Upgrade wird vorbereitet

ONTAP MetroCluster

NetApp
February 28, 2025

Inhalt

Upgrade wird vorbereitet . . . 1
Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens . . . 1
Plattformen, die durch dieses Verfahren unterstützt werden . . . 1
Anforderungen . . . 1
Aktivieren Sie die Konsolenprotokollierung vor dem MetroCluster IP-Controller-Upgrade . . . 2
Legen Sie den erforderlichen Bootarg fest (für MetroCluster IP-Upgrades auf Systemen ab ONTAP 9.15.1). . . . 3
Schritt 1: Bestimmen Sie den Bootarg, den Sie auf den alten Controllern einstellen müssen . . . 3
Schritt 2: Stellen Sie den erforderlichen Bootarg auf den alten Controllern ein . . . 3
Bereiten Sie das MetroCluster IP-System für das Upgrade vor . . . 4
Aktualisieren Sie die RCFs des MetroCluster-Switches, bevor Sie die Controller aktualisieren . . . 5
Weisen Sie den neuen Nodes Ports von den alten Nodes zu . . . 6
Booten Sie die neuen Controller ein . . . 7
Löschen Sie die Konfiguration auf einem Controller-Modul . . . 9
Überprüfen Sie vor Standort-Upgrade den MetroCluster-Zustand . . . 10
Sammeln Sie vor dem Upgrade Informationen . . . 11
Entfernen Sie die Mediator- oder Tiebreaker-Überwachung . . . 14
Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht . . . 14

Upgrade wird vorbereitet

Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens

Überprüfen Sie vor dem Controller-Upgrade, ob Ihr System alle Anforderungen erfüllt.

Plattformen, die durch dieses Verfahren unterstützt werden

- Die Plattformen müssen ONTAP 9.8 oder höher ausführen.
- Die Ziel-Plattform (neue) muss ein anderes Modell sein als die ursprüngliche Plattform.
- Mit diesem Verfahren können Sie nur bestimmte Plattformmodelle in einer MetroCluster IP-Konfiguration aktualisieren.
  - Informationen darüber, welche Plattformupgrade-Kombinationen unterstützt werden, finden Sie in der Tabelle MetroCluster IP-Upgrade in "Wählen Sie ein Controller-Upgrade-Verfahren".

    Siehe "Wahl einer Upgrade- oder Aktualisierungsmethode" Für zusätzliche Verfahren.

Anforderungen

- Dieses Verfahren gilt für Controller-Module in einer MetroCluster IP-Konfiguration.
- Upgrades für alle Controller der Konfiguration sollten während des gleichen Wartungszeitraums durchgeführt werden.

  Das Ausführen der MetroCluster-Konfiguration mit unterschiedlichen Controller-Typen wird außerhalb dieser Wartungsaktivitäten nicht unterstützt.

- Auf den MetroCluster IP-Systemen muss an beiden Standorten dieselbe ONTAP-Version ausgeführt werden.
- Die MetroCluster IP Switches (Switch-Typ, Anbieter und Modell) und Firmware-Version müssen von den vorhandenen und neuen Controllern in Ihrer Upgrade-Konfiguration unterstützt werden.

  Informationen zu unterstützten Switches und Firmware-Versionen finden Sie im "Hardware Universe" oder im "IMT" .

- Wenn Sie ein Upgrade von Systemen durchführen, die über mehr Steckplätze oder Ports als das neue System verfügen, müssen Sie überprüfen, ob das neue System über genügend Steckplätze und Ports verfügt.

  Bevor Sie mit dem Upgrade beginnen, lesen Sie die Informationen zur Überprüfung der "Hardware Universe"Anzahl der Steckplätze und Ports auf dem neuen System.

- Wenn es auf Ihrem System aktiviert ist, "End-to-End-Verschlüsselung deaktivieren" bevor Sie das Upgrade durchführen.
- Wenn die neue Plattform weniger Steckplätze als das ursprüngliche System besitzt oder weniger oder unterschiedliche Ports vorhanden sind, müssen Sie dem neuen System möglicherweise einen Adapter hinzufügen.
- Sie verwenden die IP-Adressen, Netmasken und Gateways der ursprünglichen Plattformen auf den neuen Plattformen wieder.

Folgende Beispielnamen werden in diesem Verfahren verwendet:

- Cluster_A an Standort_A
  - Vor dem Upgrade:
    - Node_A_1-alt
    - Node_A_2-alt
  - Nach dem Upgrade:
    - Node_A_1-neu
    - Node_A_2-neu
- Cluster_B an Standort_B
  - Vor dem Upgrade:
    - Node_B_1-alt
    - Node_B_2-alt
  - Nach dem Upgrade:
    - Node_B_1-neu
    - Node_B_2-neu

Was kommt als Nächstes?

