Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration

ONTAP MetroCluster

NetApp
April 12, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap-metrocluster/upgrade/concept_choosing_an_upgrade_method_mcc.html on April 12, 2024. Always check docs.netapp.com for the latest.

Inhalt

Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration . . . 1
Beginnen Sie hier - Wählen Sie Ihre Prozedur . . . 1
Aktualisieren Sie Controller in einer MetroCluster IP-Konfiguration mit vier Nodes mithilfe von Switchover und Switchback mit Befehlen, die den System-Controller ersetzen (ONTAP 9.13.1 und höher). . . . 8
Controller-Upgrade in einer MetroCluster FC-Konfiguration durch Switchover und Switchback . . . 30
Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher) . . . 57
Controller-Upgrade in einer MetroCluster FC-Konfiguration mit vier Nodes durch Umschaltung und Switchback mit Befehlen zum Austausch eines System-Controllers (ONTAP 9.10.1 und höher) . . . 85
Controller-Upgrade in einer MetroCluster IP-Konfiguration durch Switchover und Switchback (ONTAP 9.8 und höher) . . . 103
Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher) . . . 134
Aktualisieren einer MetroCluster FC-Konfiguration mit vier Nodes . . . 164
Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher) . . . 166
Erweitern Sie eine MetroCluster FC Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes . 176
Erweitern Sie eine MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes . 216
Erweitern einer MetroCluster IP-Konfiguration . . . 253
Entfernen einer Disaster Recovery-Gruppe . . . 282
Wo Sie weitere Informationen finden . . . 287

Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration

Beginnen Sie hier - Wählen Sie Ihre Prozedur

Hier starten: Sie haben die Wahl zwischen Controller-Upgrade, Systemaktualisierung oder Erweiterung

Je nach Umfang des Geräte-Upgrades wählen Sie ein Controller-Upgrade-Verfahren, ein Systemaktualisierungsverfahren oder ein Erweiterungsverfahren.

- Das Controller-Upgrade gilt nur für die Controller-Module. Die Controller werden durch ein neues Controller-Modell ersetzt.

  Modelle für Storage Shelfs werden nicht aktualisiert.

  - Bei Switchover- und Switchover-Prozessen wird der MetroCluster Switchover-Betrieb verwendet, um Clients unterbrechungsfreien Service zu bieten, während die Controller-Module im Partner-Cluster aktualisiert werden.
  - Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.
- Aktualisierungsverfahren gelten für die Controller und die Storage Shelfs.

  Im Aktualisierungsverfahren werden der MetroCluster Konfiguration neue Controller und Shelves hinzugefügt, eine zweite DR-Gruppe erstellt und die Daten werden unterbrechungsfrei zu den neuen Nodes migriert.

  Die ursprünglichen Controller werden dann außer Betrieb genommen.

- Erweiterungsverfahren fügen der MetroCluster-Konfiguration zusätzliche Controller und Shelves hinzu, ohne dass jegliche entfernt werden muss.

  Das von Ihnen verwendete Verfahren hängt vom MetroCluster-Typ und der Anzahl der vorhandenen Controller ab.

Upgrade-Typ	Gehe zu…
Für Controller-Upgrade	"Wählen Sie ein Controller-Upgrade-Verfahren"
Systemaktualisierung	"Wählen Sie ein Verfahren zur Systemaktualisierung aus"
Erweiterung	• "MetroCluster mit zwei Nodes auf vier Nodes" • "MetroCluster FC mit vier Nodes auf acht Nodes" • "MetroCluster IP mit vier Nodes auf acht Nodes"

Wählen Sie ein Controller-Upgrade-Verfahren

Das von Ihnen verwendete Controller-Upgrade-Verfahren hängt vom Plattformmodell und dem Typ der MetroCluster-Konfiguration ab.

Bei einem Upgrade-Verfahren werden die Controller durch ein neues Controller-Modell ersetzt. Modelle für Storage Shelfs werden nicht aktualisiert.

- Bei Switchover- und Switchover-Prozessen wird der MetroCluster Switchover-Betrieb verwendet, um Clients unterbrechungsfreien Service zu bieten, während die Controller-Module im Partner-Cluster aktualisiert werden.
- Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.

Auswahl eines Verfahrens, bei dem der Switchover- und Switchback-Prozess verwendet wird

Wählen Sie Ihre aktuelle Plattform aus der unten stehenden FC- oder IP-Tabelle aus. Wenn die Schnittmenge der Spalte Aktuelle Plattform und Zielplattform leer ist, wird das Upgrade nicht unterstützt.

Unterstützte MetroCluster IP-Controller-Upgrades

Wenn Ihre Plattform nicht aufgeführt ist, gibt es keine unterstützte Kombination für Controller-Upgrades.

> Wenn Sie ein Controller-Upgrade durchführen, stimmen der alte und der neue Plattformtyp **muss** überein.
>
> - Sie können ein FAS System auf ein FAS System oder ein AFF A-Series auf ein AFF A-Series System aufrüsten.
> - Sie können kein FAS System auf eine AFF A-Serie oder eine AFF A-Serie auf eine AFF C-Serie aufrüsten.
>
> Wenn Sie beispielsweise eine FAS8200 als Plattform aktualisieren möchten, können Sie ein Upgrade auf eine FAS9000 durchführen. Sie können kein Upgrade eines FAS8200 Systems auf ein AFF A700 System durchführen.

		Target MetroCluster IP platform									
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150										
	FAS2750 AFF A220										
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250										
	FAS8200 AFF A300										Note 2
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										Note 2
	FAS8700										Note 2
	FAS9000 AFF A700										Note 1
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

- Hinweis 1: Verwenden Sie für dieses Upgrade das Verfahren "Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher)"
- Hinweis 2: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Auf den neuen Controllern muss beispielsweise dieselbe ONTAP-Version wie auf den alten Controllern ausgeführt werden.

Unterstützte MetroCluster FC-Controller-Upgrades

Wenn Ihre Plattform nicht aufgeführt ist, gibt es keine unterstützte Kombination für Controller-Upgrades.

> Wenn Sie ein Controller-Upgrade durchführen, stimmen der alte und der neue Plattformtyp **muss** überein.
>
> - Sie können ein FAS System auf ein FAS System oder ein AFF A-Series auf ein AFF A-Series System aufrüsten.
> - Sie können kein FAS System auf eine AFF A-Serie oder eine AFF A-Serie auf eine AFF C-Serie aufrüsten.
>
> Wenn Sie beispielsweise eine FAS8200 als Plattform aktualisieren möchten, können Sie ein Upgrade auf eine FAS9000 durchführen. Sie können kein Upgrade eines FAS8200 Systems auf ein AFF A700 System durchführen.

		Target MetroCluster FC platform											
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1			Note 1				
	AFF8020		Note 1		Note 1		Note 1			Note 1			
	FAS8040 FAS8060 FAS8080												
	AFF8040 AFF8060 AFF8080												
	FAS8200					Note 2			Note 2		Note 4		
	AFF A300						Note 2			Note 2		Note 4	
	FAS8300										Note 4		
	AFF A400											Note 4	
	ASA A400												Note 5
	FAS9000										Note 3		
	AFF A700											Note 3	
	FAS9500												
	AFF A900												
	ASA A900												

- Hinweis 1: Für das Upgrade von Controllern, wenn FCVI-Verbindungen auf vorhandenen FAS8020 oder AFF8020 Nodes die Ports 1c und 1d verwenden, lesen Sie Folgendeshttps://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/MetroCluster/Upgrading_controllers_when_FCVI_connections_on_existing_FAS8020_or_AFF8020_nodes_use_ports_1c_and_1d["Knowledge Base-Artikel"^].
- Hinweis 2: Controller-Upgrades von AFF A300- oder FAS8200-Plattformen mit integrierten Ports 0e und 0f als FC-VI-Verbindungen werden nur auf den folgenden Systemen unterstützt:
  - ONTAP 9.9.1 und frühere Versionen
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1 GA
  - ONTAP 9.13.1 und höher

    Weitere Informationen finden Sie im "Öffentlicher Bericht".
- Hinweis 3: Für dieses Upgrade siehe "Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher)"
- Hinweis 4: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.
- Hinweis 5: Controller-Upgrades werden auf Systemen mit ONTAP 9.14.1 oder höher unterstützt.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Auf den neuen Controllern muss beispielsweise dieselbe ONTAP-Version wie auf den alten Controllern ausgeführt werden.

MetroCluster-Typ	Upgrade-Methode	ONTAP-Version	Verfahren
IP	Upgrade mit Befehlen zum Ersetzen des System-Controllers	9.13.1 und höher	"Link zum Verfahren"

FC	Upgrade mit Befehlen zum Ersetzen des System-Controllers	9.10.1 und höher	"Link zum Verfahren"
FC	Manuelles Upgrade mit CLI-Befehlen (nur AFF A700/FAS9000 auf AFF A900/FAS9500)	9.10.1 und höher	"Link zum Verfahren"
IP	Manuelles Upgrade mit CLI-Befehlen (nur AFF A700/FAS9000 auf AFF A900/FAS9500)	9.10.1 und höher	"Link zum Verfahren"
FC	Manuelles Upgrade mit CLI-Befehlen	9.8 und höher	"Link zum Verfahren"
IP	Manuelles Upgrade mit CLI-Befehlen	9.8 und höher	"Link zum Verfahren"

Wählen eines Verfahrens mithilfe der Aggregatverschiebung

Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.

MetroCluster-Typ	Aggregatverschiebung	ONTAP-Version	Verfahren
FC	Verwenden Sie Befehle „System Controller ersetzen“, um Controller-Modelle im gleichen Chassis zu aktualisieren	9.10.1 und höher	"Link zum Verfahren"
FC	Wird Verwendet `system controller replace` Befehle	9.8 und höher	"Link zum Verfahren"

MetroCluster-Typ	Aggregatverschiebung	ONTAP-Version	Verfahren
FC	Wird Verwendet `system controller replace` Befehle	9.5 bis 9.7	"Link zum Verfahren"
FC	Verwenden von manuellen ARL-Befehlen	9.8	"Link zum Verfahren"
FC	Verwenden von manuellen ARL-Befehlen	9.7 und früher	"Link zum Verfahren"

Auswahl der Methode zur Systemaktualisierung

Das von Ihnen verwendete Verfahren zur Systemaktualisierung hängt vom Plattformmodell und dem Typ der MetroCluster-Konfiguration ab. Aktualisierungsverfahren gelten für die Controller und die Storage Shelfs. Im Aktualisierungsverfahren werden der MetroCluster Konfiguration neue Controller und Shelves hinzugefügt, eine zweite DR-Gruppe erstellt und die Daten werden unterbrechungsfrei zu den neuen Nodes migriert. Die ursprünglichen Controller werden dann außer Betrieb genommen.

Unterstützte Kombinationen von MetroCluster FC-Technologie zur Aktualisierung

		Target MetroCluster FC platform									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8200										
	AFF A300										
	FAS8300										
	AFF A400										
	ASA A400										
	FAS9000										
	AFF A700										
	FAS9500										
	AFF A900										
	ASA A900										

- Sie müssen das Verfahren zur Technologieaktualisierung abschließen, bevor Sie eine neue Last hinzufügen.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen.
- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielplattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster neu konfigurieren, damit sie die Grenzen der Zielplattform erreichen oder darunter liegen, bevor Sie die neuen Nodes hinzufügen.
- Siehe "Hardware Universe" Für Plattformgrenzen

Unterstützte Kombinationen aus MetroCluster IP-technischen Aktualisierungen

		Target MetroCluster IP platform									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150 ASA A150	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS2750 AFF A220	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										
	FAS8700										
	FAS9000 AFF A700										
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

Anmerkung 1: Diese Kombination erfordert ONTAP 9.13.1 oder höher.

- Sie müssen das Verfahren zur Technologieaktualisierung abschließen, bevor Sie eine neue Last hinzufügen.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen.
- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielplattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster neu konfigurieren, damit sie die Grenzen der Zielplattform erreichen oder darunter liegen, bevor Sie die neuen Nodes hinzufügen.
- Siehe "Hardware Universe" Für Plattformgrenzen

Aktualisierungsmethode	Konfigurationstyp	ONTAP-Version	Verfahren
• Methode: Erweitern Sie die MetroCluster-Konfiguration, und entfernen Sie dann die alten Knoten	FC mit vier Nodes	9.6 und höher	"Link zum Verfahren"
• Methode: Erweitern Sie die MetroCluster-Konfiguration, und entfernen Sie dann die alten Knoten	IP mit vier Nodes	9.8 und höher	"Link zum Verfahren"

Wählen Sie ein Erweiterungsverfahren aus

Das von Ihnen verwendete Erweiterungsverfahren hängt vom Typ der MetroCluster-Konfiguration und der ONTAP-Version ab.

Beim Erweiterungsverfahren muss der MetroCluster Konfiguration neue Controller und neuer Storage hinzugefügt werden. Die Erweiterung muss an jedem Standort eine geraden Anzahl an Controllern beibehalten. Das Verfahren, das Sie verwenden, hängt von der Anzahl der Nodes in der ursprünglichen MetroCluster Konfiguration ab.

Erweiterungsmethode	Konfigurationstyp	ONTAP-Version	Verfahren
Methode: Erweitern Sie eine MetroCluster FC mit zwei Nodes auf vier	FC mit zwei Nodes	ONTAP 9 und höher (Plattformen müssen in ONTAP 9.2 und höher unterstützt werden)	"Link zum Verfahren"
Methode: Erweitern Sie eine MetroCluster FC mit vier Nodes auf acht	FC mit vier Nodes	ONTAP 9 oder höher	"Link zum Verfahren"
Methode: Erweitern Sie eine MetroCluster-IP mit vier Knoten auf acht	IP mit vier Nodes	ONTAP 9.9.1 und höher	"Link zum Verfahren"

Aktualisieren Sie Controller in einer MetroCluster IP-Konfiguration mit vier Nodes mithilfe von Switchover und Switchback mit Befehlen, die den System-Controller ersetzen (ONTAP 9.13.1 und höher).

Sie können diese geführte automatische MetroCluster-Umschaltung verwenden, um ein unterbrechungsfreies Controller-Upgrade für eine MetroCluster IP-Konfiguration mit vier Nodes durchzuführen. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Unterstützte Plattformkombinationen

Dieses Verfahren unterstützt die folgenden Controller-Upgrades auf Systemen mit ONTAP 9.13.1 und höher.

Alter Controller	Ersatz-Controller
AFF A300	AFF A900
FAS8200	FAS9500

> Sie können die in der Tabelle oben aufgeführten Controller-Upgrades auf Systemen mit ONTAP 9.12.1 oder 9.11.1 mit dem beschriebenen manuellen Upgrade durchführen "Hier".

Weitere Informationen zu Kombinationen von Plattformupgrades finden Sie in der Tabelle MetroCluster IP-Upgrade in "Wählen Sie ein Controller-Upgrade-Verfahren".

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

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Andere Komponenten in der Konfiguration, wie z. B. Storage Shelfs oder Switches, können nicht gleichzeitig aktualisiert werden.

- Dieses Verfahren gilt für Controller-Module in einer MetroCluster IP-Konfiguration mit vier Nodes, auf der ONTAP 9.13.1 oder höher ausgeführt wird.

  "NetApp Hardware Universe"

- Auf den MetroCluster Systemen muss an beiden Standorten dieselbe ONTAP-Version ausgeführt werden.
- Folgende Vorgehensweise eignet sich zum Upgrade von Controllern in einer MetroCluster IP-Konfiguration mit vier Nodes mithilfe von NSO-basiertem automatischem Switchover und Switchback.

  > Ein Upgrade mittels Aggregatverschiebung (Aggregate Relocation, ARL) mit Befehlen „System-Controller ersetzen“ wird für eine MetroCluster IP-Konfiguration mit vier Nodes nicht unterstützt.

- Sie müssen das automatische NSO-Controller-Upgrade durchführen, um die Controller an beiden Standorten nacheinander aktualisieren zu können.
- Durch dieses automatische NSO-basierte Controller-Upgrade-Verfahren können Sie den Controller-Ersatz an einen MetroCluster Disaster Recovery (DR)-Standort initiieren. Sie können jeweils nur einen Controller-Austausch an einem Standort initiieren.
- Um an Standort A einen Controller-Austausch zu initiieren, müssen Sie den Startbefehl für den Controller-Austausch von Standort B ausführen Der Vorgang leitet Sie weiter, Controller beider Nodes nur an Standort A zu ersetzen. Um die Controller an Standort B zu ersetzen, müssen Sie den Startbefehl für den Controller-Ersatz von Standort A ausführen Es wird eine Meldung angezeigt, in der der Standort identifiziert wird, an dem die Controller ersetzt werden.

Folgende Beispielnamen werden in diesem Verfahren verwendet:

- Standort_A
  - Vor dem Upgrade:
    - Node_A_1-alt
    - Node_A_2-alt
  - Nach dem Upgrade:
    - Node_A_1-neu
    - Node_A_2-neu
- Standort_B

- Vor dem Upgrade:
  - Node_B_1-alt
  - Node_B_2-alt
- Nach dem Upgrade:
  - Node_B_1-neu
  - Node_B_2-neu

Bereiten Sie sich auf das Upgrade vor

Zur Vorbereitung auf das Controller Upgrade müssen Sie die System-Vorabprüfungen durchführen und die Konfigurationsinformationen erfassen.

Wenn der ONTAP Mediator installiert ist, wird er vor Beginn der Vorabprüfungen automatisch erkannt und entfernt. Um das Entfernen zu bestätigen, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wenn Sie das Upgrade abgeschlossen haben oder die Vorabprüfungen fehlschlagen oder Sie das Upgrade nicht fortsetzen möchten, müssen Sie dies tun Konfigurieren Sie ONTAP Mediator manuell neu.

Während des Upgrades können Sie die ausführen `system controller replace show` Oder `system controller replace show-details` Befehl von Standort A, um den Status zu überprüfen. Wenn die Befehle eine leere Ausgabe zurückgeben, warten Sie einige Minuten, und führen Sie den Befehl erneut aus.

