den folgenden Shelfs und Geräten verbunden:

- Steckplatz 0: Interne Laufwerke (lokale Laufwerke)
- Steckplatz 3: Externe Shelf-ID 75 und 76 (lokale Laufwerke)
- Steckplatz 0: Virtueller iSCSI-Host-Adapter 0 m (Remote-Laufwerke)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
```

```
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
```

```
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von Shared Storage MetroCluster Switches

Möglicherweise müssen Sie einem MetroCluster NS224-Shelfs mit Shared-Storage-MetroCluster-Switches hinzufügen.

Ab ONTAP 9.10.1 können Sie NS224-Shelfs von einem MetroCluster aus mithilfe der Shared Storage-/MetroCluster-Switches hinzufügen. Sie können mehrere Shelfs gleichzeitig hinzufügen.

Bevor Sie beginnen

- Nodes müssen ONTAP 9.9.1 oder höher ausführen.
- Alle derzeit verbundenen NS224-Shelfs müssen mit den gleichen Switches verbunden sein wie die MetroCluster (Konfiguration für Shared Storage/MetroCluster-Switches).
- Mit diesem Verfahren können Konfigurationen nicht mit direkt verbundenen NS224-Shelfs oder mit dedizierten Ethernet-Switches verbundenen NS224-Shelfs in eine Konfiguration mit Shared Storage/MetroCluster-Switches umgewandelt werden.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport

Meldung, damit das Upgrade ausgeführt wird.

a. Geben Sie den folgenden Befehl ein:

```
system node autosupport invoke -node * -type all -message "Maint=10h Adding
or Removing NS224 shelves"_
```

Dieses Beispiel gibt ein Wartungsfenster von 10 Stunden an. Je nach Plan sollten Sie möglicherweise zusätzliche Zeit einplanen.

Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

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

a. Wiederholen Sie den Befehl im Partner-Cluster.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie müssen den Zustand und die Konnektivität der MetroCluster Konfiguration vor der Durchführung der Transition überprüfen.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

```
node run -node node-name sysconfig -a
```

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

```
system health alert show
```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

   d. Durchführen einer MetroCluster-Prüfung:

```
metrocluster check run
```

   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

   f. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

   g. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.
2. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

3. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

   `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  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: node_A_2-old

                                                  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

4 entries were displayed.

cluster_A::>
```

4. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

   `network interface show -vserver Cluster`

   Jede Cluster-LIF sollte True für IS Home anzeigen und einen Status Admin/Oper von up/Up haben

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Vergewissern Sie sich, dass die automatische Umrüstung auf allen Cluster-LIFs aktiviert ist:

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

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Anwenden der neuen RCF-Datei auf die Switches

Wenn Ihr Switch bereits richtig konfiguriert ist, können Sie diese nächsten Abschnitte überspringen und direkt zu gehen Konfiguration der MACsec-Verschlüsselung bei Cisco 9336C-Switches, Sofern zutreffend oder für Anschließen des neuen NS224-Regals.

- Sie müssen die Switch-Konfiguration ändern, um Shelfs hinzuzufügen.
- Sie sollten sich die Details zur Verkabelung unter ansehen "Zuweisung von Plattform-Ports".
- Sie müssen das **RcfFileGenerator**-Tool verwenden, um die RCF-Datei für Ihre Konfiguration zu erstellen. Der "RCfFileGenerator" Bietet außerdem eine Übersicht über die Verkabelung pro Port für jeden Switch. Stellen Sie sicher, dass Sie die richtige Anzahl an Shelves auswählen. Es gibt zusätzliche Dateien, die zusammen mit der RCF-Datei erstellt werden, die ein detailliertes Verkabelungslayout bieten, das Ihren spezifischen Optionen entspricht. Mithilfe dieser Verkabelungsübersicht können Sie bei der Verkabelung der neuen Shelves Ihre Verkabelung überprüfen.

Aktualisieren von RCF-Dateien auf MetroCluster IP-Switches

Wenn Sie neue Switch-Firmware installieren, müssen Sie die Switch-Firmware installieren, bevor Sie die RCF-Datei aktualisieren.

Dieses Verfahren unterbricht den Datenverkehr auf dem Switch, auf dem die RCF-Datei aktualisiert wird. Der Datenverkehr wird wieder aufgenommen, sobald die neue RCF-Datei angewendet wurde.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

    a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

metrocluster check run