"Aktivieren Sie die Konsolenprotokollierung".

Aktivieren Sie die Konsolenprotokollierung vor dem MetroCluster IP-Controller-Upgrade

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie das Controller-Upgrade durchführen.

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Was kommt als Nächstes?

Prüfen Sie die Informationen in"Legen Sie den erforderlichen Bootarg fest (für Upgrades auf Systeme, die ab 9.15.1 eingeführt wurden).", um zu bestätigen, ob Sie einen erforderlichen Bootarg auf dem vorhandenen System festlegen müssen.

Legen Sie den erforderlichen Bootarg fest (für MetroCluster IP-Upgrades auf Systemen ab ONTAP 9.15.1).

Controller-Upgrades für Systeme, die in ONTAP 9.15.1 oder höher eingeführt wurden, erfordern es, ein Boot-arg einzurichten, bevor Sie mit dem Upgrade beginnen können.

Schritt 1: Bestimmen Sie den Bootarg, den Sie auf den alten Controllern einstellen müssen

Für alle unterstützten Upgrades auf den folgenden Systemen müssen Sie vor der Durchführung des Controller-Upgrades ein Boot-arg auf den alten Controllern einrichten:

- AFF A70, AFF A90, AFF A1K
- FAS70, FAS90
- AFF C80
- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60

> Wenn Sie ein Upgrade auf eines der aufgeführten Systeme durchführen, müssen Sie * einen erforderlichen Bootarg auf dem vorhandenen System festlegen, bevor Sie das Upgrade durchführen. Für alle anderen Upgrades können Sie diese Aufgabe überspringen und direkt zu gehen "Bereiten Sie das System für das Upgrade vor".

Bei den meisten Upgrades von Systemen, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie den Bootarg auf den alten Controllern einstellen `hw.cxgbe.toe_keepalive_disable`. Bestimmte Upgrade-Pfade erfordern jedoch, dass Sie stattdessen den Bootarg einstellen `bootarg.siw.interop_enabled`.

Verwenden Sie die folgende Tabelle, um zu bestimmen, welche Bootarg Sie für Ihre spezifische Upgrade-Kombination einstellen müssen.

Für dieses Upgrade…	Bootarg festlegen…
Von AFF A250 nach AFF A30	`bootarg.siw.interop_enabled`
Von AFF C250 nach AFF C30	`bootarg.siw.interop_enabled`
Von AFF A150 nach AFF A20	`bootarg.siw.interop_enabled`
Von AFF A220 nach AFF A20	`bootarg.siw.interop_enabled`
Alle anderen unterstützten Upgrades auf AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30 oder AFF C60 Systeme	`hw.cxgbe.toe_keepalive_disable`

Schritt 2: Stellen Sie den erforderlichen Bootarg auf den alten Controllern ein

Diese Aufgabe ist **nur** erforderlich, wenn Sie ein Upgrade auf ein AFF A70-, AFF A90-, AFF A1K-, FAS70-, FAS90-, AFF C80-, AFF A50-, AFF A20-, AFF A30-, AFF C30- oder AFF C60-System durchführen.

Schritte

1. Halten Sie einen Node an jedem Standort an und erlauben Sie dem HA-Partner, einen Storage-Takeover des Node durchzuführen:

   ```
   halt -node <node_name>
   ```

2. Stellen Sie den erforderlichen Bootarg für Ihre Upgrade-Kombination ein. Sie haben bereits den Bootarg festgelegt, den Sie mithilfe der Tabelle in festlegen müssenBestimmen Sie, welchen Bootarg Sie einstellen müssen.

   hw.cxgbe.toe_keepalive_disable

   a. Geben Sie an `LOADER` der Eingabeaufforderung des angehaltenen Node Folgendes ein:

      ```
      setenv hw.cxgbe.toe_keepalive_disable 1

      saveenv

      printenv hw.cxgbe.toe_keepalive_disable
      ```

   bootarg.siw.interop_enabled

   a. Geben Sie an `LOADER` der Eingabeaufforderung des angehaltenen Node Folgendes ein:

      ```
      setenv bootarg.siw.interop_enabled 1

      saveenv

      printenv bootarg.siw.interop_enabled
      ```

3. Booten des Node:

   ```
   boot_ontap
   ```

4. Führen Sie beim Booten des Node ein Giveback für den Node durch, um folgende Eingabeaufforderung zu erhalten:

   ```
   storage failover giveback -ofnode <node_name>
   ```

5. Wiederholen Sie die Schritte für jeden Knoten in der DR-Gruppe, der aktualisiert wird.

Was kommt als Nächstes?