Schritte

1. Starten Sie das Verfahren zum automatischen Austausch der Controller von Standort A, um die Controller an Standort B zu ersetzen:

   ```
   system controller replace start -nso true
   ```

   Der automatisierte Vorgang führt die Vorabprüfungen durch. Wenn keine Probleme gefunden werden, wird der Vorgang angehalten, sodass Sie die konfigurationsbezogenen Informationen manuell erfassen können.

- Wenn Sie den nicht ausführen `system controller replace start -nso true` Befehl, das Controller-Upgrade wählt NSO basierte automatische Umschaltung und Switchback als Standardverfahren bei MetroCluster IP-Systemen.
- Das aktuelle Quellsystem und alle kompatiblen Zielsysteme werden angezeigt. Wenn Sie den Quell-Controller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang angehalten und ein Fehler meldet, nachdem die neuen Nodes gestartet wurden. Um den Cluster wieder in einen ordnungsgemäßen Zustand zu versetzen, müssen Sie die manuelle Recovery-Prozedur befolgen.

  Der `system controller replace start` Der Befehl meldet möglicherweise den folgenden Vorprüffehler:

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- --------------
-------------------------------------
Node-A-1    Failed         MetroCluster check failed.
Reason : MCC check showed errors in component aggregates
```

  Überprüfen Sie, ob dieser Fehler aufgetreten ist, weil Sie nicht gespiegelte Aggregate oder ein anderes Problem an Aggregaten haben. Vergewissern Sie sich, dass sich alle gespiegelten Aggregate in einem ordnungsgemäßen Zustand befinden und dass sie nicht beeinträchtigt bzw. gespiegelt werden. Wenn dieser Fehler nur auf nicht gespiegelte Aggregate zurückzuführen ist, können Sie diesen Fehler durch Auswahl des überschreiben `-skip-metrocluster-check true` Option auf der `system controller replace start` Befehl. Wenn auf Remote-Storage zugegriffen werden kann, sind die nicht gespiegelten Aggregate nach einer Umschaltung online. Falls die Remote-Storage-Verbindung ausfällt, können die nicht gespiegelten Aggregate nicht online geschaltet werden.

2. Erfassen Sie manuell die Konfigurationsinformationen, indem Sie sich bei Standort B anmelden und den Befehlen folgen, die in der Konsolenmeldung unter der aufgeführt sind `system controller replace show` Oder `system controller replace show-details` Befehl.

Sammeln von Informationen vor dem Upgrade

Vor dem Upgrade, wenn das Root-Volume verschlüsselt ist, müssen Sie den Sicherungsschlüssel und andere Informationen sammeln, um die neuen Controller mit den alten verschlüsselten Root-Volumes zu booten.

Über diese Aufgabe

Diese Aufgabe wird für die bestehende MetroCluster IP-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel für die vorhandenen Controller, damit Sie bei der Einrichtung der neuen Controller problemlos die Kabel identifizieren können.
2. Zeigen Sie die Befehle an, um den Backup-Schlüssel und weitere Informationen zu erfassen:

   `system controller replace show`

Führen Sie die unter aufgeführten Befehle aus `show` Befehl aus dem Partner-Cluster.

Der `show` In der Befehlsausgabe werden drei Tabellen angezeigt, die die MetroCluster-Schnittstellen-IPs, System-IDs und System-UUIDs enthalten. Diese Informationen sind später im Verfahren zum Festlegen der Bootargs erforderlich, wenn Sie den neuen Node booten.

3. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

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

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster-IP-Konfiguration mit vier Knoten werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260
   - Node_B_1-alt: 4068741254
   - Node_B_2-alt: 4068741256

   ```
   metrocluster-siteA::> 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-old    4068741258
   4068741260              4068741256             4068741256
   1                    Cluster_A       Node_A_2-old    4068741260
   4068741258              4068741254             4068741254
   1                    Cluster_B       Node_B_1-old    4068741254
   4068741256              4068741258             4068741260
   1                    Cluster_B       Node_B_2-old    4068741256
   4068741254              4068741260             4068741258
   4 entries were displayed.
   ```

   In diesem Beispiel für eine MetroCluster-IP-Konfiguration mit zwei Knoten werden die folgenden alten System-IDs abgerufen:

   - Node_A_1: 4068741258
   - Knoten_B_1: 4068741254

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

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `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`

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

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

6. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

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

7. 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 Verschlüsselungsmanagementinformationen".

   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
```

8. Setzen Sie den Vorgang fort, nachdem Sie die Konfigurationsinformationen erfasst haben:

```
system controller replace resume
```

Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration über den Tiebreaker oder eine andere Software entfernen, bevor der alte Controller ersetzt wird.

Schritte

1. "Entfernen der vorhandenen MetroCluster-Konfiguration" Über die Tiebreaker Software.
2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Ersetzen der alten Controller und Booten der neuen Controller

Nachdem Sie Informationen gesammelt und den Vorgang fortgesetzt haben, wird die Automatisierung mit dem Switchover fortgesetzt.

Über diese Aufgabe

Der Automatisierungsvorgang initiiert die Umschaltvorgänge. Nach Abschluss dieser Vorgänge wird der Vorgang bei **pausiert für Benutzereingriff** angehalten, sodass Sie die Controller racken und installieren können, die Partner-Controller hochfahren und die Root-Aggregat-Festplatten dem neuen Controller-Modul aus dem Flash-Backup mit dem neu zuweisen können `sysids` Früher gesammelt.

Bevor Sie beginnen

Vor dem Starten der Umschaltung hält der Automatisierungsvorgang pausiert, sodass Sie manuell überprüfen können, ob alle LIFs „`up`“ an Standort B. sind Ggf. Beliebige LIFs mit „`deigenen`“ bis „`up`“ bereitstellen und den Automatisierungsvorgang mit dem fortsetzen `system controller replace resume` Befehl.

Vorbereiten der Netzwerkkonfiguration der alten Controller

Um sicherzustellen, dass das Netzwerk auf den neuen Controllern ordnungsgemäß fortgesetzt wird, müssen Sie LIFs auf einen gemeinsamen Port verschieben und dann die Netzwerkkonfiguration der alten Controller entfernen.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie verwenden die in erfassten Informationen Bereiten Sie sich auf das Upgrade vor.

Schritte

1. Booten Sie die alten Nodes, und melden Sie sich dann bei den Nodes an:

   `boot_ontap`

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      `network interface show`

      Alle Daten-LIFS einschließlich SAN und NAS sind admin „`up`“ und betrieblich „`down`“, da sie sich am Switchover-Standort (Cluster_A) befinden.

   b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

      „`e0d`“ ist zum Beispiel ein physischer Port an alten Controllern und ist auch auf neuen Controllern vorhanden. „`e0d`“ wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

      Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

   c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

      `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

      Im folgenden Beispiel lautet „`e0d`“.

      Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Ändern Sie Broadcast-Domänen, um VLAN und physische Ports zu entfernen, die gelöscht werden müssen:

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Wiederholen Sie diesen Schritt für alle VLAN- und physischen Ports.

4. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und Schnittstellengruppen, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

   `network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

   Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN- und Interface Group-Ports aus der Broadcast-Domäne:

   `network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

   `ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

5. Anhalten der Knoten:

   `halt -inhibit-takeover true -node node-name`

   Dieser Schritt muss auf beiden Knoten durchgeführt werden.

Einrichten der neuen Controller

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Wenn die neuen Controller-Module nicht eigene FC-VI-Karten enthalten und FC-VI-Karten von alten Controllern mit neuen Controllern kompatibel sind, tauschen Sie FC-VI-Karten aus und installieren Sie diese in den richtigen Steckplätzen.

   Siehe "NetApp Hardware Universe" Für Slot-Informationen für FC-VI-Karten.

5. Verkabeln Sie die Strom-, seriellen Konsolen- und Managementverbindungen der Controller, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

Schließen Sie derzeit keine anderen Kabel an, die von den alten Controllern getrennt wurden.

"Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Eingabeaufforderung Strg-C, um die LOADER-Eingabeaufforderung anzuzeigen.

Netbootting der neuen Controller

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.

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

   Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit der Kernel-Datei enthalten: ontap-Version_image.tgz

   Sie müssen nicht die Datei ontap-Version_image.tgz extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

     ```
     ifconfig e0M -auto
     ```

   - Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

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

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

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
. 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`
```

```
Enter username/password if applicable, or press Enter to continue.
```

7. 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}
```

8. 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 der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   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.

Wiederherstellen der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA-Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
FC-Ziel	`fcadmin config -t target` *`adapter-name`*
FC-Initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl

CNA	`ucadmin show`
FC	`fcadmin show`

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte sein `mccip`.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mccip
   ```

   ```
   ha-config modify chassis mccip
   ```

3. Stoppen Sie den Knoten: `halt`

   Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

4. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `show date`
5. Stellen Sie bei Bedarf das Datum in UTC oder GMT ein: `set date <mm/dd/yyyy>`
6. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`
7. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`
8. Einstellungen speichern: `saveenv`
9. Umgebungsvariablen erfassen: `printenv`

Aktualisieren Sie die RCF-Dateien des Switches, um die neuen Plattformen aufzunehmen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

Befolgen Sie die im Abschnitt für den Switch-Anbieter aufgeführten Schritte im Abschnitt *MetroCluster IP Installation and Configuration*.

"Installation und Konfiguration von MetroCluster IP"

- "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
- "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"

2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Folgen Sie den Schritten im Abschnitt Ihres Switch-Anbieters vom "Installation und Konfiguration von MetroCluster IP".

   - "Herunterladen und Installieren der Broadcom RCF-Dateien"
   - "Herunterladen und Installieren der Cisco IP RCF-Dateien"

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

Für die neuen Controller-Module müssen bestimmte MetroCluster IP-Bootarg-Werte konfiguriert werden. Die Werte müssen mit den auf den alten Controller-Modulen konfigurierten übereinstimmen.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie die UUIDs und System-IDs, die bereits im Upgrade-Verfahren in identifiziert wurden "Sammeln von Informationen vor dem Upgrade".

Schritte

1. Am `LOADER>` Eingabeaufforderung: Legen Sie folgende Bootargs auf den neuen Knoten an Standort_B fest:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   Im folgenden Beispiel werden die Werte für Node_B_1 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   Im folgenden Beispiel werden die Werte für Node_B_2 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

2. Bei den neuen Nodes `LOADER` Eingabeaufforderung, UUUIDs festlegen:

   `setenv bootarg.mgwd.partner_cluster_uuid` *partner-cluster-UUID*

   `setenv bootarg.mgwd.cluster_uuid` *local-cluster-UUID*

   `setenv bootarg.mcc.pri_partner_uuid` *DR-partner-node-UUID*

   `setenv bootarg.mcc.aux_partner_uuid` *DR-aux-partner-node-UUID*

   `setenv bootarg.mcc_iscsi.node_uuid` *local-node-UUID*

   a. Legen Sie die UUIDs auf Node_B_1 fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1 gezeigt:

      ```
      setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
      setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
      00a098ca379f
      setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
      00a098908039
      ```

   b. Legen Sie die UUIDs auf Node_B_2 fest:

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2 gezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Wenn die Originalsysteme für ADP konfiguriert wurden, aktivieren Sie an der LOADER-Eingabeaufforderung der Ersatz-Nodes ADP:

   `setenv bootarg.mcc.adp_enabled true`

4. Legen Sie die folgenden Variablen fest:

   `setenv bootarg.mcc.local_config_id` *`original-sys-id`*

   `setenv bootarg.mcc.dr_partner` *`dr-partner-sys-id`*

   > Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls Node_B_1 gesetzt werden.

   a. Setzen Sie die Variablen auf Node_B_1.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1 gezeigt:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Setzen Sie die Variablen auf Node_B_2.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2 gezeigt:

   ```
   setenv bootarg.mcc.local_config_id 537403321
   setenv bootarg.mcc.dr_partner 537403323
   ```

5. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

   `setenv bootarg.kmip.init.ipaddr`

   `setenv bootarg.kmip.kmip.init.netmask`

   `setenv bootarg.kmip.kmip.init.gateway`

   `setenv bootarg.kmip.kmip.init.interface`

Neuzuweisen von Root-Aggregatfestplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul mithilfe des neu zu `sysids` Früher gesammelt

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln von Informationen vor dem Upgrade".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID

Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Beenden Sie das System und das Booten in den Wartungsmodus von der LOADER-Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
   node_B_1-old(4068741254)  node_B_1-old(4068741254)
   ...
   ```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   ```
   disk reassign -s old-sysid -d new-sysid
   ```

> Wenn Ihr MetroCluster IP-System mit erweiterter Festplattenpartitionierung konfiguriert ist, müssen Sie die ID des DR-Partnersystems angeben, indem Sie den ausführen `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid` Befehl.

Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

   ```
   disk show
   ```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Sie können VLANs und Schnittstellengruppen neu konfigurieren. Falls erforderlich, ändern Sie die Ports für die Cluster-LIFs und Broadcast-Domänen manuell, bevor Sie den Vorgang mit der fortsetzen `system controller replace resume` Befehl.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

4. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

5. Führen Sie im Startmenü die Option „`6`“ aus.

   > Mit der Option „`6`“ wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

Während eines Neustarts nach der Option „6“ wird die Bestätigungsaufforderung angezeigt `Override system ID? {y|n}` Angezeigt. Eingabe `y`.

6. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „10“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „11“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „10“ oder die Option „11“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „6“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „1“ (normaler Start) wiederholen.

7. Starten der Knoten:

```
boot_ontap
```

8. Warten Sie, bis die ersetzten Nodes gestartet werden.

   Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

9. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

   a. Broadcast-Domänen anzeigen:

   ```
   network port broadcast-domain show
   ```

   b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

   "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

   c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast-Domäne hostet.

   d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

   e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

"Erstellen einer Cluster-Peer-Beziehung"

f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

"Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

a. Überprüfen Sie, ob das Partner-Cluster erreichbar ist und ob die Konfiguration auf dem Partner-Cluster erfolgreich resynchronisiert ist:

```
metrocluster switchback -simulate true
```

10. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

11. Bevor Sie den Vorgang fortsetzen, überprüfen Sie, ob die MetroCluster ordnungsgemäß konfiguriert ist. Prüfen Sie den Knoten-Status:

```
metrocluster node show
```

Überprüfen Sie, ob sich die neuen Knoten (site_B) in **warten auf den Status wechseln** von site_A befinden

12. Vorgang fortsetzen:

```
system controller replace resume
```

Abschluss des Upgrades

Der Automatisierungsvorgang führt Überprüfungen des Verifikationssystems durch und hält anschließend Pausen ein, um die Erreichbarkeit des Netzwerks zu überprüfen. Nach der Überprüfung wird die Rückgewinnungsphase für die Ressourcen eingeleitet und der Automatisierungsvorgang führt den Wechsel zurück an Standort A durch und hält die Prüfungen nach dem Upgrade an. Nachdem Sie den Automatisierungsvorgang fortgesetzt haben, führt er die Prüfungen nach dem Upgrade durch und markiert, wenn keine Fehler erkannt werden, das Upgrade als abgeschlossen.

Schritte

1. Überprüfen Sie die Netzwerkzuwachbarkeit, indem Sie die Konsolenmeldung ausführen.
2. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

   ```
   system controller replace resume
   ```

3. Der Automatisierungsvorgang wird durchgeführt `heal-aggregate`, `heal-root-aggregate`, Und die Umschaltung Operationen an Standort A, und die nach dem Upgrade prüft. Wenn der Vorgang angehalten wird, überprüfen Sie den SAN-LIF-Status manuell und überprüfen Sie die Netzwerkkonfiguration anhand der Konsolenmeldung.
4. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

   ```
   system controller replace resume
   ```

5. Prüfen Sie den Status der Prüfungen nach der Aktualisierung:

   ```
   system controller replace show
   ```

   Wenn bei den Prüfungen nach der Aktualisierung keine Fehler gemeldet wurden, ist das Upgrade abgeschlossen.

6. Melden Sie sich nach Abschluss des Controller-Upgrades bei Standort B an und überprüfen Sie, ob die ersetzten Controller ordnungsgemäß konfiguriert sind.

Konfigurieren Sie ONTAP Mediator neu

Konfigurieren Sie ONTAP Mediator manuell, der vor dem Start des Upgrades automatisch entfernt wurde.

1. Verwenden Sie die Schritte in "Konfigurieren Sie den ONTAP Mediator-Dienst über eine MetroCluster-IP-Konfiguration".

Wiederherstellen des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Hinzufügen von MetroCluster Konfigurationen".

Controller-Upgrade in einer MetroCluster FC-Konfiguration durch Switchover und Switchback

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Unterstützte Plattformkombinationen

Bei bestimmten Plattformen können Sie in einer MetroCluster FC-Konfiguration über den Switchover- und Switchback-Betrieb aufrüsten.

Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster FC-

Upgrade-Tabelle in "Wählen Sie ein Controller-Upgrade-Verfahren".

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

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Andere Komponenten in der Konfiguration, wie z. B. Storage Shelfs oder Switches, können nicht gleichzeitig aktualisiert werden.

- Sie können dieses Verfahren mit bestimmten ONTAP-Versionen verwenden:
  - ONTAP 9.3 und höher unterstützen Konfigurationen mit zwei Nodes.
  - In ONTAP 9.8 und höher werden Konfigurationen mit vier oder acht Nodes unterstützt.

    Verwenden Sie diese Vorgehensweise nicht bei Konfigurationen mit vier oder acht Nodes und ONTAP Versionen vor 9.8.

- Ihre ursprünglichen und neuen Plattformen müssen kompatibel sein und unterstützt werden.

  "NetApp Hardware Universe"

  > Wenn die ursprünglichen oder neuen Plattformen FAS8020 oder AFF8020 Systeme mit den Ports 1c und 1d im FC-VI-Modus sind, lesen Sie den Knowledge Base-Artikel "Controller-Upgrade bei FCVI-Verbindungen auf vorhandenen FAS8020 oder AFF8020 Nodes verwenden die Ports 1c und 1d."

- Die Lizenzen an beiden Standorten müssen übereinstimmen. Sie können neue Lizenzen von beziehen "NetApp Support".
- Dieses Verfahren gilt für Controller-Module in einer MetroCluster FC-Konfiguration (eine Fabric-Attached MetroCluster Konfiguration mit zwei Nodes oder eine Fabric-Attached MetroCluster Konfiguration mit zwei, vier oder acht Nodes).
- Alle Controller in derselben DR-Gruppe sollten während des gleichen Wartungszeitraums aktualisiert werden.

  Das Bebetreiben der MetroCluster-Konfiguration mit unterschiedlichen Controller-Typen in derselben DR-Gruppe wird außerhalb dieser Wartungsaktivitäten nicht unterstützt. Bei MetroCluster Konfigurationen mit acht Nodes müssen die Controller in einer DR-Gruppe identisch sein. Jedoch können beide DR-Gruppen unterschiedliche Controller-Typen verwenden.

- Für eine vorab-Zuordnung von Storage-, FC- und Ethernet-Verbindungen zwischen Original-Nodes und neuen Nodes wird empfohlen.
- 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.

  Weitere Informationen finden Sie im "NetApp Hardware Universe"

Folgende Beispielnamen werden in diesem Verfahren verwendet:

- Standort_A

    - Vor dem Upgrade:
        - Node_A_1-alt
        - Node_A_2-alt
    - Nach dem Upgrade:
        - Node_A_1-neu
        - Node_A_2-neu
- Standort_B
    - Vor dem Upgrade:
        - Node_B_1-alt
        - Node_B_2-alt
    - Nach dem Upgrade:
        - Node_B_1-neu
        - Node_B_2-neu

Vorbereitung auf das Upgrade

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die neuen Plattformen vorbereiten und andere verschiedene Aufgaben ausführen.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

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`

    Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

    b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

    ```
    storage disk show -broken
    ```

    Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

    c. Überprüfen Sie auf Statusmeldungen:

    ```
    system health alert show
    ```

    Sie sollten diesen Befehl für jedes Cluster ausgeben.

    d. Überprüfen Sie die Lizenzen auf den Clustern:

    ```
    system license show
    ```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

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

```
storage switch show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

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

```
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
```

4. 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.