```
cluster_A::*> metrocluster check run
```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführung `metrocluster check show` Um die Ergebnisse anzuzeigen.

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Um den Status des laufenden MetroCluster-Prüfvorgangs zu überprüfen, verwenden Sie den Befehl: **metrocluster operation history show -job-id 38**

b. Stellen Sie sicher, dass es keine Zustandswarnmeldungen gibt: **system health alert show**

2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen

Bevor Sie eine neue Softwareversion und RCFs installieren, müssen Sie die Cisco Switch-Konfiguration löschen und eine grundlegende Konfiguration durchführen.

Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

a. Löschen Sie die vorhandene Konfiguration: `write erase`

b. Laden Sie die Switch-Software neu: `reload`

Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung Auto Provisioning abbrechen und mit der normalen Einrichtung fortfahren?(ja/nein)[n], sollten Sie antworten `yes` Fortfahren.

c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:
   - Admin-Passwort
   - Switch-Name
   - Out-of-Band-Managementkonfiguration
   - Standard-Gateway
   - SSH-Service (RSA) nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

   Das folgende Beispiel zeigt die Eingabeaufforderungen und Systemantworten bei der Konfiguration des Switches. Die Winkelklammern (`<<<`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

   Sie geben grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Managementadresse und Gateway, und wählen SSH mit RSA aus.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
   Number of rsa key bits <1024-2048> [1024]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Reihe von Eingabeaufforderungen vervollständigt die Konfiguration:

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch-A-1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch-A-1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco Switch NX-OS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Software-Download"

2. Kopieren Sie die Switch-Software auf den Switch: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In diesem Beispiel wird die Datei nxos.7.0.3.I4.6.bin vom SFTP-Server 10.10.99.99 auf den lokalen Bootflash kopiert:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind: `dir bootflash:`

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software: `install all nxos bootflash:nxos.version-number.bin`

   Der Switch wird automatisch neu geladen (neu gestartet), nachdem die Switch-Software installiert wurde.

   Das folgende Beispiel zeigt die Softwareinstallation auf IP_Switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 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                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   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.
IP_switch_A_1#
```

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vergewissern Sie sich, dass die Switch-Software installiert ist: `show version`

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Konfiguration der MACsec-Verschlüsselung bei Cisco 9336C-Switches

Auf Wunsch können Sie die MACsec-Verschlüsselung für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

Die MACsec-Verschlüsselung kann nur auf die WAN-ISL-Ports angewendet werden.

Lizenzierungsanforderungen für MACsec

MACsec erfordert eine Sicherheitslizenz. Eine vollständige Erläuterung des Cisco NX-OS-Lizenzschemas und der Beschaffung und Anwendung von Lizenzen finden Sie im "Cisco NX-OS Licensing Guide"

Aktivierung von Cisco MACs Encryption WAN-ISLs in MetroCluster IP-Konfigurationen

Sie können die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration aktivieren.

1. Den globalen Konfigurationsmodus aufrufen: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Aktivieren Sie MACsec und MKA auf dem Gerät: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Kopieren Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Deaktivieren von Cisco MACsec Encryption

Möglicherweise müssen Sie die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration deaktivieren.

Wenn Sie die Verschlüsselung deaktivieren, müssen Sie auch Ihre Schlüssel löschen.

1. Den globalen Konfigurationsmodus aufrufen: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Deaktivieren Sie die MACsec-Konfiguration auf dem Gerät: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Durch Auswahl der Option „Keine“ wird die Funktion „MACsec“ wiederhergestellt.

3. Wählen Sie die Schnittstelle aus, die Sie bereits mit MACsec konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Entfernen Sie die auf der Schnittstelle konfigurierte Schlüsselanhänger, Richtlinie und Fallback-keychain, um die MACsec-Konfiguration zu entfernen: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Wiederholen Sie die Schritte 3 und 4 auf allen Schnittstellen, für die MACsec konfiguriert ist.
6. Kopieren Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Konfigurieren einer MACsec-Schlüsselkette und -Tasten

Weitere Informationen zur Konfiguration einer MACsec-Schlüsselkette finden Sie in der Cisco-Dokumentation für Ihren Switch.