"Bereiten Sie das System für das Upgrade vor".

Bereiten Sie das MetroCluster IP-System für das Upgrade vor

Bevor Sie Änderungen an der vorhandenen MetroCluster Konfiguration vornehmen, überprüfen Sie den Zustand der Konfiguration, bereiten die neuen Plattformen vor und führen verschiedene andere Aufgaben aus.

Aktualisieren Sie die RCFs des MetroCluster-Switches, bevor Sie die Controller aktualisieren

Je nach den alten und neuen Plattformmodellen müssen Sie möglicherweise die Referenzkonfigurationsdateien (RCFs) des MetroCluster-Switches aktualisieren, bevor Sie ein Controller-Upgrade durchführen.

Über diese Aufgabe

Führen Sie diese Aufgabe unter folgenden Umständen aus:

- Die Switch-RCF-Konfiguration ist nicht auf der Mindestversion.
- Sie müssen die VLAN-IDs ändern, die von den Back-End-MetroCluster-Verbindungen verwendet werden.

Bevor Sie beginnen

Prüfen Sie, ob Sie die RCFs vor dem Upgrade der Controller aktualisieren müssen:

- Wenn die Switch-Konfiguration nicht mit der unterstützten RCF-Mindestversion konfiguriert wurde, müssen Sie die RCFs vor dem Upgrade Ihrer Controller aktualisieren:

Switch-Modell	Erforderliche RCF-Version
Cisco 3132Q-V	1.7 oder höher
Cisco 3232C	1.7 oder höher
Broadcom BES-53248	1.3 oder höher
NVIDIA SN2100	2.0 oder höher

- Wenn beide Ihrer alten und neuen Plattformmodelle in der folgenden Liste aufgeführt sind, müssen Sie die VLAN-ID vor dem Upgrade der Controller * nicht * aktualisieren:
  - FAS8200 oder AFF A300
  - AFF A320
  - FAS9000 oder AFF A700
  - AFF A800, AFF C800, ASA A800 oder ASA C800

    Wenn eines Ihrer alten oder neuen Plattformmodelle oben nicht aufgeführt ist, müssen Sie bestätigen, dass die MetroCluster-Schnittstellen eine unterstützte VLAN-ID verwenden. Unterstützte VLAN-IDs für die MetroCluster-Schnittstellen: 10, 20 oder im Bereich von 101 bis 4096.

  - Wenn die VLAN-ID nicht 10, 20 oder im Bereich von 101 bis 4096 lautet, müssen Sie die Switch-RCF aktualisieren, bevor Sie die Controller aktualisieren.
  - Die lokalen Cluster-Verbindungen können jedes beliebige VLAN verwenden, sie müssen sich nicht im angegebenen Bereich befinden.
  - Die neue RCF, auf die Sie aktualisieren, muss die VLANs 10, 20 oder im Bereich 101 bis 4096 verwenden. Ändern Sie das VLAN für den lokalen Cluster nur, wenn es erforderlich ist.

Schritte

1. Bereiten Sie die IP-Switches auf die Anwendung der neuen RCFs vor.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   > Sie sollten die Schalter in der folgenden Reihenfolge aktualisieren: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

   - "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"

2. Laden Sie die RCFs herunter, und installieren Sie sie.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   - "Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"
   - "Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"
   - "Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

Sie müssen überprüfen, ob die physischen Ports auf Node_A_1-old den physischen Ports auf Node_A_1-New richtig zugeordnet sind. Dadurch kann Node_A_1-New nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Beim ersten Booten des neuen Node während des Upgrades wird die aktuellste Konfiguration des alten Node wiedergegeben, den er ersetzt. Wenn Sie Node_A_1-New booten, versucht ONTAP, LIFs auf denselben Ports zu hosten, die in Node_A_1-old verwendet wurden. Das bedeutet, dass Sie im Rahmen des Upgrades die Port- und LIF-Konfiguration anpassen müssen, sodass sie mit der Konfiguration des alten Node kompatibel ist. Während des Upgrades führen Sie sowohl für die alten als auch für die neuen Nodes Schritte aus, um die korrekte Konfiguration der Cluster-, Management- und Daten-LIFs zu gewährleisten

Die folgende Tabelle zeigt Beispiele für Konfigurationsänderungen in Bezug auf die Portanforderungen der neuen Nodes.