Zuordnen von Ports von den alten Nodes zu den neuen Nodes

Sie müssen die Zuordnung der LIFs zu physischen Ports auf den alten Nodes zu den physischen Ports auf den neuen Nodes planen.

Über diese Aufgabe

Wenn der neue Node zum ersten Mal während des Upgrades gebootet wird, stellt er die aktuellste

Konfiguration des alten Node wieder dar, der ersetzt wird. Wenn Sie Node_A_1-New booten, versucht ONTAP, LIFs auf denselben Ports zu hosten, die in Node_A_1-old verwendet wurden. Deshalb müssen Sie im Rahmen des Upgrades die Port- und LIF-Konfiguration anpassen, sodass diese mit der der des alten Node kompatibel ist. Während des Upgrades führen Sie sowohl für die alten als auch für die neuen Nodes Schritte durch, um eine korrekte Cluster-, Management- und Daten-LIF-Konfiguration sicherzustellen.

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 Cluster-Ports neu erstellen."Vorbereiten von Cluster-Ports auf einem vorhandenen Controller-Modul"
e0c, e0d	e0a, e0b, e0c, e0d	e0c und e0d sind passende Anschlüsse. Sie müssen die Konfiguration nicht ändern, aber nach einem Upgrade können Sie die Cluster-LIFs über 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 von erfassen "NetApp Hardware Universe".

   Identifizieren Sie außerdem die Auslastung des FC-VI-Kartensteckplatzes.

2. Planen Sie Ihre Portnutzung und füllen Sie auf Wunsch 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						

Sammeln von Informationen vor dem Upgrade

Vor der Aktualisierung müssen Sie Informationen für jeden der alten Knoten erfassen und bei Bedarf die Netzwerk-Broadcast-Domänen anpassen, VLANs und Schnittstellengruppen entfernen und Verschlüsselungsinformationen sammeln.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel der vorhandenen Controller, damit Sie beim Einrichten der neuen Controller Kabel problemlos identifizieren können.
2. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

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

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260
   - Node_B_1-alt: 4068741254
   - Node_B_2-alt: 4068741256

```
metrocluster-siteA::> 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-old
4068741258              4068741260                       4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                       4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                        4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                       4068741260
4068741258
4 entries were displayed.
```

In diesem Beispiel für eine MetroCluster FC-Konfiguration mit zwei Nodes werden die folgenden alten System-IDs abgerufen:

- Node_A_1: 4068741258
- Knoten_B_1: 4068741254

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

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `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`

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `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 das Schlüsselmanagement 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 Verschlüsselungsmanagementinformationen".

   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
   ```

Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "Entfernen von MetroCluster-Konfigurationen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

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 die Wartung läuft.

   a. Geben Sie den folgenden Befehl ein:

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

      `maintenance-window-in-hours` 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
```

   a. Wiederholen Sie den Befehl im Partner-Cluster.

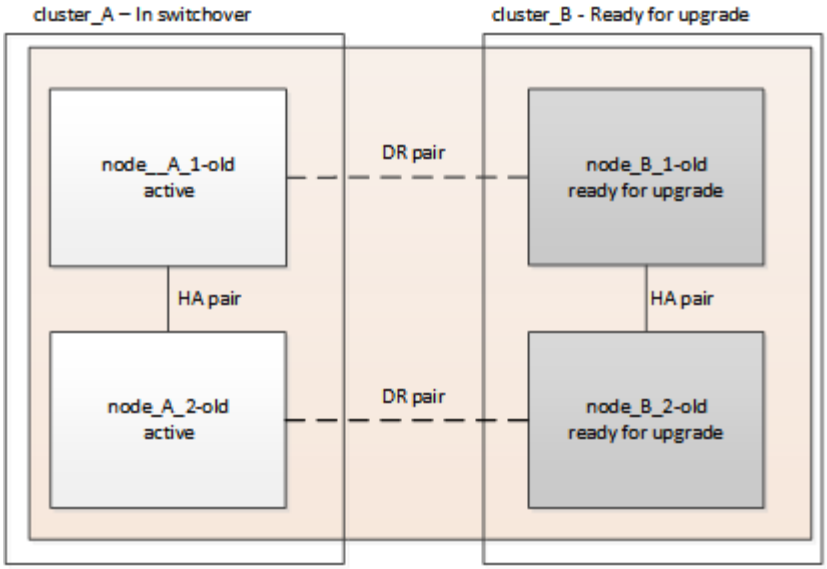
Umschalten der MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Cluster_A aktiv und stellt Daten für beide Standorte bereit. Cluster_B ist inaktiv und bereit, den Upgrade-Prozess zu starten, wie in der folgenden Abbildung dargestellt.



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Wählen Sie die Option aus, die Ihrer Konfiguration entspricht, und geben Sie den korrekten Befehl auf Cluster_A aus:

   > **Option 1: FC-Konfiguration mit vier oder acht Nodes und ONTAP 9.8 oder höher**
   >
   > Führen Sie den Befehl aus: `metrocluster switchover -controller-replacement true`
   >
   > **Option 2: FC-Konfiguration mit zwei Nodes und ONTAP 9.3 und höher**
   >
   > Führen Sie den Befehl aus: `metrocluster switchover`

   Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   d. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

2. Heilen Sie die Datenaggregate.

   a. Heilen der Datenaggregate:

   ```
   metrocluster heal data-aggregates
   ```

   b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster`

`operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Heilen Sie die Root-Aggregate.
   a. Heilen der Datenaggregate:

      ```
      metrocluster heal root-aggregates
      ```

   b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

      ```
      cluster_A::> metrocluster operation show
        Operation: heal-root-aggregates
            State: successful
       Start Time: 7/29/2020 20:58:41
         End Time: 7/29/2020 20:59:42
           Errors: -
      ```

Vorbereiten der Netzwerkkonfiguration der alten Controller

Um sicherzustellen, dass das Netzwerk auf den neuen Controllern ordnungsgemäß fortgesetzt wird, müssen Sie LIFs auf einen gemeinsamen Port verschieben und dann die Netzwerkkonfiguration der alten Controller entfernen.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie verwenden die in erfassten Informationen "Zuordnen von Ports von den alten Nodes zu den neuen Nodes".

Schritte

1. Booten Sie die alten Nodes, und melden Sie sich dann bei den Nodes an:

   ```
   boot_ontap
   ```

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      ```
      network interface show
      ```

Alle Daten-LIFS einschließlich SAN und NAS befinden sich in Betrieb, da sie sich am Switchover-Standort (Cluster_A) befinden.

b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

   e0d ist zum Beispiel ein physischer Port auf den alten Controllern und ist auch auf neuen Controllern vorhanden. e0d wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

   Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

   Im folgenden Beispiel ist dies "e0d".

   Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Ändern Sie Broadcast-Domänen, um vlan und physische Ports zu entfernen, die gelöscht werden müssen:

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Wiederholen Sie diesen Schritt für alle VLAN- und physischen Ports.

4. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und ifgrps, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

   b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

      `network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

      Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

   a. Entfernen Sie VLAN und Interface Group Ports aus Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Anhalten der Knoten:

```
halt -inhibit-takeover true -node node-name
```

Dieser Schritt muss auf beiden Knoten durchgeführt werden.

Entfernen der alten Plattformen

Die alten Controller müssen aus der Konfiguration entfernt werden.

Über diese Aufgabe

Diese Aufgabe wird auf Site_B. ausgeführt

Schritte

1. Stellen Sie eine Verbindung mit der seriellen Konsole der alten Controller (Node_B_1-old und Node_B_2-old) an Site_B her, und überprüfen Sie, dass die LOADER-Eingabeaufforderung angezeigt wird.
2. Trennen Sie die Speicher- und Netzwerkverbindungen auf Node_B_1-old und Node_B_2-old, und kennzeichnen Sie die Kabel, damit sie wieder mit den neuen Nodes verbunden werden können.
3. Trennen Sie die Stromkabel von Node_B_1-old und Node_B_2-old.
4. Entfernen Sie die Controller Node_B_1-old und Node_B_2-old aus dem Rack.

Konfigurieren der neuen Controller

Sie müssen die Controller im Rack unterbringen und installieren, die erforderliche Einrichtung im Wartungsmodus durchführen und dann die Controller booten und die LIF-Konfiguration auf den Controllern überprüfen.

Einrichten der neuen Controller

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Wenn die neuen Controller-Module nicht eigene FC-VI-Karten enthalten und FC-VI-Karten von alten

Controllern mit neuen Controllern kompatibel sind, tauschen Sie FC-VI-Karten aus und installieren Sie diese in den richtigen Steckplätzen.

Siehe "NetApp Hardware Universe" Für Slot-Informationen für FC-VI-Karten.

5. Verkabeln Sie die Strom-, seriellen Konsolen- und Managementverbindungen der Controller, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

   Schließen Sie derzeit keine anderen Kabel an, die von den alten Controllern getrennt wurden.

   "Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Eingabeaufforderung Strg-C, um die LOADER-Eingabeaufforderung anzuzeigen.

Netbootting der neuen Controller

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.

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	Extrahieren Sie den Inhalt der ontap-Version_image.tgzfile in das Zielverzeichnis: Tar -zxvf ontap-Version_image.tgz HINWEIS: Wenn Sie den Inhalt auf Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot Image zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: ontap-Version_image.tgz Sie müssen nicht die ontap-Version_image.tgz-Datei extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

```
ifconfig e0M -auto
```

- Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

```
ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

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

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

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . 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`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. 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}
   ```

8. 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 der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   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.

Wiederherstellen der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA-Ethernet	`ucadmin modify -mode cna` *`adapter-name`*

FC-Ziel	`fcadmin config -t target` *`adapter-name`*
FC-Initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Einstellen des HA-Status auf den neuen Controllern und dem Chassis

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   der HA-Status für alle Komponenten sollte mcc sein.

Wenn die MetroCluster-Konfiguration…	Der HA-Status sollte…
Zwei Nodes	mcc-2n
Vier oder acht Nodes	mcc

2. Wenn der angezeigte Systemzustand des Controllers nicht richtig ist, setzen Sie den HA-Status für das Controller-Modul und das Chassis:

Wenn die MetroCluster-Konfiguration…	Geben Sie diese Befehle ein…

Zwei Knoten	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Vier oder acht Knoten	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Neuzuweisen von Root-Aggregatfestplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln von Informationen vor dem Upgrade".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Beenden Sie das System und das Booten in den Wartungsmodus von der LOADER-Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   `disk reassign -s old-sysid -d new-sysid`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status           Options
   aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                            mirrored
   mirror_resync_priority=high(fixed)
                            fast zeroed
                            64-bit
   ```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

4. Wenn Sie die Stammverschlüsselung verwenden, wählen Sie je nach der verwendeten ONTAP-Version die Startmenü-Option oder geben Sie den Startmenü-Befehl für Ihre Konfiguration für die Schlüsselverwaltung aus.

ONTAP 9.8 und höher

Ab ONTAP 9.8 wählen Sie die Startmenü-Option.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

ONTAP 9.7 und frühere Versionen

Geben Sie bei ONTAP 9.7 und früheren Versionen den Befehl des Startmenüs ein.

Sie verwenden…	Geben Sie diesen Befehl an der Eingabeaufforderung des Startmenüs aus…
Integriertes Verschlüsselungsmanagement	`recover_onboard_keymanager`
Externes Verschlüsselungskeymanagement	`recover_external_keymanager`

5. Wenn Autoboot aktiviert ist, unterbrechen Sie den Autoboot, indem Sie STRG-C. drücken
6. Führen Sie im Startmenü die Option „`6`“ aus.

   Mit der Option „`6`“ wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist:

   ```
   printenv partner-sysid
   ```

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

8. Wenn Sie die Stammverschlüsselung verwenden, wählen Sie je nach der verwendeten ONTAP-Version die Startmenü-Option oder geben Sie den Startmenü-Befehl für Ihre Konfiguration für das Verschlüsselungsmanagement erneut aus.

   ONTAP 9.8 und höher

   Ab ONTAP 9.8 wählen Sie die Startmenü-Option.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

   Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „`6`“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

   ONTAP 9.7 und frühere Versionen

   Geben Sie bei ONTAP 9.7 und früheren Versionen den Befehl des Startmenüs ein.

Sie verwenden…	Geben Sie diesen Befehl an der Eingabeaufforderung des Startmenüs aus…
Integriertes Verschlüsselungsmanagement	`recover_onboard_keymanager`
Externes Verschlüsselungskeymanagement	`recover_external_keymanager`

   Möglicherweise müssen Sie die ausgeben `recover_xxxxxxxx_keymanager` Befehl wird mehrmals am Boot-Menü angezeigt, bis die Nodes vollständig gebootet werden.

9. Starten der Knoten:

   ```
   boot_ontap
   ```

10. Warten Sie, bis die ersetzten Nodes gestartet werden.

Führen Sie ein Giveback durch, wenn sich einer der beiden Knoten im Übernahmemodus befindet:

```
storage failover giveback
```

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

    ```
    network port broadcast-domain show
    ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

    "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast Domain hostet.

    d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

    e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

    Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

    "Erstellen einer Cluster-Peer-Beziehung"

    f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

    VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

    "Erstellen eines VLANs"

    "Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

LIF-Konfiguration wird überprüft

Stellen Sie vor dem Wechsel sicher, dass LIFs auf den entsprechenden Nodes/Ports gehostet werden. Folgende Schritte sind auszuführen

Über diese Aufgabe

Diese Aufgabe wird in Site_B ausgeführt, wo die Nodes mit Root-Aggregaten gestartet wurden.

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Wenn Sie den eingeben `network interface modify` Befehl im `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können die erstellen `network interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   ```
   network interface revert * -vserver vserver-name
   ```

   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Installieren Sie die neuen Lizenzen

Vor dem Wechsel-Back-Vorgang müssen Sie Lizenzen für die neuen Controller installieren.

Schritte

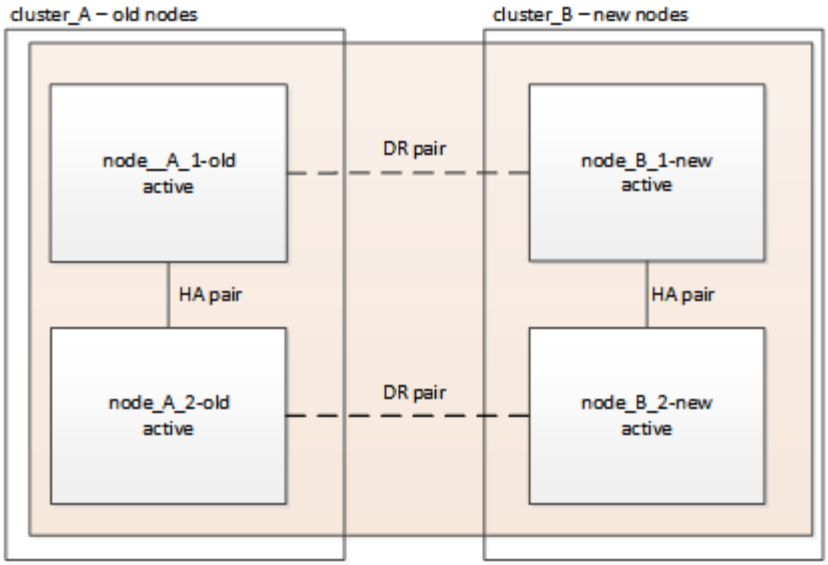
1. "Installieren von Lizenzen für das neue Controller-Modul"

Umschalten der MetroCluster-Konfiguration

Nachdem die neuen Controller konfiguriert wurden, schalten Sie die MetroCluster Konfiguration zurück und kehren den normalen Betrieb zurück.