Anschließen des neuen NS224-Regals

Schritte

1. Installieren Sie das im Lieferumfang des Regals beiliegte Schienensatz mithilfe des im Kit enthaltenen Installationsflyers.
2. Montieren und befestigen Sie das Regal mithilfe des Installationsflyers an den Halterungen und Rack oder Schrank.
3. Schließen Sie die Stromkabel an das Shelf an, befestigen Sie sie in der Kabelhalterung, und schließen Sie die Netzkabel anschließend an verschiedene Stromquellen an, um für Ausfallsicherheit zu sorgen.

   Ein Shelf schaltet sich ein, wenn es mit einer Stromquelle verbunden ist. Es verfügt nicht über Netzschalter. Bei ordnungsgemäßer Funktion leuchtet die zweifarbige LED des Netzteils grün.

4. Legen Sie die Shelf-ID auf eine Zahl fest, die innerhalb des HA-Paars und über die Konfiguration eindeutig ist.
5. Verbinden Sie die Shelf-Ports in folgender Reihenfolge:

a. NSM-A, e0a mit dem Switch verbinden (Switch-A1 oder Switch-B1)
b. NSM-B, e0a mit dem Switch verbinden (Switch-A2 oder Switch-B2)
c. Verbinden Sie NSM-A, e0b mit dem Switch (Switch-A1 oder Switch-B1).
d. Verbinden Sie NSM-B, e0b mit dem Switch (Switch-A2 oder Switch-B2).

6. Verwenden Sie das aus dem **RcfFileGenerator**-Werkzeug generierte Verkabelungslayout, um das Shelf mit den entsprechenden Ports zu verkabeln.

   Sobald das neue Shelf ordnungsgemäß verkabelt ist, erkennt ONTAP es automatisch im Netzwerk.

Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration

Ab ONTAP 9.15.1 können Sie die End-to-End-Verschlüsselung zur Verschlüsselung von Back-End-Datenverkehr, wie NVLOG- und Storage-Replizierungsdaten, zwischen den Standorten einer MetroCluster IP-Konfiguration konfigurieren.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Bevor Sie die End-to-End-Verschlüsselung konfigurieren können, müssen Sie dies tun "Externes Verschlüsselungsmanagement konfigurieren".
- Prüfen Sie die unterstützten Systeme und die Mindestversion von ONTAP, die erforderlich sind, um die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration zu konfigurieren:

Minimale ONTAP-Version	Unterstützte Systeme
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700

End-to-End-Verschlüsselung

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu aktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

```
metrocluster check show
```

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

```
security key-manager external show-status
```

3. End-to-End-Verschlüsselung für jede DR-Gruppe aktivieren:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung aktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

End-to-End-Verschlüsselung deaktivieren

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu deaktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

```
metrocluster check show
```

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

```
security key-manager external show-status
```

3. Deaktivieren Sie die End-to-End-Verschlüsselung für jede DR-Gruppe:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung deaktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