Physische Ports für Cluster-Interconnect		
Alter Controller	Neuer Controller	Erforderliche Maßnahme
e0a, e0b	e3a, e3b	Kein passender Port. Nach dem Upgrade müssen Sie die Cluster-Ports neu erstellen.
e0c, e0d	e0a, e0b, e0c, e0d	e0c und e0d sind passende Anschlüsse. Sie müssen die Konfiguration nicht ändern, aber nach dem Upgrade können Sie Ihre Cluster LIFs auf die verfügbaren Cluster-Ports verteilen.

Schritte

1. Legen Sie fest, welche physischen Ports auf den neuen Controllern verfügbar sind und welche LIFs auf den Ports gehostet werden können.

   Die Port-Nutzung des Controllers hängt vom Plattformmodul ab und welche Switches Sie in der MetroCluster IP-Konfiguration verwenden werden. Sie können die Port-Nutzung der neuen Plattformen aus der "Hardware Universe".

2. Planen Sie Ihre Portnutzung und füllen Sie die folgenden Tabellen als Referenz für jeden der neuen Nodes aus.

   Sie verweisen auf die Tabelle, während Sie das Upgrade-Verfahren durchführen.

	Node_A_1-alt			Node_A_1-neu		
LIF	Ports	IPspaces	Broadcast-Domänen	Ports	IPspaces	Broadcast-Domänen
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node-Management						
Cluster-Management						
Daten 1						
Daten 2						
Daten 3						
Daten 4						
San						
Intercluster-Port						

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass

Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

Schritte

1. Netzboot der neuen Controller:

   a. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.

   b. Laden Sie die entsprechende ONTAP Software im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.

   c. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

      Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:

      ```
      _ontap-version_image.tgz
      ```

      Sie müssen die Datei nicht extrahieren `_ontap-version_image.tgz`.

   d. Konfigurieren Sie an der `LOADER` Eingabeaufforderung die Netzboot-Verbindung für eine Management-LIF:

Wenn IP-Adresse…	Dann…
DHCP	Konfigurieren der automatischen Verbindung: `ifconfig e0M -auto`
Festgelegt	Konfigurieren Sie die manuelle Verbindung: `ifconfig e0M -addr=`*`ip_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`*

   e. Führen Sie den Netzboot aus.

      ```
      netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz
      ```

   f. Wählen Sie im Startmenü die Option **(7) Neue Software zuerst installieren** aus, um das neue Software-Image auf das Startgerät herunterzuladen und zu installieren.

      Ignorieren Sie die folgende Meldung:

`"This procedure is not supported for Non-Disruptive Upgrade on an HA pair"`. Dies gilt für unterbrechungsfreie Software-Upgrades, nicht für Controller-Upgrades.

   a. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL der Bilddatei ein:

      `http://`*`web_server_ip/path_to_web-accessible_directory/ontap-`*

*version*_image.tgz

b. Geben Sie ggf. den Benutzernamen und das Kennwort ein, oder drücken Sie die Eingabetaste, um fortzufahren.

c. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

```
Do you want to restore the backup configuration now? {y|n} n
```