Über diese Aufgabe

In dieser Aufgabe führen Sie den Vorgang zum Zurückkehren aus und kehren die MetroCluster-Konfiguration in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Zurückwechseln des Clusters:

   ```
   metrocluster switchback
   ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

   ```
   cluster_B::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_B         Configuration state configured
                             Mode                switchover
                             AUSO Failure Domain -
   Remote: cluster_A         Configuration state configured
                             Mode                waiting-for-switchback
                             AUSO Failure Domain -
   ```

   Der Umkehrvorgang ist abgeschlossen, wenn die Ausgabe angezeigt wird `normal`:

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

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:

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

   ```
   metrocluster show
   ```

   b. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   > Nach dem Ausführen von `metrocluster check run` Und `metrocluster check show`, Sie sehen eine Fehlermeldung ähnlich der folgenden:

   Beispiel

   ```
   Failed to validate the node and cluster components before the switchover
   operation.
                    Cluster_A:: node_A_1 (non-overridable veto): DR
   partner NVLog mirroring is not online. Make sure that the links between
   the two sites are healthy and properly configured.
   ```

+ Dieses Verhalten wird aufgrund einer Controller-Diskrepanz während des Upgrade-Prozesses erwartet und die Fehlermeldung kann sicher ignoriert werden.

Aktualisieren der Knoten auf Cluster_A

Sie müssen die Upgrade-Aufgaben auf „Cluster_A“ wiederholen

Schritt

1. Wiederholen Sie die Schritte, um die Nodes auf Cluster_A zu aktualisieren. Beginnen Sie mit "Vorbereitung auf das Upgrade".

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Clustern und Nodes umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

Senden einer benutzerdefinierten AutoSupport Meldung nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritt

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:

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

   b. Wiederholen Sie den Befehl im Partner-Cluster.

Wiederherstellen des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Hinzufügen von MetroCluster Konfigurationen" In *MetroCluster Tiebreaker Installation und Konfiguration*.

Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher)

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Im Rahmen dieses Verfahrens können Sie keine weiteren Komponenten (z. B. Storage Shelves oder Switches) aktualisieren.

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Sie können keine anderen Komponenten in der Konfiguration, wie Storage Shelfs oder Switches, gleichzeitig aktualisieren.

- Sie können dieses Verfahren zum Upgrade einer AFF A700 auf AFF A900 mit ONTAP 9.10.1 oder höher verwenden.
- Sie können dieses Verfahren zum Upgrade einer FAS9000 auf FAS9500 mit ONTAP 9.10.1P3 und höher verwenden.
  - In ONTAP 9.10.1 und höher werden Konfigurationen mit vier und acht Nodes unterstützt.

    Das AFF A900 System wird nur ab ONTAP 9.10.1 unterstützt.

  "NetApp Hardware Universe"

- Upgrades für alle Controller der Konfiguration sollten während des gleichen Wartungszeitraums durchgeführt werden.

  In der folgenden Tabelle ist die unterstützte Modellmatrix für das Controller-Upgrade aufgeführt.

Altes Plattform-Modell	Neues Plattformmodell
• AFF A700	• AFF A900
• FAS9000	• FAS9500

- Während des Upgrade-Verfahrens müssen Sie die MetroCluster Fabric ändern, einschließlich RCF und physischen Kabeländerungen. Sie können die RCF- und Verkabelungsänderungen durchführen, bevor Sie die Controller-Aktualisierung durchführen.
- Für dieses Upgrade sind keine Änderungen der Storage-, FC- und Ethernet-Verbindungen zwischen den ursprünglichen Nodes und den neuen Nodes erforderlich.
- Während des Upgrades sollten Sie keine anderen Karten zum AFF A700 oder FAS9000 System hinzufügen oder entfernen. Weitere Informationen finden Sie im "NetApp Hardware Universe"

Folgende Beispielnamen werden in Beispielen und Grafiken in diesem Verfahren verwendet:

- Standort_A
  - Vor dem Upgrade:
    - Node_A_1-A700
    - Node_A_2-A700
  - Nach dem Upgrade:
    - Node_A_1-A900
    - Node_A_2-A900
- Standort_B
  - Vor dem Upgrade:
    - Node_B_1-A700

        - Node_B_2-A700
    - Nach dem Upgrade:
        - Node_B_1-A900
        - Node_B_2-A900

Bereiten Sie sich auf das Upgrade vor

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die RCF-Dateien und die Verkabelung mit der neuen für die AFF A900 oder FAS9000 Fabric MetroCluster-Konfiguration erforderlichen Port-Konnektivitätstopologie abstimmen und weitere verschiedene Aufgaben ausführen.

Steckplatz 7 am AFF A700 Controller löschen

Die MetroCluster Konfiguration auf einem AFF A900 oder FAS9500 erfordert 8 FC-VI-Ports über FC-VI-Karten in den Steckplätzen 5 und 7. Wenn beim AFF A700 oder der FAS9000 Karten in Steckplatz 7 vorhanden sind, müssen Sie die Karten in andere Steckplätze für alle Nodes des Clusters verschieben.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Bevor Sie die RCF-Dateien und die Verkabelung für die Fabric MetroCluster-Konfiguration von AFF A900 oder FAS9500 aktualisieren, müssen Sie den Zustand und die Konnektivität der 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`

    Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

    b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

    ```
    storage disk show -broken
    ```

    Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

    c. Überprüfen Sie auf Statusmeldungen:

    ```
    system health alert show
    ```

    Sie sollten diesen Befehl für jedes Cluster ausgeben.

    d. Überprüfen Sie die Lizenzen auf den Clustern:

    ```
    system license show
    ```

    Sie sollten diesen Befehl für jedes Cluster ausgeben.

    e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

    ```
    network device-discovery show
    ```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

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

```
storage switch show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

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

```
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
```

4. 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.

Aktualisieren Sie die RCF-Dateien des Fabric Switch

Für die AFF A900 oder FAS9500 Fabric MetroCluster sind zwei FC-VI-Adapter mit vier Ports pro Node erforderlich, im Vergleich zu einem FC-VI-Adapter mit vier Ports, den eine AFF A700 benötigt. Bevor Sie das Controller-Upgrade auf den AFF A900 oder FAS9500 Controller starten, müssen Sie die Fabric Switch RCF-Dateien ändern, um die AFF A900 oder FAS9500 Verbindungstopologie zu unterstützen.

1. Von "Download-Seite für MetroCluster RCF-Dateien", Laden Sie die korrekte RCF-Datei für ein AFF A900 oder FAS9500 Fabric MetroCluster sowie das Switch-Modell herunter, das in der AFF A700 oder FAS9000 Konfiguration verwendet wird.
2. Aktualisieren Sie die RCF-Datei auf den Fabric-A-Schaltern, wechseln Sie A1 und wechseln Sie B1, indem Sie die Schritte unter befolgen "Konfigurieren der FC-Switches".

> Das RCF-Dateiupdate zur Unterstützung der AFF A900 oder FAS9500 Fabric MetroCluster-Konfiguration hat keine Auswirkungen auf die Ports und Verbindungen, die für die Konfiguration der AFF A700 oder FAS9000 Fabric MetroCluster verwendet werden.

3. Nach Aktualisierung der RCF-Dateien auf den Fabric A Switches sollten alle Storage- und FC-VI-Verbindungen online geschaltet werden. Prüfen Sie die FC-VI-Verbindungen:

   ```
   metrocluster interconnect mirror show
   ```

   a. Vergewissern Sie sich, dass die lokalen und Remote-Standortlaufwerke in aufgeführt sind `sysconfig` Ausgabe:

4. nach der RCF-Dateiaktualisierung für Fabric A-Switches müssen Sie überprüfen, ob sich MetroCluster in einem ordnungsgemäßen Zustand befindet.

   a. Verbindungen des Metro-Clusters prüfen: `metrocluster interconnect mirror show`

   b. MetroCluster-Prüfung ausführen: `metrocluster check run`

   c. Nach Abschluss des Laufes sind die Ergebnisse der MetroCluster-Ausführung zu sehen: `metrocluster check show`

5. Aktualisieren Sie die Fabric-B-Schalter (Schalter 2 und 4), indem Sie sich wiederholen Schritt 2 Bis Schritt 5.

Überprüfen Sie nach dem Update der RCF-Datei den Zustand der MetroCluster-Konfiguration

Sie müssen den Zustand und die Konnektivität der MetroCluster Konfiguration überprüfen, bevor Sie das Upgrade durchführen.

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`

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

   ```
   storage disk show -broken
   ```

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   c. Überprüfen Sie auf Statusmeldungen:

   ```
   system health alert show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

   ```
   system license show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

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

```
storage switch show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

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

```
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
```

4. 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.

Zuordnung der Ports des AFF A700 oder FAS9000 Nodes zu den AFF A900 oder FAS9500 Nodes

Während des Controller-Upgrades dürfen nur die in diesem Verfahren erwähnten Verbindungen geändert werden.

Wenn die AFF A700 oder FAS9000 Controller über eine Karte in Steckplatz 7 verfügen, sollten Sie sie in einen anderen Steckplatz verschieben, bevor Sie das Controller-Upgrade durchführen. Sie müssen Steckplatz 7 für die Hinzufügung des zweiten FC-VI-Adapters besitzen, der für die Funktionsweise von Fabric MetroCluster auf den AFF A900 oder FAS9500 Controllern erforderlich ist.

Sammeln Sie vor dem Upgrade Informationen

Vor der Aktualisierung müssen Sie Informationen für jeden der alten Knoten erfassen und bei Bedarf die Netzwerk-Broadcast-Domänen anpassen, VLANs und Schnittstellengruppen entfernen und Verschlüsselungsinformationen sammeln.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Erfassen der System-IDs für die MetroCluster-Konfiguration-Nodes:

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

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-A700: 537037649
   - Node_A_2-A700: 537407030
   - Node_B_1-A700: 0537407114
   - Node_B_2-A700: 537035354

   ```
   Cluster_A::*> 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  nodeA_1-A700   537407114     537035354
   537411005           537410611
   1           Cluster_A  nodeA_2-A700   537035354     537407114
   537410611           537411005
   1           Cluster_B  nodeB_1-A700   537410611     537411005
   537035354           537407114
   1           Cluster_B  nodeB_2-A700   537411005

   4 entries were displayed.
   ```

2. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `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`

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

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

4. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

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

5. 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 Verschlüsselungsmanagementinformationen".

   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
   ```

Entfernen Sie die vorhandene Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "Entfernen von MetroCluster-Konfigurationen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

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. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit die Wartung läuft.

   a. Geben Sie den folgenden Befehl ein:

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

      `maintenance-window-in-hours` 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
```

   a. Wiederholen Sie den Befehl im Partner-Cluster.

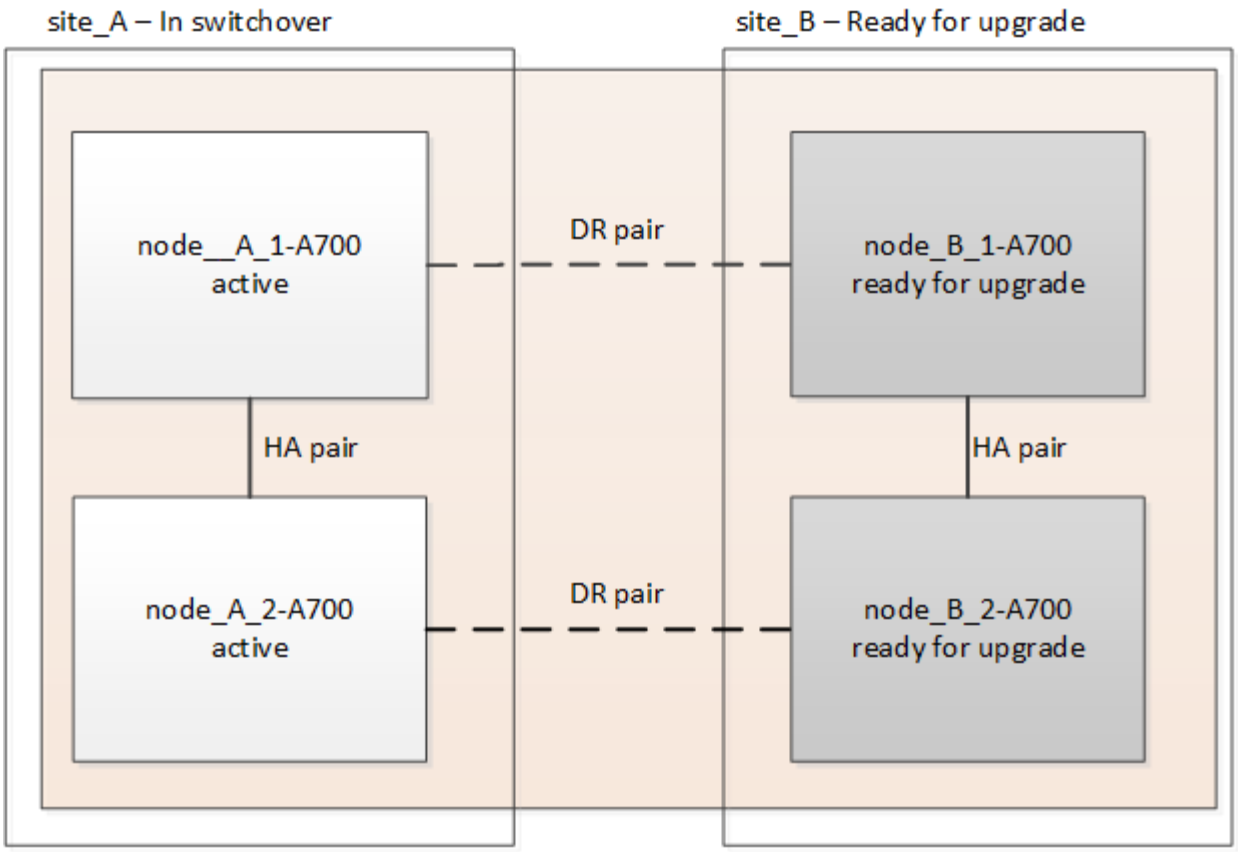
Wechseln Sie über die MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Site_A aktiv und stellt Daten für beide Standorte bereit. Site_B ist inaktiv und bereit, den Upgrade-Prozess zu starten, wie in der folgenden Abbildung dargestellt. (Diese Abbildung gilt auch für das Upgrade einer FAS9000 auf einen FAS9500 Controller.)



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl auf Site_A aus:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Der Vorgang kann einige Minuten dauern.

   a. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   b. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   c. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

2. Heilen Sie die Datenaggregate.

   a. Heilen der Datenaggregate:

   ```
   metrocluster heal data-aggregates
   ```

b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Heilen Sie die Root-Aggregate.

a. Heilen der Datenaggregate:

```
metrocluster heal root-aggregates
```

b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul und den NVS an Site_B

Sie müssen die alten Controller aus der Konfiguration entfernen.

Sie führen diese Aufgabe auf Site_B. aus

Bevor Sie beginnen

Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Schritte

1. Stellen Sie eine Verbindung zur seriellen Konsole der alten Controller (Node_B_1-700 und Node_B_2-700) an Site_B her, und überprüfen Sie, ob der angezeigt wird `LOADER` Eingabeaufforderung:
2. Ermitteln Sie die Bootarg-Werte von beiden Knoten an Site_B: `printenv`
3. Schalten Sie das Chassis an Site_B. aus

Entfernen Sie das Controller-Modul und den NVS von beiden Nodes an Site_B

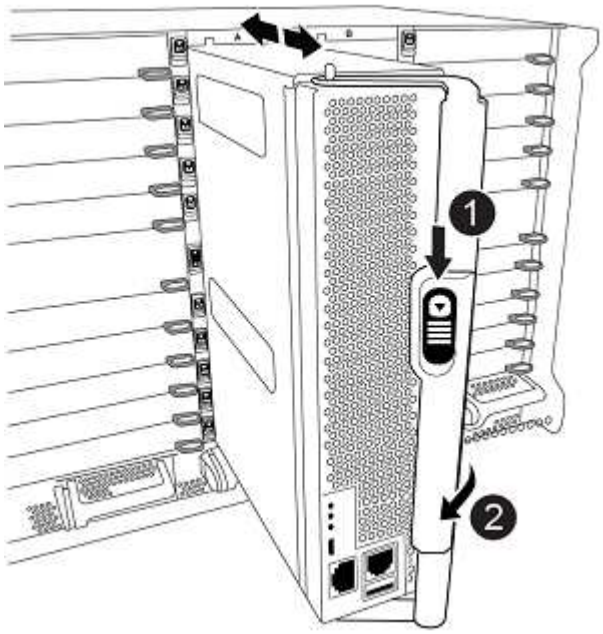
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

Gehen Sie wie folgt vor, um das AFF A700 oder das FAS9000 Controller-Modul zu entfernen.

Schritte

1. Trennen Sie gegebenenfalls das Konsolenkabel und das Managementkabel vom Controller-Modul, bevor Sie das Controller-Modul entfernen.
2. Entriegeln und entfernen Sie das Controller-Modul aus dem Gehäuse.

   a. Schieben Sie die orangefarbene Taste am Nockengriff nach unten, bis sie entsperrt ist.



	Freigabetaste für den CAM-Griff
	CAM-Griff

   a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse. Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul wie folgt:

> Das AFF A700 oder FAS9000 NVS-Modul befindet sich in Steckplatz 6 und ist im Vergleich zu den anderen Modulen im System doppelt so hoch.

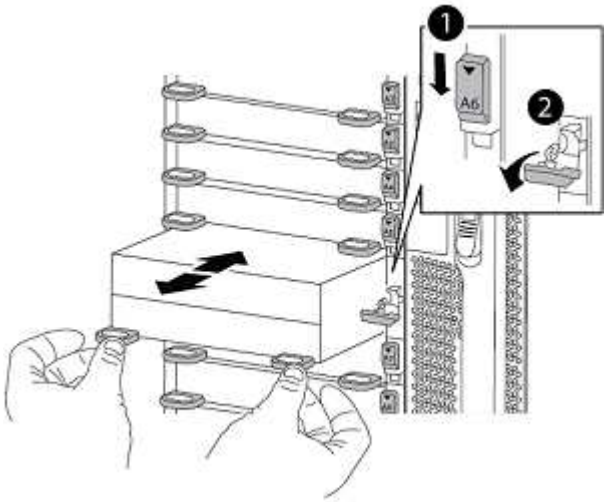
1. Entriegeln und entfernen Sie den NVS aus Steckplatz 6.

   a. Drücken Sie die Taste mit der Nummerierung und dem Buchstaben. Die Nockentaste bewegt sich vom Gehäuse weg.

   b. Drehen Sie die Nockenverriegelung nach unten, bis sie sich in horizontaler Position befindet. Der NVS

löst sich aus dem Gehäuse und bewegt sich ein paar Zentimeter.

c. Entfernen Sie den NVS aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

- Übertragen Sie keine Add-On-Module, die als Coredump-Geräte auf dem nichtflüchtigen Speichermodul AFF A700 in Steckplatz 6 verwendet werden, auf das AFF A900 NVS-Modul. Übertragen Sie keine Teile vom AFF A700-Controller und NVS-Modulen auf das AFF A900-Controller-Modul.
- Bei Upgrades von FAS9000 zu FAS9500 sollten Sie Flash Cache Module des FAS9000 NVS-Moduls nur in das FAS9500 NVS-Modul übertragen. Übertragen Sie keine anderen Teile vom FAS9000 Controller und NVS-Modulen auf das FAS9500 Controller-Modul.

Installieren Sie das AFF A900 oder FAS9500 NVS und das Controller-Modul

Sie müssen das AFF A900 oder FAS9500 NVS und das Controller-Modul aus dem Upgrade-Kit auf beiden Knoten in Site_B. installieren Verschieben Sie das coredump-Gerät nicht vom AFF A700 oder FAS9000 NVS-Modul in das AFF A900 oder FAS9500 NVS Modul.

Bevor Sie beginnen

Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

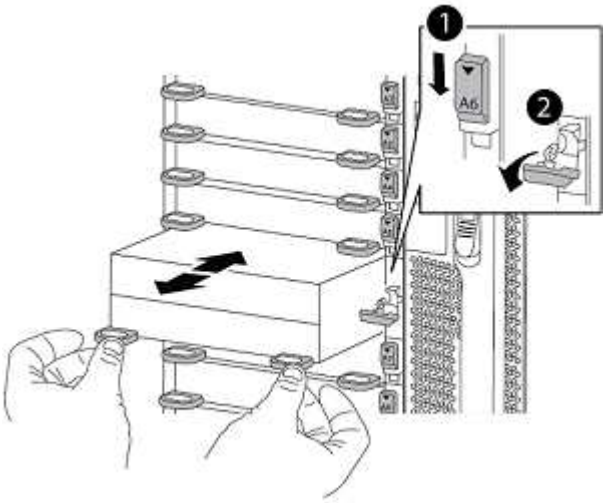
Installieren Sie den AFF A900 oder FAS9500 NVS

Gehen Sie wie folgt vor, um den AFF A900 oder FAS9500 NVS in Steckplatz 6 beider Nodes an Site_B zu installieren

Schritte

1. Richten Sie den NVS an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie den NVS vorsichtig in den Schlitz, bis der vorletzte und nummerierte E/A-Nockenriegel mit

dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVS.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

Installieren Sie das AFF A900 oder FAS9500 Controller-Modul

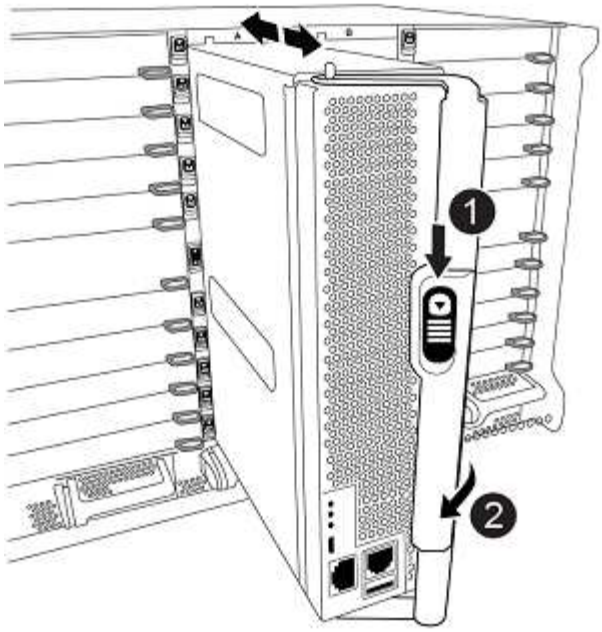
Gehen Sie wie folgt vor, um das AFF A900 oder FAS9500 Controller-Modul zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
2. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist.

   Beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden, um Schäden an den Anschlüssen zu vermeiden.

3. Verkabeln Sie die Management- und Konsolen-Ports mit dem Controller-Modul.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

4. Installieren Sie die zweite X91129A-Karte in Steckplatz 7 jedes Knotens.
   a. Verbinden Sie die FC-VI-Ports aus Steckplatz 7 mit den Switches. Siehe "Installation und Konfiguration über Fabric-Attached Storage" Dokumentation und gehen Sie zu den AFF A900 oder FAS9500 Fabric MetroCluster Verbindungsanforderungen für den Switch-Typ in Ihrer Umgebung.
5. Schalten Sie das Chassis EIN, und verbinden Sie die serielle Konsole.
6. Wenn der Knoten nach der BIOS-Initialisierung den Autoboot startet, unterbrechen Sie DEN AUTOBOOT, indem Sie Control-C drücken
7. Nachdem Sie den Autoboot unterbrochen haben, werden die Nodes an der LOADER-Eingabeaufforderung angehalten. Wenn Sie die automatische Bootzeit nicht unterbrechen und node1 den Startvorgang startet, warten Sie, bis die Eingabeaufforderung Control-C drücken kann, um in das Startmenü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option 8, um den Node neu zu booten und den Autoboot während des Neubootens zu unterbrechen.
8. Am `LOADER` Geben Sie die Standardvariablen für die Umgebung an: `set-defaults`
9. Speichern Sie die Standardeinstellungen für Umgebungsvariablen: `saveenv`

Netzboot der Nodes über Site_B

Nach Austausch des AFF A900 oder FAS9500 Controller-Moduls und der NVS müssen Sie die AFF A900 oder FAS9500 Nodes als Netzboot einsetzen. Die ONTAP-Version und die Patch-Ebene, die auf dem Cluster ausgeführt werden, müssen dann installiert werden. Laufzeit `netboot` Bedeutet, dass Sie von einem auf einem Remote-Server gespeicherten ONTAP Image booten. Bei der Vorbereitung auf `netboot`, Sie müssen eine Kopie des ONTAP 9-Startabbilds auf einem Webserver hinzufügen, auf den das System zugreifen kann.

Es ist nicht möglich, die auf den Boot-Medien eines AFF A900 oder FAS9500 Controller-Moduls installierte ONTAP Version zu überprüfen, es sei denn, sie ist in einem Chassis installiert und eingeschaltet. Die ONTAP

Version auf dem AFF A900 oder FAS9500 Startmedium muss mit der ONTAP Version übereinstimmen, die auf dem AFF A700 oder FAS9000 System ausgeführt wird und bei dem Upgrade sowohl die Primär- als auch die Backup-Boot-Images übereinstimmen. Sie können die Bilder konfigurieren, indem Sie eine ausführen `netboot` Gefolgt von `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Sie müssen die erforderlichen Systemdateien für Ihr System und die korrekte Version von ONTAP von der herunterladen "NetApp Support" Standort. Über diese Aufgabe müssen Sie wissen `netboot` Die neuen Controller, wenn die installierte ONTAP Version nicht mit der auf den ursprünglichen Controllern installierten Version identisch ist. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Datenzugriff "NetApp Support" Zum Herunterladen der Dateien müssen Sie einen Netzboot zum Ausführen des Netzboots des Systems ausführen.
2. Laden Sie die entsprechende ONTAP Software im Software Download Bereich der NetApp Support Site herunter und speichern Sie die `<ontap_version>_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind. Ihre Verzeichnisliste sollte enthalten `<ontap_version>_image.tgz`.
4. Konfigurieren Sie die `netboot` Verbindung durch Auswahl einer der folgenden Aktionen. Hinweis: Sie sollten den Management-Port und die IP als verwenden `netboot` Verbindung. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`

Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` Ist die IP-Adresse des Storage-Systems. `<netmask>` Ist die Netzwerkmaske des Storage-Systems. `<gateway>` Ist das Gateway für das Storage-System. `<dns_addr>` Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. Dieser Parameter ist optional. `<dns_domain>` Der Domain Name (DNS) ist der Domain-Name. Dieser Parameter ist optional. HINWEIS: Andere Parameter können für Ihre Schnittstelle erforderlich sein. Geben Sie an der Firmware-Eingabeaufforderung die Hilfe ifconfig ein, um Details zu erhalten.

5. Performance `netboot` Bei Knoten 1: `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

   Unterbrechen Sie den Startvorgang nicht.

6. Warten Sie, bis Knoten 1 auf dem AFF A900 oder FAS9500 Controller-Modul ausgeführt wird, um die Startmenü-Optionen anzuzeigen, wie unten gezeigt:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

7. Wählen Sie im Startmenü Option `(7) Install new software first`. Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

> Ignorieren Sie die folgende Meldung: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair.` Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades. Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen.

8. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz[]
9. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
   a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird: `Do you want to restore the backup configuration now? {y|n}`
   b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`

      Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.
10. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium:
    a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`: `This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:`
    b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.
11. Wählen Sie die Option `5` Wechseln Sie vom Boot-Menü zum Wartungsmodus. Antwort `yes` Zu den Aufforderungen, bis der Node im Wartungsmodus und mit der Eingabeaufforderung angehalten wird `*>`.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:
   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`
   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA-Ethernet	`ucadmin modify -mode cna` *`adapter-name`*

FC-Ziel	`fcadmin config -t target` *`adapter-name`*
FC-Initiator	`fcadmin config -t initiator` *`adapter-name`*

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   der HA-Status für alle Komponenten sollte mcc sein.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mcc
   ```

   ```
   ha-config modify chassis mcc
   ```

3. Stoppen Sie den Knoten: `halt`Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:
4. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `Show date`
5. Stellen Sie bei Bedarf das Datum in UTC oder Greenwich Mean Time (GMT) ein: `set date <mm/dd/yyyy>`
6. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`
7. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`
8. Einstellungen speichern: `saveenv`
9. Umgebungsvariablen erfassen: `printenv`
10. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden: `boot_ontap maint`
11. Überprüfen Sie, ob die Änderungen wirksam sind, und ucadmin zeigt FC Initiator-Ports online an.

Wenn Sie diesen Typ von HBA… haben	Verwenden Sie diesen Befehl…
CNA	`ucadmin show`
FC	`fcadmin show`

12. Überprüfen Sie den HA-config-Modus: `ha-config show`

a. Stellen Sie sicher, dass Sie die folgende Ausgabe haben:

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   der HA-Status für alle Komponenten sollte mcc sein.

Wenn die MetroCluster-Konfiguration…	Der HA-Status sollte…
Zwei Nodes	mcc-2n
Vier oder acht Nodes	mcc

2. Wenn der angezeigte Systemzustand des Controllers nicht richtig ist, setzen Sie den HA-Status für das Controller-Modul und das Chassis:

Wenn die MetroCluster-Konfiguration…	Geben Sie diese Befehle ein…
Zwei Knoten	`ha-config modify controller mcc-2n` `ha-config modify chassis mcc-2n`
Vier oder acht Knoten	`ha-config modify controller mcc` `ha-config modify chassis mcc`

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln von Informationen vor dem Upgrade".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Halten Sie das System an und starten Sie von der in den Wartungsmodus `LOADER` Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Laufwerke von Node_B_1-A700 an:

   ```
   disk show -a
   ```

   Die Beispielausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

   ```
   *> disk show -a
   Local System ID: 1574774970

     DISK         OWNER                     POOL   SERIAL NUMBER    HOME
   DR HOME
   ------------   -------------             -----  -------------
   -------------             -------------
   ...
   rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
   node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
   ...
   ```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   ```
   disk reassign -s old-sysid -d new-sysid
   ```

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden: `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. Zeigt den Aggregatstatus an: `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-A900).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten: `halt`
2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Anzeigen des Startmenüs: `boot_ontap menu`
4. Wenn die Stammverschlüsselung verwendet wird, geben Sie den Startmenü-Befehl für Ihre Verschlüsselungsmanagementkonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

5. Wenn Autoboot aktiviert ist, unterbrechen Sie den Autostart, indem Sie Control-C drücken
6. Führen Sie im Startmenü die Option (6) aus.

Mit Option 6 wird der Node vor Abschluss zweimal neu gestartet.

Antworten `y` Zu den Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist: `printenv partner-sysid`

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest: `setenv partner-sysid` *`partner-sysID`*

8. Wenn die Stammverschlüsselung verwendet wird, geben Sie den Startmenü-Befehl für Ihre Verschlüsselungsmanagementkonfiguration erneut aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

   Möglicherweise müssen Sie die ausgeben `recover_xxxxxxxx_keymanager` Befehl wird mehrmals am Boot-Menü angezeigt, bis die Nodes vollständig gebootet werden.

9. Starten der Knoten: `boot_ontap`
10. Warten Sie, bis die ersetzten Nodes gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

       `network port broadcast-domain show`

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

       "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast Domain hostet.

d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

   Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

   "Erstellen einer Cluster-Peer-Beziehung"

f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

   VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

   "Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

LIF-Konfiguration überprüfen

Stellen Sie vor dem Wechsel sicher, dass LIFs auf den entsprechenden Nodes/Ports gehostet werden. Folgende Schritte sind auszuführen

Über diese Aufgabe

Diese Aufgabe wird in Site_B ausgeführt, wo die Nodes mit Root-Aggregaten gestartet wurden.

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

      ```
      set -privilege advanced
      ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

      ```
      vserver config override -command "network interface modify" -vserver
      vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
      new_node_name"
      ```

Wenn Sie den eingeben `network interface modify` Befehl im `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können die erstellen `network interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

a. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   `network interface revert * -vserver` *`vserver-name`*

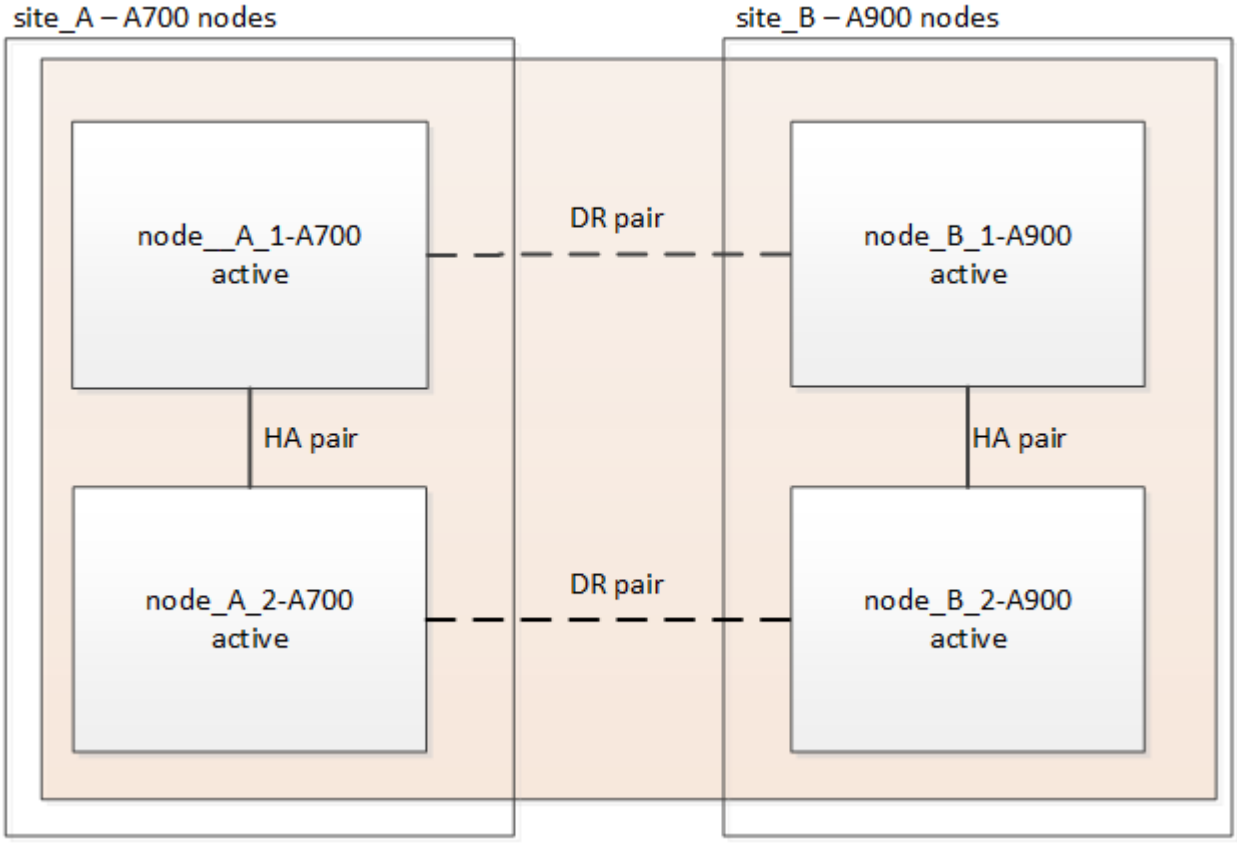
   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Schalten Sie die MetroCluster-Konfiguration zurück

Nachdem die neuen Controller konfiguriert wurden, schalten Sie die MetroCluster Konfiguration zurück und kehren den normalen Betrieb zurück.

Über diese Aufgabe

In dieser Aufgabe führen Sie den Vorgang zum Zurückkehren aus und kehren die MetroCluster-Konfiguration in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade, wie in der folgenden Abbildung dargestellt. (Diese Abbildung gilt auch für das Upgrade einer FAS9000 auf einen FAS9500 Controller.)



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.

a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.

2. Zurückwechseln des Clusters:

```
metrocluster switchback
```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