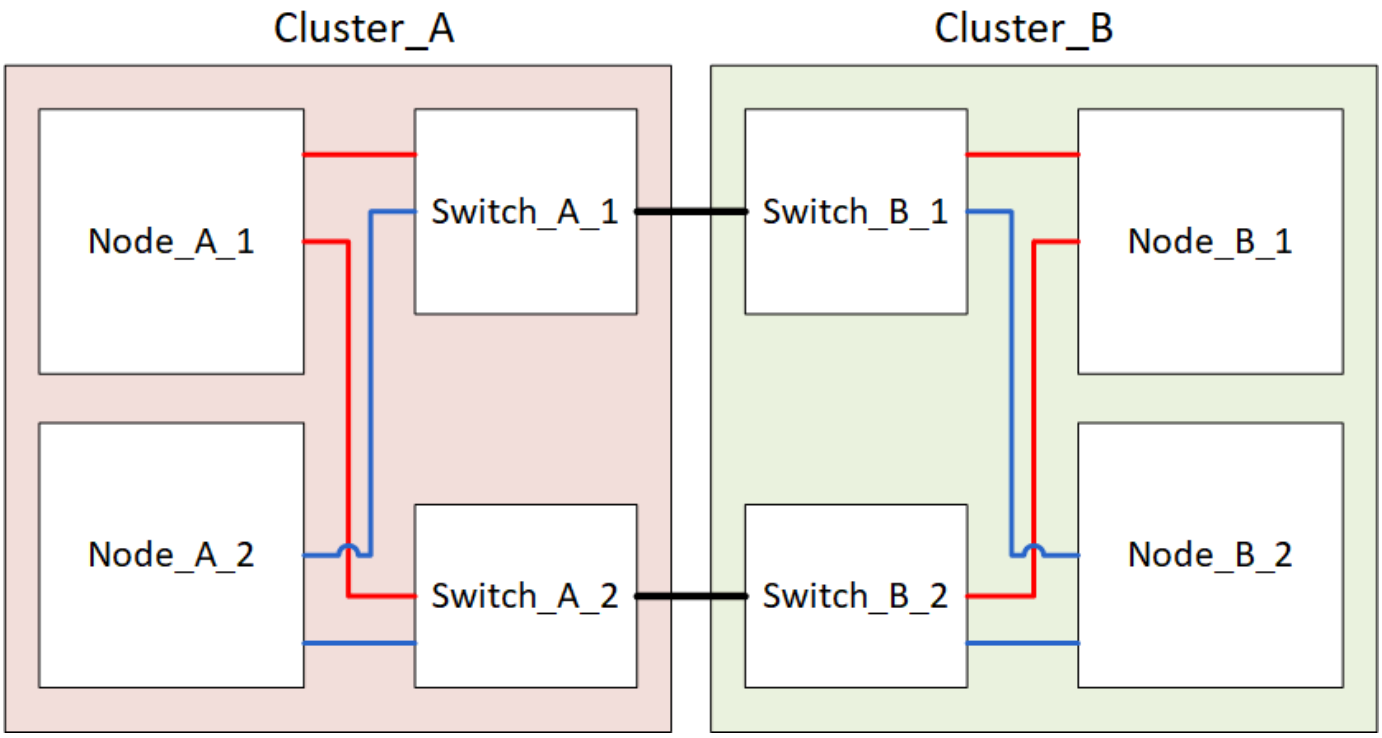
```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Schalten Sie einen einzelnen Standort in einer MetroCluster IP-Konfiguration aus und wieder ein

Wenn Sie eine Standortwartung durchführen oder einen einzelnen Standort in einer MetroCluster IP-Konfiguration verlagern müssen, müssen Sie wissen, wie Sie den Standort ausschalten und einschalten müssen.

Wenn Sie einen Standort verschieben und neu konfigurieren müssen (wenn Sie z. B. von einem Cluster mit vier Nodes auf ein Cluster mit acht Nodes erweitern müssen), können diese Aufgaben nicht gleichzeitig ausgeführt werden. Dieser Vorgang deckt nur die Schritte ab, die zur Durchführung von Wartungsarbeiten am Standort oder zum Standortwechsel ohne Änderung der Konfiguration erforderlich sind.

Das folgende Diagramm zeigt eine MetroCluster-Konfiguration. Cluster_B wird aus Wartungszwecken ausgeschaltet.



Schalten Sie einen MetroCluster-Standort aus

Sie müssen einen Standort und die gesamte Ausrüstung abschalten, bevor die Wartung oder der Standortwechsel beginnen können.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von dem Standort ausgegeben, der weiterhin eingeschaltet bleibt.

Schritte

1. Bevor Sie beginnen, überprüfen Sie, ob alle nicht gespiegelten Aggregate am Standort offline sind.
2. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      ```
      system health alert show
      ```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

      ```
      metrocluster show
      ```

   d. Führen Sie eine MetroCluster-Prüfung durch:
      `metrocluster check run`
   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

      ```
      metrocluster check show
      ```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

h. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

3. Implementieren Sie von dem Standort aus, an dem Sie weiterhin arbeiten möchten, die Umschaltung:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Der Vorgang kann einige Minuten dauern.

4. Überwachen und überprüfen Sie den Abschluss der Umschaltung:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Wenn Sie eine MetroCluster IP-Konfiguration mit ONTAP 9.6 oder höher ausführen, warten Sie, bis die Plexe der Disaster-Site online geschaltet sind und die Heilungsvorgänge automatisch abgeschlossen sind.

Bei MetroCluster IP-Konfigurationen mit ONTAP 9.5 oder älteren Versionen werden die Knoten der Disaster-Standorte nicht automatisch von ONTAP gebootet, und die Plexe bleiben offline.

6. Verschieben Sie alle Volumes und LUNs, die zu nicht gespiegelten Aggregaten gehören, offline.

a. Verschieben Sie die Volumes in den Offline-Modus.