d. Starten Sie den Neustart durch Eingabe **`y`** Wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
```

Löschen Sie die Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

   ```
   boot_ontap menu
   ```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Überprüfen Sie vor Standort-Upgrade den MetroCluster-Zustand

Vor dem Upgrade müssen Sie den Zustand und die Konnektivität der MetroCluster Konfiguration überprüfen.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:

   a. Prüfen Sie, ob die Knoten multipathed sind:
   `node run -node <node_name> sysconfig -a`

      Geben Sie diesen Befehl für jeden Node in der MetroCluster-Konfiguration ein.

   b. Stellen Sie sicher, dass in der Konfiguration: + keine defekten Festplatten vorhanden sind `storage disk show -broken`

      Geben Sie diesen Befehl für jeden Node in der MetroCluster-Konfiguration ein.

   c. Überprüfen Sie auf Statusmeldungen:

      `system health alert show`

      Geben Sie diesen Befehl für jedes Cluster ein.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

      `system license show`

      Geben Sie diesen Befehl für jedes Cluster ein.

   e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

      `network device-discovery show`

      Geben Sie diesen Befehl für jedes Cluster ein.

   f. Vergewissern Sie sich, dass Zeitzone und Uhrzeit auf beiden Standorten richtig eingestellt sind:

      `cluster date show`

   Geben Sie diesen Befehl für jedes Cluster ein. Sie können die Uhrzeit und die Zeitzone mit den `cluster date` Befehlen konfigurieren.

2. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.

   a. Bestätigen Sie die MetroCluster-Konfiguration und den Betriebsmodus `normal`:
   `metrocluster show`

   b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:
   `metrocluster node show`

   c. Geben Sie den folgenden Befehl ein:

      `metrocluster check run`

d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

3. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.
   a. Laden Sie Config Advisor herunter und führen Sie sie aus.

      "NetApp Downloads: Config Advisor"

   b. 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.

Sammeln Sie vor dem Upgrade Informationen

Vor dem Upgrade müssen Informationen für alle Nodes gesammelt und bei Bedarf die Netzwerk-Broadcast-Domänen angepasst, beliebige VLANs und Schnittstellengruppen entfernt und Verschlüsselungsinformationen gesammelt werden.

Schritte

1. Notieren Sie die physische Verkabelung für jeden Node und kennzeichnen Sie die Kabel nach Bedarf, damit die neue Nodes ordnungsgemäß verkabelt werden.
2. Sammeln Sie Interconnect-, Port- und LIF-Informationen für die einzelnen Nodes.

   Sammeln Sie die Ausgabe der folgenden Befehle für jeden Node:

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node <node_name> -type physical`
   - `network port vlan show -node <node_name>`
   - `network port ifgrp show -node <node_name> -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node <node_name> sysconfig -a`
   - `aggr show -r`
   - `disk show`
   - `system node run <node-name> disk show`
   - `vol show -fields type`
   - `vol show -fields type , space-guarantee`

- ◦ `vserver fcp initiator show`
- ◦ `storage disk show`
- ◦ `metrocluster configuration-settings interface show`

3. Erfassen Sie die UUIDs für Site_B (die Site, an der die Plattformen gerade aktualisiert werden):

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Diese Werte müssen auf den neuen Controller-Modulen „Site_B“ genau konfiguriert werden, um eine erfolgreiche Aktualisierung zu gewährleisten. Kopieren Sie die Werte in eine Datei, damit Sie sie später im Aktualisierungsvorgang in die Befehle kopieren können.

   Im folgenden Beispiel wird die Befehlsausgabe mit den UUIDs angezeigt:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

   NetApp empfiehlt, die UUIDs in einer Tabelle wie der folgenden aufzuzeichnen:

Cluster oder Node	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Knoten_B_1	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Knoten_B_2	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Wenn sich die MetroCluster-Nodes in einer SAN-Konfiguration befinden, sammeln Sie die relevanten Informationen.

   Sammeln Sie die Ausgabe der folgenden Befehle:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für den Schlüsselmanager verwendete Passphrase:

   ```
   security key-manager backup show
   ```

6. Wenn die MetroCluster Nodes Verschlüsselung für Volumes oder Aggregate nutzen, kopieren Sie Informationen zu Schlüsseln und Passphrases.

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

   a. Wenn Onboard Key Manager konfiguriert ist:
   `security key-manager onboard show-backup`

      Sie benötigen die Passphrase später im Upgrade-Verfahren.

   b. Wenn das Enterprise-Verschlüsselungsmanagement (KMIP) konfiguriert ist, geben Sie die folgenden Befehle ein:

      ```
      security key-manager external show -instance security key-manager key query
      ```

7. Ermitteln Sie die System-IDs der vorhandenen Nodes:

   ```
   metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
   ```

   Die folgende Ausgabe zeigt die neu zugewiesen Laufwerke.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Entfernen Sie die Mediator- oder Tiebreaker-Überwachung

Vor dem Aktualisieren der Plattformen müssen Sie die Überwachung entfernen, wenn die MetroCluster-Konfiguration mit dem Tiebreaker oder Mediator Utility überwacht wird.

Schritte

1. Sammeln Sie die Ausgabe für den folgenden Befehl:

   ```
   storage iscsi-initiator show
   ```

2. Entfernen Sie die vorhandene MetroCluster-Konfiguration von Tiebreaker, Mediator oder einer anderen Software, die die Umschaltung initiieren kann.

Sie verwenden…	Gehen Sie folgendermaßen vor:
Tiebreaker	"Entfernen von MetroCluster-Konfigurationen"
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

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. Melden Sie sich bei dem Cluster an.
2. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Der `maintenance-window-in-hours` Parameter gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. 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
   ```

3. Wiederholen Sie diese Schritte auf der Partner-Site.

Was kommt als Nächstes?

"Wechseln Sie über die MetroCluster-Konfiguration".