```
metrocluster show
```

Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umkehrvorgang ist abgeschlossen, wenn die Ausgabe angezeigt wird `normal`:

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

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:

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

   ```
   metrocluster show
   ```

   b. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   Nach dem Ausführen des `metrocluster check run` Und `metrocluster check show` Zeigt möglicherweise einen Fehler an, der dem folgenden Beispiel ähnelt:

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+ Dieser Fehler tritt auf, weil der Controller während des Upgrades nicht stimmt. Sie können den Fehler ohne Bedenken ignorieren und mit dem Upgrade der Nodes auf Site_A fortfahren

Aktualisieren Sie die Knoten auf site_A

Sie müssen die Upgrade-Aufgaben auf Site_A wiederholen

Schritt

1. Wiederholen Sie die Schritte, um die Knoten auf Standort_A zu aktualisieren. Beginnen Sie mit "Bereiten Sie sich auf das Upgrade vor".

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Standorten und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Site_A verwendet wird, werden Sie von Site_B. umschalten

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritt

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.

   a. Geben Sie den folgenden Befehl ein:

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

   b. Wiederholen Sie den Befehl im Partner-Cluster.

Wiederherstellung des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte unter: "Hinzufügen von MetroCluster Konfigurationen" Im Abschnitt *MetroCluster Tiebreaker Installation and Configuration*.

Controller-Upgrade in einer MetroCluster FC-Konfiguration mit vier Nodes durch Umschaltung und Switchback mit Befehlen zum Austausch eines System-Controllers (ONTAP 9.10.1 und höher)

Mithilfe dieses geführten automatisierten MetroCluster-Switchover-Vorgangs lässt sich ein unterbrechungsfreies Controller-Upgrade auf einer MetroCluster FC-Konfiguration mit vier Nodes durchführen. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Unterstützte Plattformkombinationen

- Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster FC-Upgrade-Tabelle in "Wählen Sie ein Controller-Upgrade-Verfahren".

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

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Andere Komponenten in der Konfiguration, wie z. B. Storage Shelfs oder Switches, können nicht gleichzeitig aktualisiert werden.

- Dieses Verfahren gilt für Controller-Module in einer MetroCluster FC-Konfiguration mit vier Nodes.
- Die Plattformen müssen ONTAP 9.10.1 oder höher ausführen.

  "NetApp Hardware Universe"

- Mit diesem Verfahren können Controller in einer MetroCluster FC-Konfiguration mit vier Nodes mithilfe von NSO basierter, automatisierter Umschaltung und zurückwechseln. Wenn Sie ein Controller-Upgrade mithilfe von Aggregate Relocation (ARL) durchführen möchten, lesen Sie "Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen". Es wird empfohlen, das NSO-basierte automatische Verfahren zu verwenden.
- Wenn sich die MetroCluster Standorte physisch an zwei verschiedenen Standorten befinden, sollten Sie das automatische NSO Controller-Upgrade-Verfahren einsetzen, um die Controller an beiden Standorten nacheinander zu aktualisieren.
- Durch dieses automatische NSO-basierte Controller-Upgrade-Verfahren können Sie den Controller-Ersatz an einen MetroCluster Disaster Recovery (DR)-Standort initiieren. Sie können jeweils nur einen Controller-Austausch an einem Standort initiieren.
- Um an Standort A einen Controller-Austausch zu initiieren, müssen Sie den Startbefehl für den Controller-

Austausch von Standort B ausführen Der Vorgang leitet Sie weiter, Controller beider Nodes nur an Standort A zu ersetzen. Um die Controller an Standort B zu ersetzen, müssen Sie den Startbefehl für den Controller-Ersatz von Standort A ausführen Es wird eine Meldung angezeigt, in der der Standort identifiziert wird, an dem die Controller ersetzt werden.

Folgende Beispielnamen werden in diesem Verfahren verwendet:

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

Vorbereitung auf das Upgrade

Zur Vorbereitung auf das Controller Upgrade müssen Sie die System-Vorabprüfungen durchführen und die Konfigurationsinformationen erfassen.

Während des Upgrades können Sie die ausführen `system controller replace show` Oder `system controller replace show-details` Befehl von Standort A, um den Status zu überprüfen. Wenn die Befehle eine leere Ausgabe zurückgeben, warten Sie einige Minuten, und führen Sie den Befehl erneut aus.

Schritte

1. Starten Sie das Verfahren zum automatischen Austausch der Controller von Standort A, um die Controller an Standort B zu ersetzen:

   ```
   system controller replace start
   ```

   Der automatisierte Vorgang führt die Vorabprüfungen durch. Wenn keine Probleme gefunden werden, wird der Vorgang angehalten, sodass Sie die konfigurationsbezogenen Informationen manuell erfassen können.

   > Das aktuelle Quellsystem und alle kompatiblen Zielsysteme werden angezeigt. Wenn Sie den Quell-Controller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang angehalten und ein Fehler meldet, nachdem die neuen Nodes gestartet wurden. Um den Cluster wieder in einen ordnungsgemäßen Zustand zu versetzen, müssen Sie die manuelle Recovery-Prozedur befolgen.

   Der `system controller replace start` Der Befehl meldet möglicherweise den folgenden

Vorprüffehler:

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- -------------- ------------------------------------
Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
showed errors in component aggregates
```

Überprüfen Sie, ob dieser Fehler aufgetreten ist, weil Sie nicht gespiegelte Aggregate oder ein anderes Problem an Aggregaten haben. Vergewissern Sie sich, dass sich alle gespiegelten Aggregate in einem ordnungsgemäßen Zustand befinden und dass sie nicht beeinträchtigt bzw. gespiegelt werden. Wenn dieser Fehler nur auf nicht gespiegelte Aggregate zurückzuführen ist, können Sie diesen Fehler durch Auswahl des überschreiben `-skip-metrocluster-check true` Option auf der `system controller replace start` Befehl. Wenn auf Remote-Storage zugegriffen werden kann, sind die nicht gespiegelten Aggregate nach einer Umschaltung online. Falls die Remote-Storage-Verbindung ausfällt, können die nicht gespiegelten Aggregate nicht online geschaltet werden.

2. Erfassen Sie manuell die Konfigurationsinformationen, indem Sie sich bei Standort B anmelden und den Befehlen folgen, die in der Konsolenmeldung unter der aufgeführt sind `system controller replace show` Oder `system controller replace show-details` Befehl.

Sammeln von Informationen vor dem Upgrade

Vor dem Upgrade, wenn das Root-Volume verschlüsselt ist, müssen Sie den Sicherungsschlüssel und andere Informationen sammeln, um die neuen Controller mit den alten verschlüsselten Root-Volumes zu booten.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel für die vorhandenen Controller, damit Sie bei der Einrichtung der neuen Controller problemlos die Kabel identifizieren können.
2. Zeigen Sie die Befehle an, um den Backup-Schlüssel und weitere Informationen zu erfassen:

   ```
   system controller replace show
   ```

   Führen Sie die unter aufgeführten Befehle aus `show` Befehl aus dem Partner-Cluster.

3. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

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

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260

- Node_B_1-alt: 4068741254
- Node_B_2-alt: 4068741256

```
metrocluster-siteA::> 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-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

In diesem Beispiel für eine MetroCluster FC-Konfiguration mit zwei Nodes werden die folgenden alten System-IDs abgerufen:

- Node_A_1: 4068741258
- Knoten_B_1: 4068741254

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

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `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`

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

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

6. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

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

7. 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 Verschlüsselungsmanagementinformationen".

   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
   ```

8. Setzen Sie den Vorgang fort, nachdem Sie die Konfigurationsinformationen erfasst haben:

   ```
   system controller replace resume
   ```

Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration über den Tiebreaker oder eine andere Software entfernen, bevor der alte Controller ersetzt wird.

Schritte

1. "Entfernen der vorhandenen MetroCluster-Konfiguration" Über die Tiebreaker Software.
2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Ersetzen der alten Controller und Booten der neuen Controller

Nachdem Sie Informationen gesammelt und den Vorgang fortgesetzt haben, wird die Automatisierung mit dem Switchover fortgesetzt.

Über diese Aufgabe

Der Automatisierungsvorgang initiiert die Umschaltung, `heal-aggregates`, und `heal root-aggregates` Betrieb: Nach Abschluss dieser Vorgänge wird der Vorgang bei **pausiert für Benutzereingriff** angehalten, sodass Sie die Controller racken und installieren können, die Partner-Controller hochfahren und die Root-Aggregat-Festplatten dem neuen Controller-Modul aus dem Flash-Backup mit dem neu zuweisen können `sysids` Früher gesammelt.

Bevor Sie beginnen

Vor dem Starten der Umschaltung hält der Automatisierungsvorgang pausiert, sodass Sie manuell überprüfen können, ob alle LIFs „`up`“ an Standort B. sind Ggf. Beliebige LIFs mit „`deigenen`“ bis „`up`“ bereitstellen und den Automatisierungsvorgang mit dem fortsetzen `system controller replace resume` Befehl.

Vorbereiten der Netzwerkkonfiguration der alten Controller

Um sicherzustellen, dass das Netzwerk auf den neuen Controllern ordnungsgemäß fortgesetzt wird, müssen Sie LIFs auf einen gemeinsamen Port verschieben und dann die Netzwerkkonfiguration der alten Controller entfernen.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie verwenden die in erfassten Informationen Vorbereitung auf das Upgrade.

Schritte

1. Booten Sie die alten Nodes, und melden Sie sich dann bei den Nodes an:

   ```
   boot_ontap
   ```

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      ```
      network interface show
      ```

      Alle Daten-LIFS einschließlich SAN und NAS sind admin „`up`“ und betrieblich „`down`“, da sie sich am Switchover-Standort (Cluster_A) befinden.

   b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

      „`e0d`“ ist zum Beispiel ein physischer Port an alten Controllern und ist auch auf neuen Controllern

vorhanden. „`e0d`“ wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

`network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

Im folgenden Beispiel lautet „`e0d`“.

Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Ändern Sie Broadcast-Domänen, um VLAN und physische Ports zu entfernen, die gelöscht werden müssen:

`broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

Wiederholen Sie diesen Schritt für alle VLAN- und physischen Ports.

4. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und Schnittstellengruppen, die Cluster-Ports als Mitgliedsports verwenden.

a. VLAN-Ports löschen:

`network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

`network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN- und Interface Group-Ports aus der Broadcast-Domäne:

`network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname,..`*

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Anhalten der Knoten:

   ```
   halt -inhibit-takeover true -node node-name
   ```

   Dieser Schritt muss auf beiden Knoten durchgeführt werden.

Einrichten der neuen Controller

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Wenn die neuen Controller-Module nicht eigene FC-VI-Karten enthalten und FC-VI-Karten von alten Controllern mit neuen Controllern kompatibel sind, tauschen Sie FC-VI-Karten aus und installieren Sie diese in den richtigen Steckplätzen.

   Siehe "NetApp Hardware Universe" Für Slot-Informationen für FC-VI-Karten.

5. Verkabeln Sie die Strom-, seriellen Konsolen- und Managementverbindungen der Controller, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

   Schließen Sie derzeit keine anderen Kabel an, die von den alten Controllern getrennt wurden.

   "Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Eingabeaufforderung Strg-C, um die LOADER-Eingabeaufforderung anzuzeigen.

Netbootting der neuen Controller

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.

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp

Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.

3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	Extrahieren Sie den Inhalt der ontap-Version_image.tgzfile in das Zielverzeichnis: Tar -zxvf ontap-Version_image.tgz HINWEIS: Wenn Sie den Inhalt auf Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot Image zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: ontap-Version_image.tgz Sie müssen nicht die ontap-Version_image.tgz-Datei extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

     ```
     ifconfig e0M -auto
     ```

   - Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

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

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

```
 Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
. 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`
```

```
Enter username/password if applicable, or press Enter to continue.
```