```
cluster_A::* volume offline <volume name>
```

b. Verschieben Sie die LUNs in den Offline-Modus.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Nicht gespiegelte Aggregate lassen sich offline verschieben: `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. Identifizieren und verschieben Sie je nach Konfiguration und ONTAP-Version die betroffenen Plexe, die sich am Disaster-Standort (Cluster_B) befinden, offline.

   Sie sollten die folgenden Plexe offline verschieben:

   - Nicht gespiegelte Plexe befinden sich auf Festplatten am DR-Standort.

     Wenn Sie die nicht gespiegelten Plexe am Disaster-Standort nicht offline schalten, kann es zu einem Ausfall kommen, wenn der Disaster-Standort später ausgeschaltet wird.

   - Gespiegelte Plexe auf Festplatten am Disaster Site zur Aggregatspiegelung Nachdem sie offline verschoben wurden, sind die Plexe nicht mehr zugänglich.

   a. Identifizieren Sie die betroffenen Plexe.

      Plexe, die Nodes auf dem verbleibenden Platz gehören, bestehen aus Pool1-Festplatten. Plexe, die im Eigentum von Nodes am Disaster-Site sind, bestehen aus Pool0-Platten.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

Die betroffenen Plexe sind diejenigen, die Remote zu Cluster A sind In der folgenden Tabelle wird gezeigt, ob die Festplatten lokal oder Remote relativ zu Cluster A sind:

Knoten	Disks im Pool	Sollten die Festplatten offline geschaltet werden?	Beispiel für Plexe, die offline verschoben werden sollen
Node_A_1 und Node_A_2	Laufwerke im Pool 0	Nein Festplatten sind lokal für Cluster A	-

Festplatten in Pool 1	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Node _B_1 und Node _B_2
Laufwerke im Pool 0	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Festplatten in Pool 1

b. Verschieben Sie die betroffenen Plexe offline:

`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

Führen Sie diesen Schritt für alle Plexe aus, die über Remote-Festplatten für Cluster_A verfügen

9. Die ISL-Switch-Ports werden je nach Switch-Typ permanent offline geschaltet.
10. Beenden Sie die Nodes, indem Sie für jeden Node den folgenden Befehl ausführen:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Schalten Sie die Geräte am DR-Standort aus.

    Sie müssen die folgenden Geräte in der angegebenen Reihenfolge ausschalten:

    - Speicher-Controller: Die Speicher-Controller sollten sich derzeit am befinden `LOADER` Sie müssen sie vollständig ausschalten.
    - MetroCluster IP-Switches
    - Storage Shelfs

Verlagerung des ausgeschalteten Standorts des MetroCluster

Nachdem der Standort ausgeschaltet ist, können Sie mit der Wartung beginnen. Das Verfahren ist dasselbe, ob die MetroCluster Komponenten innerhalb desselben Datacenters verlegt oder in ein anderes Datacenter verlagert werden.

- Die Hardware sollte auf die gleiche Weise wie der vorherige Standort verkabelt werden.
- Wenn sich die Geschwindigkeit, Länge oder Zahl der Inter-Switch-Verbindung (ISL) geändert hat, müssen

alle neu konfiguriert werden.

Schritte

1. Vergewissern Sie sich, dass die Verkabelung aller Komponenten sorgfältig aufgezeichnet wurde, damit sie am neuen Standort wieder richtig angeschlossen werden kann.
2. Physische Verlagerung der gesamten Hardware, der Storage-Controller, der IP-Switches, FibreBridges und der Storage-Shelfs
3. Konfiguration der ISL-Ports und Überprüfung der Konnektivität zwischen Standorten
   a. Schalten Sie die IP-Switches ein.

      Schalten Sie keine anderen Geräte ein.

4. Überprüfen Sie mithilfe von Tools auf den Switches (wie sie verfügbar sind) die Verbindung zwischen den Standorten.

   Sie sollten nur fortfahren, wenn die Links korrekt konfiguriert und stabil sind.

5. Deaktivieren Sie die Links erneut, wenn sie stabil sind.

Einschalten der MetroCluster-Konfiguration und Zurückkehren zum normalen Betrieb

Nach Abschluss der Wartung oder Verschieben des Standorts müssen Sie den Standort einschalten und die MetroCluster Konfiguration wiederherstellen.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von der Website ausgegeben, die Sie einschalten.

Schritte

1. Schalten Sie die Schalter ein.

   Schalten Sie die Schalter zuerst ein. Möglicherweise wurden sie im vorherigen Schritt eingeschaltet, wenn der Standort verlegt wurde.

   a. Konfigurieren Sie den Inter-Switch Link (ISL), falls erforderlich, oder falls dieser nicht Teil der Verschiebung abgeschlossen wurde.
   b. ISL aktivieren, falls Fechten abgeschlossen wurde.
   c. ISL überprüfen.

2. Schalten Sie die Storage-Controller ein, und warten Sie, bis die angezeigt wird `LOADER` Eingabeaufforderung: Die Controller dürfen nicht vollständig gebootet werden.

   Wenn der automatische Start aktiviert ist, drücken Sie `Ctrl+C` Um das automatische Booten der Controller zu stoppen.

3. Schalten Sie die Shelfs ein, damit sie sich vollständig einschalten können.
4. Vergewissern Sie sich, dass der Speicher sichtbar ist.
   a. Vergewissern Sie sich, dass der Speicher vom verbleibenden Standort aus sichtbar ist. Versetzen Sie die Offline-Plexe wieder in den Online-Modus, um die Neusynchronisierung neu zu starten und die SyncMirror wiederherzustellen.

b. Überprüfen Sie, ob der lokale Speicher vom Knoten im Wartungsmodus sichtbar ist:

```
disk show -v
```

5. Wiederherstellung der MetroCluster-Konfiguration

Befolgen Sie die Anweisungen unter "Überprüfen, ob das System für einen Wechsel bereit ist" Um Healing- und Switchback-Vorgänge gemäß Ihrer MetroCluster-Konfiguration durchzuführen.

Ausschalten einer gesamten MetroCluster IP-Konfiguration

Bevor die Wartung oder Umsiedlung beginnen kann, müssen Sie die gesamte MetroCluster IP-Konfiguration und alle Geräte ausschalten.

Ab ONTAP 9.8 beginnt der **`storage switch`** Befehl wird durch ersetzt **`system switch`**. Die folgenden Schritte zeigen das **`storage switch`** Befehl, aber wenn Sie ONTAP 9.8 oder höher ausführen, der **`system switch`** Befehl ist bevorzugt.

1. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.
   a. Vergewissern Sie sich, dass die MetroCluster-Konfiguration und der Betriebsmodus normal sind.
   `metrocluster show`
   b. Führen Sie den folgenden Befehl aus:
   `metrocluster interconnect show`
   c. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:
   `run local sysconfig -v`
   d. Führen Sie den folgenden Befehl aus:
   `storage port show`
   e. Führen Sie den folgenden Befehl aus:
   `storage switch show`
   f. Führen Sie den folgenden Befehl aus:
   `network interface show`
   g. Führen Sie den folgenden Befehl aus:
   `network port show`
   h. Führen Sie den folgenden Befehl aus:
   `network device-discovery show`
   i. Führen Sie eine MetroCluster-Prüfung durch:
   `metrocluster check run`
   j. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
   `metrocluster check show`
   k. Führen Sie den folgenden Befehl aus:
   `metrocluster configuration-settings interface show`
2. Deaktivieren Sie gegebenenfalls AUSO, indem Sie die AUSO-Fehlerdomäne in ändern

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

In einer MetroCluster-IP-Konfiguration ist die AUSO-Fehlerdomäne bereits auf „deaktiviert“ gesetzt, es sei denn, die Konfiguration ist mit dem ONTAP-Mediator konfiguriert.

3. Die Änderung wird mit dem Befehl überprüft

   metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Anhalten der Knoten:

   halt

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. Schalten Sie die folgenden Geräte am Standort aus:
   - Storage Controller
   - MetroCluster IP-Switches
   - Storage Shelfs
6. Warten Sie dreißig Minuten, und schalten Sie dann alle Storage Shelfs, MetroCluster IP Switches und Storage-Controller ein.
7. Nachdem die Controller eingeschaltet sind, überprüfen Sie die MetroCluster-Konfiguration von beiden Standorten aus.

   Um die Konfiguration zu überprüfen, wiederholen Sie Schritt 1.

8. Führen Sie Prüfungen der Einschaltzyklus durch.
   a. Vergewissern Sie sich, dass alle Sync-Source-SVMs online sind:
      vserver show
   b. Starten Sie alle Sync-Source-SVMs, die nicht online sind:
      vserver start