7. 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}
```

8. 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 der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   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.

Wiederherstellen der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA-Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
FC-Ziel	`fcadmin config -t target` *`adapter-name`*
FC-Initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl

CNA	`ucadmin show`
FC	`fcadmin show`

Neuzuweisen von Root-Aggregatfestplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul mithilfe des neu zu `sysids` Früher gesammelt

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln von Informationen vor dem Upgrade".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Beenden Sie das System und das Booten in den Wartungsmodus von der LOADER-Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   `disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   `aggr status`

   ```
   *> aggr status
              Aggr            State       Status           Options
   aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                              mirrored
   mirror_resync_priority=high(fixed)
                              fast zeroed
                              64-bit
   ```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Sie können VLANs und Schnittstellengruppen neu konfigurieren. Falls erforderlich, ändern Sie die Ports für die Cluster-LIFs und Broadcast-Domänen manuell, bevor Sie den Vorgang mit der fortsetzen `system controller replace resume` Befehl.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   `halt`

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Anzeigen des Startmenüs:

   `boot_ontap menu`

4. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…

Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

5. Wenn Autoboot aktiviert ist, unterbrechen Sie die Autoboot-Taste, indem Sie Strg+C drücken
6. Führen Sie im Startmenü die Option „`6`“ aus.

   Mit der Option „`6`“ wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist:

   `printenv partner-sysid`

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

   `setenv partner-sysid` *`partner-sysID`*

8. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „`6`“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

9. Starten der Knoten:

   ```
   boot_ontap
   ```

10. Warten Sie, bis die ersetzten Nodes gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

       ```
       network port broadcast-domain show
       ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

       "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast-Domäne hostet.

    d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

    e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

       Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

       "Erstellen einer Cluster-Peer-Beziehung"

    f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

       VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

       "Erstellen eines VLANs"

    "Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

    a. Überprüfen Sie, ob das Partner-Cluster erreichbar ist und ob die Konfiguration auf dem Partner-Cluster erfolgreich resynchronisiert ist:

       ```
       metrocluster switchback -simulate true
       ```

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

13. Bevor Sie den Vorgang fortsetzen, überprüfen Sie, ob die MetroCluster ordnungsgemäß konfiguriert ist. Prüfen Sie den Knoten-Status:

    ```
    metrocluster node show
    ```

    Überprüfen Sie, ob sich die neuen Knoten (site_B) in **warten auf den Status wechseln** von site_A befinden

14. Vorgang fortsetzen:

    ```
    system controller replace resume
    ```

Abschluss des Upgrades

Der Automatisierungsvorgang führt Überprüfungen des Verifikationssystems durch und hält anschließend Pausen ein, um die Erreichbarkeit des Netzwerks zu überprüfen. Nach der Überprüfung wird die Rückgewinnungsphase für die Ressourcen eingeleitet und der Automatisierungsvorgang führt den Wechsel zurück an Standort A durch und hält die Prüfungen nach dem Upgrade an. Nachdem Sie den Automatisierungsvorgang fortgesetzt haben, führt er die Prüfungen nach dem Upgrade durch und markiert, wenn keine Fehler erkannt werden, das Upgrade als abgeschlossen.

Schritte

1. Überprüfen Sie die Netzwerkzuwachbarkeit, indem Sie die Konsolenmeldung ausführen.
2. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

    ```
    system controller replace resume
    ```

3. Der Automatisierungsvorgang kehrt an Standort A zurück und führt die Nachprüfung durch. Wenn der Vorgang angehalten wird, überprüfen Sie den SAN-LIF-Status manuell und überprüfen Sie die Netzwerkkonfiguration anhand der Konsolenmeldung.
4. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

    ```
    system controller replace resume
    ```

5. Prüfen Sie den Status der Prüfungen nach der Aktualisierung:

    ```
    system controller replace show
    ```

Wenn bei den Prüfungen nach der Aktualisierung keine Fehler gemeldet wurden, ist das Upgrade abgeschlossen.

6. Melden Sie sich nach Abschluss des Controller-Upgrades bei Standort B an und überprüfen Sie, ob die ersetzten Controller ordnungsgemäß konfiguriert sind.

Wiederherstellen des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Hinzufügen von MetroCluster Konfigurationen".

Controller-Upgrade in einer MetroCluster IP-Konfiguration durch Switchover und Switchback (ONTAP 9.8 und höher)

Mit ONTAP 9.8 ermöglicht die MetroCluster Umschaltung unterbrechungsfreien Service für Clients, während Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

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.
- Plattformmodelle mit internen Shelfs werden nicht unterstützt.
- Mit diesem Verfahren können Sie nur bestimmte Plattformmodelle in einer MetroCluster IP-Konfiguration aktualisieren.
  - Informationen darüber, welche Kombinationen von Plattform-Upgrades unterstützt werden, finden Sie in der MetroCluster IP-Upgrade-Tabelle unter "Wählen Sie ein Controller-Upgrade-Verfahren".

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

Über diese Aufgabe

- 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.

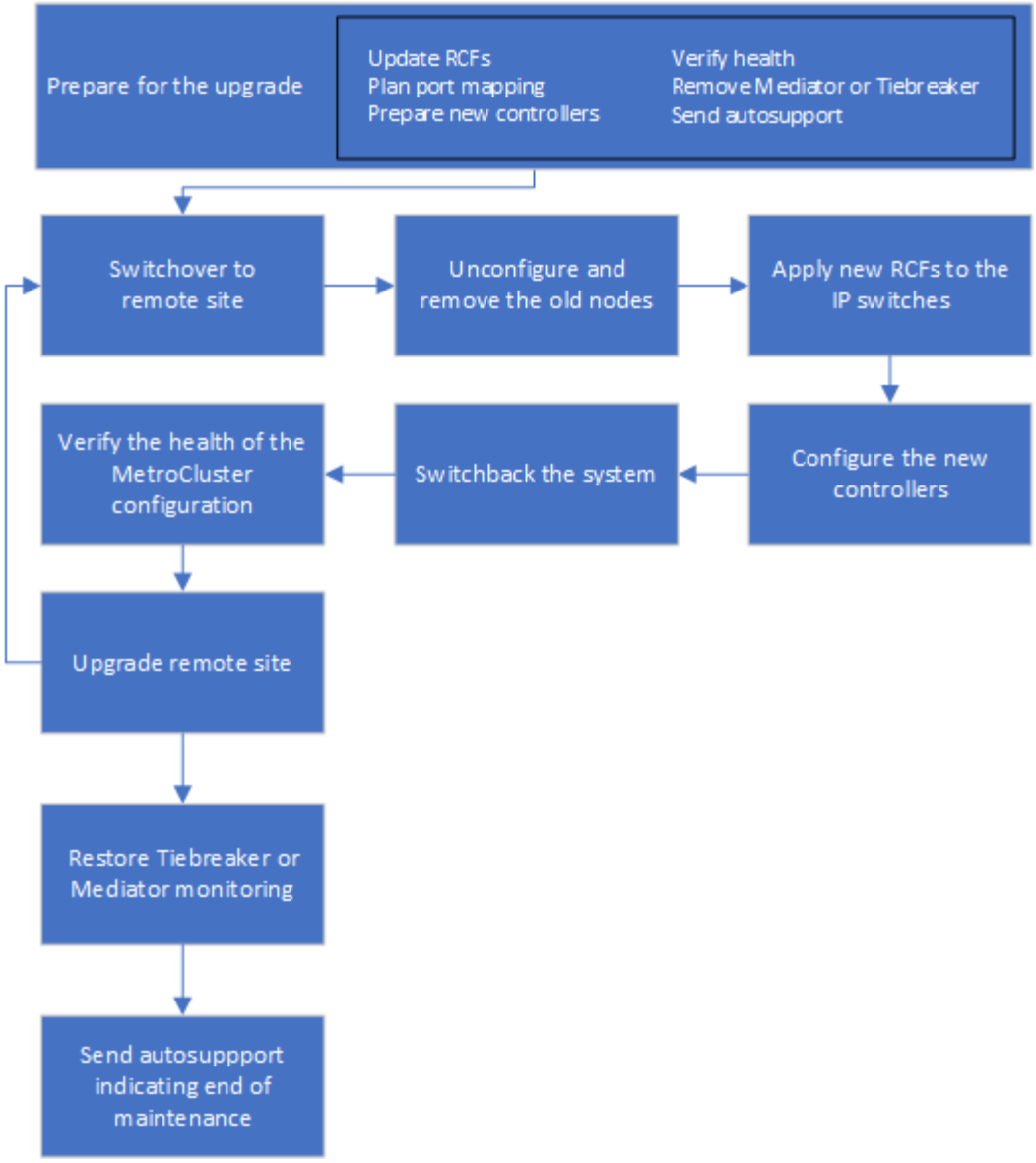
- Auf den IP-Switches muss eine unterstützte Firmware-Version ausgeführt werden.
- Wenn die neue Plattform weniger Steckplätze als das ursprüngliche System besitzt oder weniger oder unterschiedliche Ports vorhanden sind, müssen Sie dem neuen System möglicherweise einen Adapter hinzufügen.

  Weitere Informationen finden Sie im "NetApp Hardware Universe".

- Auf den neuen Plattformen werden die IP-Adressen, Netmasken und Gateways der ursprünglichen Plattformen wiederverwendet.
- Folgende Beispielnamen werden in diesem Verfahren verwendet:
  - Standort_A
    - Vor dem Upgrade:
      - Node_A_1-alt
      - Node_A_2-alt
    - Nach dem Upgrade:
      - Node_A_1-neu
      - Node_A_2-neu
  - Standort_B
    - Vor dem Upgrade:
      - Node_B_1-alt
      - Node_B_2-alt
    - Nach dem Upgrade:
      - Node_B_1-neu
      - Node_B_2-neu

Workflow für das Upgrade von Controllern in einer MetroCluster IP-Konfiguration

Mithilfe des Workflow-Diagramms können Sie Upgrade-Aufgaben planen.



Vorbereitung auf das Upgrade

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die neuen Plattformen vorbereiten und andere verschiedene Aufgaben ausführen.

Aktualisieren der RCF-Dateien des MetroCluster-Switch vor dem Aktualisieren der Controller

Abhängig von den alten Plattformmodellen, oder wenn die Switch-Konfiguration nicht auf der Mindestversion steht oder wenn Sie die von den Back-End MetroCluster-Verbindungen verwendeten VLAN-IDs ändern möchten, müssen Sie die RCF-Dateien des Switches aktualisieren, bevor Sie mit dem Verfahren zum Plattformupgrade beginnen.

Über diese Aufgabe

Sie müssen die RCF-Datei in den folgenden Szenarien aktualisieren:

- Bei bestimmten Plattformmodellen müssen die Switches eine unterstützte VLAN-ID für die Back-End MetroCluster IP-Verbindungen verwenden. Wenn sich die alten oder neuen Plattformmodelle in der folgenden Tabelle befinden, **und nicht** mit einer unterstützten VLAN-ID, müssen Sie die RCF-Dateien für

den Switch aktualisieren.

> Die lokalen Cluster-Verbindungen können jedes VLAN verwenden, sie müssen nicht im angegebenen Bereich sein.

Plattformmodell (alt oder neu)	Unterstützte VLAN-IDs
• AFF A400	• 10 • 20 • Beliebiger Wert im Bereich 101 bis 4096 inklusive.

- Die Switch-Konfiguration wurde nicht mit der minimal unterstützten RCF-Version konfiguriert:

Switch-Modell	Erforderliche RCF-Dateiversion
Cisco 3132Q-V	1.7 oder höher
Cisco 3232C	1.7 oder höher
Broadcom BES-53248	1.3 oder höher

- Sie möchten die VLAN-Konfiguration ändern.

  Der VLAN-ID-Bereich liegt zwischen 101 und 4096.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

   Folgen Sie den Schritten im Abschnitt Ihres Switch-Anbieters vom "Installation und Konfiguration von MetroCluster IP".

   - "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
   - "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"

2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Befolgen Sie die Schritte unter "Installation und Konfiguration von MetroCluster IP".

   - "Herunterladen und Installieren der Broadcom RCF-Dateien"
   - "Herunterladen und Installieren der Cisco IP RCF-Dateien"

Zuordnen von Ports von den alten Nodes zu den neuen Nodes

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

Über diese Aufgabe

Wenn der neue Node zum ersten Mal während des Upgrades gebootet wird, stellt er die aktuellste Konfiguration des alten Node wieder dar, der ersetzt wird. Wenn Sie Node_A_1-New booten, versucht ONTAP, LIFs auf denselben Ports zu hosten, die in Node_A_1-old verwendet wurden. Deshalb müssen Sie im Rahmen des Upgrades die Port- und LIF-Konfiguration anpassen, sodass diese mit der der des alten Node kompatibel ist. Während des Upgrades führen Sie sowohl für die alten als auch für die neuen Nodes Schritte durch, um eine korrekte Cluster-, Management- und Daten-LIF-Konfiguration sicherzustellen.

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 Cluster-Ports neu erstellen.
e0c, e0d	e0a, e0b, e0c, e0d	e0c und e0d sind passende Anschlüsse. Sie müssen die Konfiguration nicht ändern, aber nach einem Upgrade können Sie die Cluster-LIFs über 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 von erfassen "NetApp 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						

Netbootting der neuen Controller

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.

Wenn das Plattformmodell…	Dann…

8000 Series Systeme	Extrahieren Sie den Inhalt des `ontap-version_image.tgz` Datei zum Zielverzeichnis:
	
	`tar -zxvf ontap-version_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: `_ontap-version_image.tgz` Sie müssen den nicht extrahieren `_ontap-version_image.tgz` Datei:

d. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS 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.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Alle anderen Systeme	`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 der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   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 des MetroCluster-Systemzustands vor Standort-Upgrades

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`

      Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

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

      Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   c. Überprüfen Sie auf Statusmeldungen:

      `system health alert show`

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

      `system license show`

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

   e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

      `network device-discovery show`

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

      `cluster date show`

   Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

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 von Informationen vor dem Upgrade

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. Erfassung von Interconnect-, Port- und LIF-Informationen für jeden Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `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`
- `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 Upgrade-Prozess in die richtigen 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::*
```

   Es wird empfohlen, die UUIDs in eine Tabelle wie die folgende aufzunehmen.

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.

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `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 das Schlüsselmanagement 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 Verschlüsselungsmanagementinformationen".

   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.
```

Mediator- oder Tiebreaker-Überwachung wird entfernt

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" Im Installations- und Konfigurationshandbuch *MetroCluster Tiebreaker*
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

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. 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.

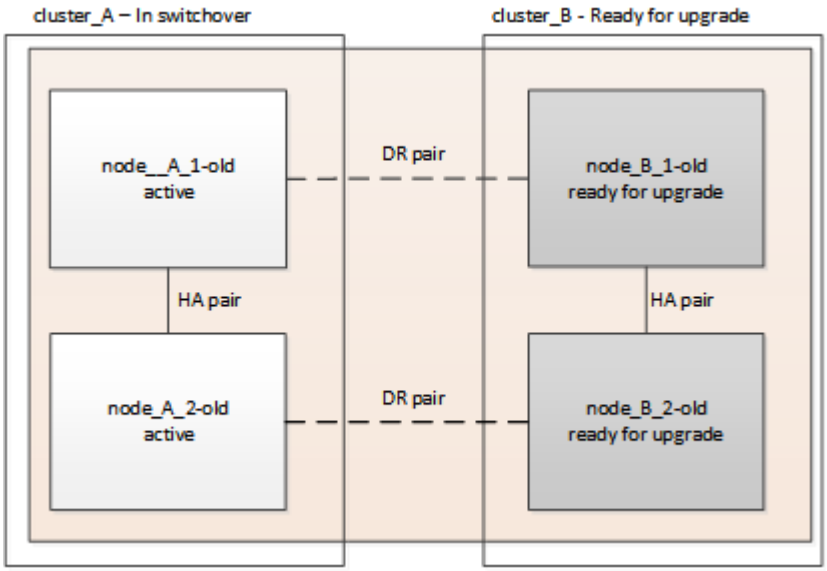
Umschalten der MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Cluster_A aktiv und stellt Daten für beide Standorte bereit. Cluster_B ist inaktiv und kann den Upgrade-Prozess starten.



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl für Cluster_A ein:

      ```
      metrocluster switchover -controller-replacement true
      ```

      Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

      ```
      metrocluster operation show
      ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

      ```
      metrocluster show
      ```

   d. Den Status der MetroCluster-Knoten überprüfen:

      ```
      metrocluster node show
      ```

   Das automatische Heilen von Aggregaten nach der ausgehandelten Umschaltung wird während eines Controller-Upgrades deaktiviert.

Entfernen von Schnittstellenkonfigurationen und Deinstallation der alten Controller

Sie müssen Daten-LIFs zu einem gemeinsamen Port verschieben, VLANs und Schnittstellengruppen auf den alten Controllern entfernen und dann die Controller physisch deinstallieren.

Über diese Aufgabe

- Diese Schritte werden auf den alten Controllern ausgeführt (Node_B_1-old, Node_B_2-old).
- Siehe die Informationen, die Sie in gesammelt haben "Zuordnen von Ports von den alten Nodes zu den neuen Nodes".

Schritte

1. Booten der alten Nodes und melden Sie sich bei den Nodes an:

   ```
   boot_ontap
   ```

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      ```
      network interface show
      ```

      Alle Daten-LIFS einschließlich SAN und NAS befinden sich in Betrieb, da sie sich am Switchover-Standort (Cluster_A) befinden.

   b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

      e0d ist zum Beispiel ein physischer Port auf den alten Controllern und ist auch auf neuen Controllern

vorhanden. e0d wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Startport zu verwenden:
`network interface modify -vserver svm-name -lif data-lif -home-port port-id`

Im folgenden Beispiel ist dies "e0d".

Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und ifgrps, die Cluster-Ports als Mitgliedsports verwenden.

a. VLAN-Ports löschen:
`network port vlan delete -node node-name -vlan-name portid-vlandid`

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN und Interface Group Ports aus Broadcast-Domäne:

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

4. Beenden Sie die Knoten der LOADER-Eingabeaufforderung:

`halt -inhibit-takeover true`

5. Stellen Sie eine Verbindung mit der seriellen Konsole der alten Controller (Node_B_1-old und Node_B_2-old) an Site_B her, und überprüfen Sie, dass die LOADER-Eingabeaufforderung angezeigt wird.

6. Ermitteln Sie die Bootarg-Werte:

   ```
   printenv
   ```

7. Trennen Sie die Speicher- und Netzwerkverbindungen auf Node_B_1-old und Node_B_2-old, und kennzeichnen Sie die Kabel, damit sie wieder mit den neuen Nodes verbunden werden können.
8. Trennen Sie die Stromkabel von Node_B_1-old und Node_B_2-old.
9. Entfernen Sie die Controller Node_B_1-old und Node_B_2-old aus dem Rack.

Aktualisierung der Switch-RCFs für die neuen Plattformen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

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

   "Installation und Konfiguration von MetroCluster IP"

   - "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
   - "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"

2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Folgen Sie den Schritten im Abschnitt Ihres Switch-Anbieters vom "Installation und Konfiguration von MetroCluster IP".

   - "Herunterladen und Installieren der Broadcom RCF-Dateien"
   - "Herunterladen und Installieren der Cisco IP RCF-Dateien"

Konfigurieren der neuen Controller

Sie müssen die Controller im Rack unterbringen und installieren, die erforderliche Einrichtung im Wartungsmodus durchführen und dann die Controller booten und die LIF-Konfiguration auf den Controllern überprüfen.

Einrichten der neuen Controller

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Verbinden Sie die Controller mit den IP-Switches, wie in beschrieben "Installation und Konfiguration von MetroCluster IP".
   - "Verkabeln der IP-Switches"
5. Starten Sie die neuen Nodes und starten Sie sie in den Wartungsmodus.

Wiederherstellen der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports:

   ```
   ucadmin show
   ```

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA-Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
FC-Ziel	`fcadmin config -t target` *`adapter-name`*
FC-Initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Einstellen des HA-Status auf den neuen Controllern und dem Chassis

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte „`mccip`“ sein.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mccip
   ```

   ```
   ha-config modify chassis mccip
   ```

Festlegen der MetroCluster-IP-Bootarg-Variablen

Für die neuen Controller-Module müssen bestimmte MetroCluster IP-Bootarg-Werte konfiguriert werden. Die Werte müssen mit den auf den alten Controller-Modulen konfigurierten übereinstimmen.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie die UUIDs und System-IDs, die bereits im Upgrade-Verfahren in identifiziert wurden "Sammeln von Informationen vor dem Upgrade".

Schritte

1. Wenn die Nodes des Upgrades die Modelle AFF A400, FAS8300 oder FAS8700 umfassen, legen Sie die folgenden Boot-Bereiche an DER LOADER-Eingabeaufforderung fest:

   ```
   setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
   partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
   ```

   ```
   setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
   partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
   ```

   > Wenn die Schnittstellen Standard-VLANs verwenden, ist keine vlan-id erforderlich.

   Mit den folgenden Befehlen werden die Werte für Node_B_1-New unter Verwendung von VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

Die folgenden Befehle legen die Werte für Node_B_2-New unter Verwendung von VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk fest:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

Das folgende Beispiel zeigt die Befehle für Node_B_1-New bei Verwendung des Standard-VLAN:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

Das folgende Beispiel zeigt die Befehle für Node_B_2-New bei Verwendung des Standard-VLAN:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. Wenn die Knoten, die aktualisiert werden, keine Systeme im vorherigen Schritt sind, legen Sie bei der LOADER-Eingabeaufforderung für jeden der verbleibenden Nodes die folgenden Bootargs mit local_IP/maska fest:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   Mit den folgenden Befehlen werden die Werte für Node_B_1-New festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

Mit den folgenden Befehlen werden die Werte für Node_B_2-New festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

3. Legen Sie an DER LOADER-Eingabeaufforderung der neuen Nodes die UUUIDs fest:

   `setenv bootarg.mgwd.partner_cluster_uuid` *partner-cluster-UUID*

   `setenv bootarg.mgwd.cluster_uuid` *local-cluster-UUID*

   `setenv bootarg.mcc.pri_partner_uuid` *DR-partner-node-UUID*

   `setenv bootarg.mcc.aux_partner_uuid` *DR-aux-partner-node-UUID*

   `setenv bootarg.mcc_iscsi.node_uuid` *local-node-UUID*

   a. Legen Sie die UUIDs auf Node_B_1-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1-New angezeigt:

      ```
      setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
      setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
      00a098ca379f
      setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
      00a098908039
      ```

   b. Legen Sie die UUIDs auf Node_B_2-New fest:

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2-New angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

4. Wenn die Originalsysteme für ADP konfiguriert wurden, aktivieren Sie an der LOADER-Eingabeaufforderung der Ersatz-Nodes ADP:

```
setenv bootarg.mcc.adp_enabled true
```

5. Legen Sie die folgenden Variablen fest:

```
setenv bootarg.mcc.local_config_id original-sys-id

setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls, Node_B_1-old, gesetzt werden.

a. Legen Sie die Variablen auf Node_B_1-New fest.

   Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1-New angezeigt:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Legen Sie die Variablen auf Node_B_2-New fest.

   Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2-New angezeigt:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Neuzuweisen von Root-Aggregatfestplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu.

Über diese Aufgabe

Diese Schritte werden im Wartungsmodus ausgeführt.

> Root-Aggregat-Festplatten sind die einzigen Festplatten, die während des Controller-Upgrades neu zugewiesen werden müssen. Die Eigentumsrechte an Datenaggregaten werden im Rahmen des Switchover/Switchback-Vorgangs übernommen.

Schritte

1. Starten des Systems in den Wartungsmodus:

   ```
   boot_ontap maint
   ```

2. Zeigen Sie die Festplatten auf Node_B_1-New in der Eingabeaufforderung Wartungsmodus an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (537403322). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

   ```
   *> disk show -a
   Local System ID: 1574774970
   DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
   DR HOME
   ------------          ---------             -----  -------------
   -------------         -------------
   prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
   node_B_1-old(537403322)  node_B_1-old(537403322)
   prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
   node_B_1-old(537403322)  node_B_1-old(537403322)
   .
   .
   .
   ```

3. Weisen Sie die Root-Aggregat-Disks in den Laufwerk-Shelfs den neuen Controllern wieder zu.

Wenn Sie ADP verwenden…	Verwenden Sie dann diesen Befehl…
Ja.	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
Nein	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Weisen Sie die Root-Aggregat-Festplatten in den Laufwerk-Shelfs den neuen Controllern neu zu:

```
disk reassign -s old-sysid -d new-sysid
```

Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken in einer nicht-ADP-Konfiguration:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob die Festplatten des Root-Aggregats ordnungsgemäß neu zugewiesen sind.

```
disk show
```

```
storage aggr status
```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                     DR HOME
------------             -------------            -----  -------------
-------------            -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Booten der neuen Controller

Sie müssen die neuen Controller booten, um sicherzustellen, dass die Bootarg-Variablen korrekt sind und, falls erforderlich, die Verschlüsselungswiederherstellungsschritte durchführen.

Schritte

1. Anhalten der neuen Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Überprüfen Sie, ob die Partner-sysid aktuell ist:

   ```
   printenv partner-sysid
   ```

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

   ```
   setenv partner-sysid partner-sysID
   ```

4. ONTAP-Startmenü anzeigen:

   ```
   boot_ontap menu
   ```

5. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option `10` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option `11` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

6. Wählen Sie im Startmenü „`(6) Flash-Update aus Backup config`“ aus.

   Mit Option 6 wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Überprüfen Sie am LOADER die Bootarg-Werte und aktualisieren Sie die Werte nach Bedarf.

   Verwenden Sie die Schritte in "Festlegen der MetroCluster-IP-Bootarg-Variablen".

8. Überprüfen Sie doppelt, ob die Partner-Sysid die richtige ist:

```
printenv partner-sysid
```

Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

9. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option `10` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ und anschließend die Option auswählen `6` Bei der ersten Eingabeaufforderung für das Startmenü. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

10. Warten Sie, bis die ersetzten Nodes gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

a. Broadcast-Domänen anzeigen:

```
network port broadcast-domain show
```

b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

"Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

c. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

"Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs zu Beginn des Upgrade-Vorgangs auf entsprechenden Nodes und Ports gehostet werden, die zugeordnet sind.

Über diesen Tsak

- Diese Aufgabe wird auf Site_B. ausgeführt
- Sehen Sie sich den Port-Mapping-Plan an, den Sie in erstellt haben "Zuordnen von Ports von den alten Nodes zu den neuen Nodes".

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Wenn Sie den Befehl zur Änderung der Netzwerkschnittstelle in eingeben `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können das Netzwerk erstellen `interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

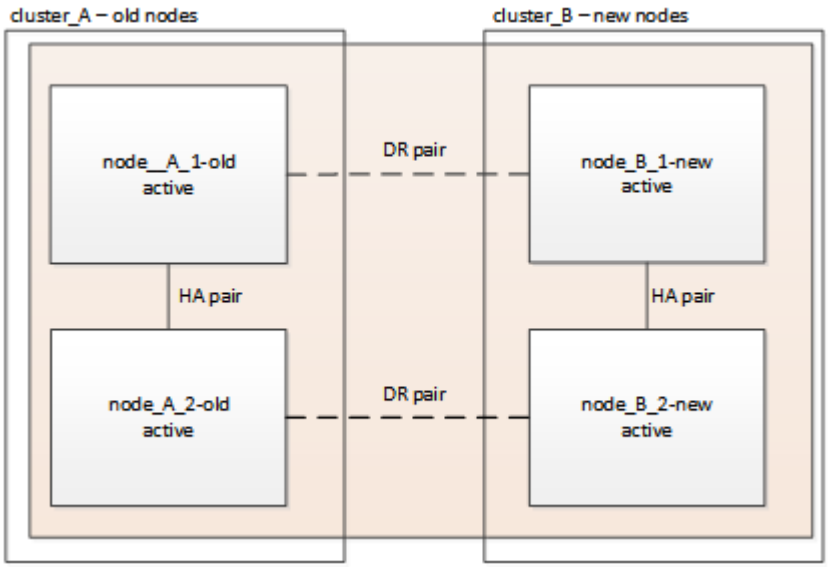
2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   ```
   network interface revert * -vserver vserver-name
   ```

Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Umschalten der MetroCluster-Konfiguration

In dieser Aufgabe führen Sie den Vorgang zum zurückwechseln durch, und die MetroCluster-Konfiguration kehrt in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Führen Sie die Reparatur und den Wechsel durch, indem Sie die erforderlichen Befehle von einem beliebigen Node im aktiven Cluster ausführen (das Cluster, das kein Upgrade durchlaufen hat).
   a. Heilen Sie die Datenaggregate:
      `metrocluster heal aggregates`
   b. Heilen Sie die Root-Aggregate:

      ```
      metrocluster heal root
      ```

   c. Zurückwechseln des Clusters:

      ```
      metrocluster switchback
      ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang normal angezeigt wird:

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

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
      `metrocluster show`
   b. Führen Sie eine MetroCluster-Prüfung durch:
      `metrocluster check run`
   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

      `metrocluster check show`
2. Überprüfen Sie die MetroCluster-Konnektivität und den Status.

a. Prüfen Sie die MetroCluster-IP-Verbindungen:

```
storage iscsi-initiator show
```

b. Prüfen Sie, ob die Knoten arbeiten:

```
metrocluster node show
```

c. Überprüfen Sie, ob die MetroCluster IP Schnittstellen aktiv sind:

```
metrocluster configuration-settings interface show
```

d. Überprüfen Sie, ob lokaler Failover aktiviert ist:

```
storage failover show
```

Aktualisieren der Knoten auf Cluster_A

Sie müssen die Upgrade-Aufgaben auf „Cluster_A“ wiederholen

Schritte

1. Wiederholen Sie die Schritte, um die Nodes auf Cluster_A zu aktualisieren. Beginnen Sie mit "Vorbereitung auf das Upgrade".

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Clustern und Nodes umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

Wiederherstellen der Tiebreaker- oder Mediator-Überwachung

Nach Abschluss des Upgrades der MetroCluster-Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

Schritte

1. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen".
Mediator	Link:../install-ip/concept_mediator_requirements.html [Konfigurieren des ONTAP Mediator-Dienstes aus einer MetroCluster IP-Konfiguration].
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden einer benutzerdefinierten AutoSupport Meldung nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung

senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritte

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:
      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher)

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Über diese Aufgabe

- Für ein Upgrade der Controller-Module der AFF A700 auf AFF A900 müssen die Controller ONTAP 9.10.1 oder höher ausgeführt werden.
- Zum Upgrade der FAS9000 Controller-Module auf FAS9500 müssen die Controller ONTAP 9.10.1P3 oder höher ausführen.
- Upgrades für alle Controller der Konfiguration sollten während des gleichen Wartungszeitraums durchgeführt werden.

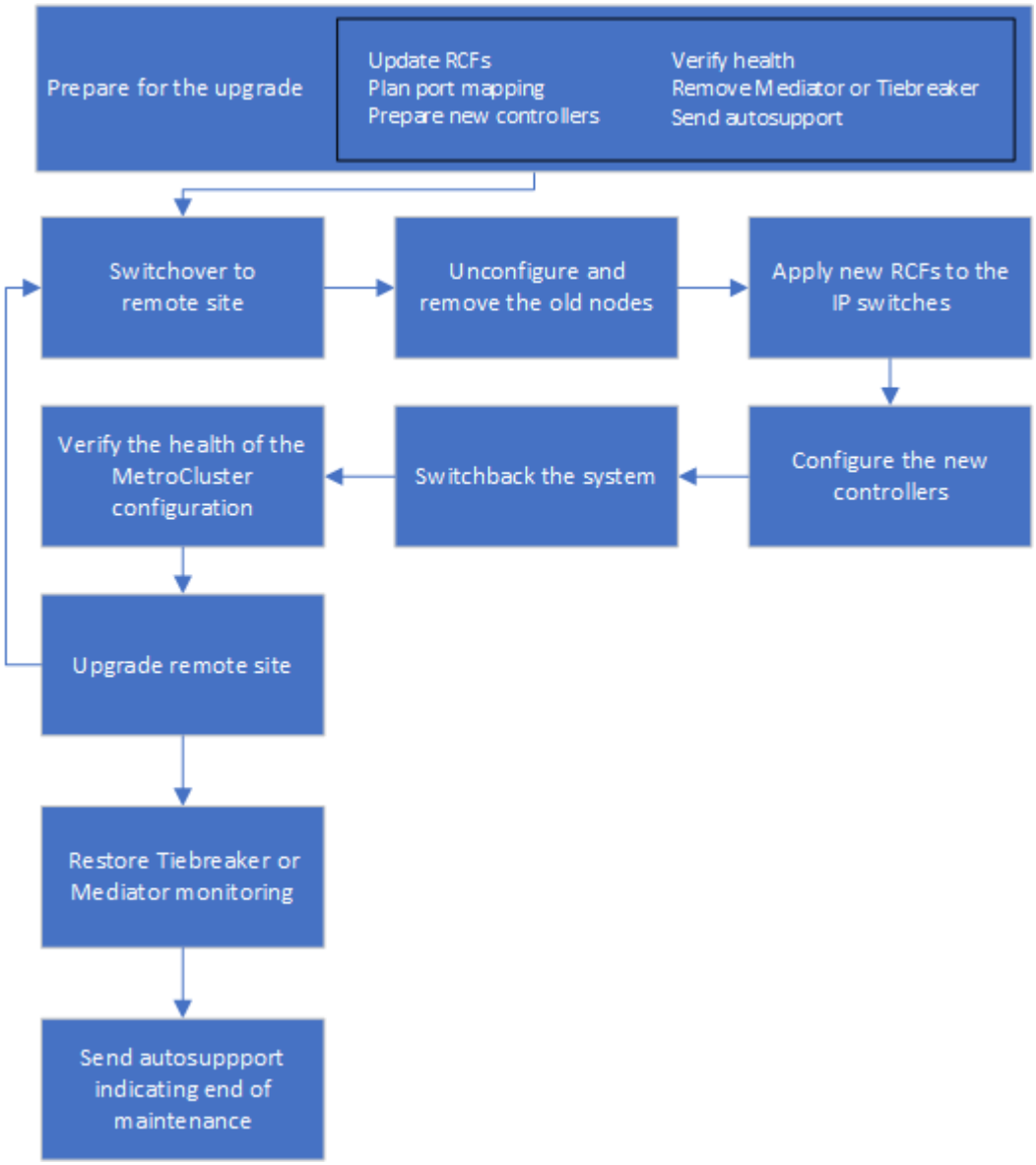
  Der Betrieb der MetroCluster Konfiguration mit einer AFF A700 und einem AFF A900 oder einem FAS9000 und FAS9500 Controller wird außerhalb dieser Wartungsaktivitäten nicht unterstützt.

- Auf den IP-Switches muss eine unterstützte Firmware-Version ausgeführt werden.
- Auf den neuen Plattformen werden die IP-Adressen, Netmasken und Gateways der ursprünglichen Plattformen wiederverwendet.
- Die folgenden Beispielnamen werden in diesem Verfahren sowohl in Beispielen als auch in Grafiken verwendet:
  - Standort_A
    - Vor dem Upgrade:
      - Node_A_1-A700
      - Node_A_2-A700
    - Nach dem Upgrade:
      - Node_A_1-A900
      - Node_A_2-A900
  - Standort_B
    - Vor dem Upgrade:
      - Node_B_1-A700

    - Node_B_2-A700
  - Nach dem Upgrade:
    - Node_B_1-A900
    - Node_B_2-A900

Workflow für das Upgrade von Controllern in einer MetroCluster IP-Konfiguration

Mithilfe des Workflow-Diagramms können Sie Upgrade-Aufgaben planen.



Bereiten Sie sich auf das Upgrade vor

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die neuen Plattformen vorbereiten und andere verschiedene Aufgaben ausführen.

Steckplatz 7 beim AFF A700 oder FAS9000 Controller löschen

Die MetroCluster-Konfiguration auf einem AFF A900 oder FAS9500 verwendet einen der Ports auf den DR-Karten in den Steckplätzen 5 und 7. Wenn beim AFF A700 oder der FAS9000 Karten in Steckplatz 7 vorhanden sind, müssen Sie die Karten in andere Steckplätze für alle Nodes des Clusters verschieben.

Aktualisieren Sie die RCF-Dateien des MetroCluster-Switch, bevor Sie die Controller aktualisieren

Sie müssen die RCF-Dateien auf MetroCluster-Switches aktualisieren, wenn Sie dieses Upgrade durchführen. In der folgenden Tabelle sind die für AFF A900/FAS9500 MetroCluster IP-Konfigurationen unterstützten VLAN-Bereiche aufgeführt.

Modell der Plattform	Unterstützte VLAN-IDs
• AFF A900 ODER FAS9500	• 10 • 20 • Beliebiger Wert im Bereich 101 bis 4096 inklusive.

- Wenn der Switch nicht mit der minimal unterstützten RCF-Dateiversion konfiguriert ist, müssen Sie die RCF-Datei aktualisieren. Informationen zur korrekten RCF-Dateiversion für Ihr Switch-Modell finden Sie im "RcfFileGenerator-Tool". Die folgenden Schritte sind für die RCF-Datei-Anwendung.

Schritte

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

   Folgen Sie den Schritten im Abschnitt Ihres Switch-Anbieters vom "Installation und Konfiguration von MetroCluster IP" Inhalt:

   - "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
   - "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"

2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Befolgen Sie die Schritte unter "Installation und Konfiguration von MetroCluster IP" Inhalt:

   - "Herunterladen und Installieren der Broadcom RCF-Dateien"
   - "Herunterladen und Installieren der Cisco IP RCF-Dateien"

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

Beim Upgrade von einer AFF A700 auf ein AFF A900 oder FAS9000 auf FAS9500 werden die Datennetzwerkports, FCP SAN-Adapterports sowie SAS- und NVMe-Storage-Ports nicht geändert. Die Daten-LIFs bleiben dort, wo sie sich während und nach dem Upgrade befinden. Daher sind Sie nicht erforderlich, die Netzwerk-Ports von den alten Nodes den neuen Nodes zuzuordnen.

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`

Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

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

Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

c. Überprüfen Sie auf Statusmeldungen:

```
system health alert show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

d. Überprüfen Sie die Lizenzen auf den Clustern:

```
system license show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

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

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehl zum Konfigurieren der Zeit- und Zeitzone.

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 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`
   - `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 Upgrade-Prozess in die richtigen 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-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

Es wird empfohlen, die UUIDs in eine Tabelle wie die folgende aufzunehmen.

Cluster oder Node	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1-A700	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2-A700	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1-A700	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2-A700	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `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 das Schlüsselmanagement 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 Verschlüsselungsmanagementinformationen".
   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-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322          537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323          537403324
1           cluster_B node_B_2-A700   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" Beim *MetroCluster Tiebreaker Installations- und Konfigurationsinhalt*
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 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.

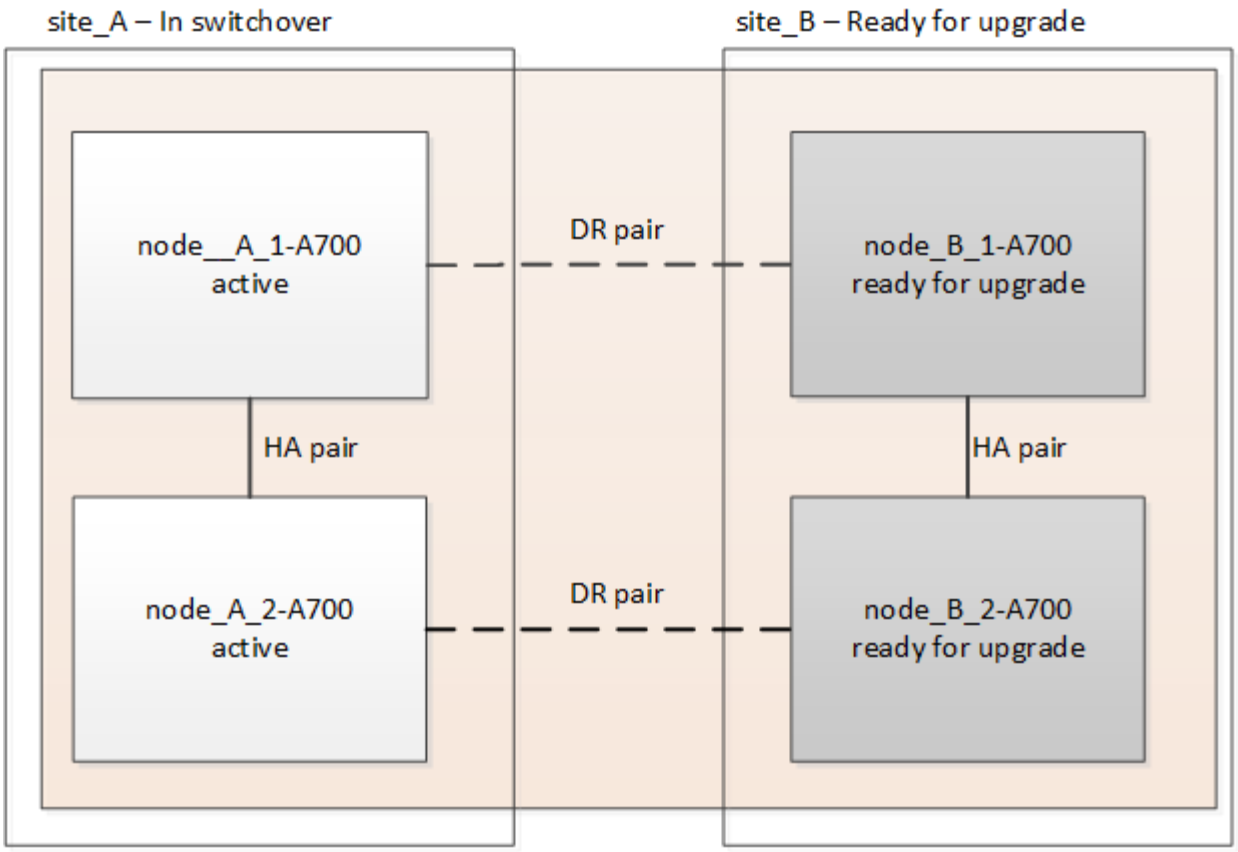
Wechseln Sie über die MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Site_A aktiv und stellt Daten für beide Standorte bereit. Site_B ist inaktiv und bereit, den Upgrade-Prozess zu starten.



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl auf Site_A aus:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   d. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

   Das automatische Heilen von Aggregaten nach der ausgehandelten Umschaltung wird während eines Controller-Upgrades deaktiviert. Nodes an Site_B werden angehalten und am angehalten `LOADER` Eingabeaufforderung:

Entfernen Sie das Controller-Modul der AFF A700 oder FAS9000 Plattform und NVS

Über diese Aufgabe

Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Schritte

1. Ermitteln Sie die Bootarg-Werte von beiden Knoten an Site_B: `printenv`
2. Schalten Sie das Chassis an Site_B. aus

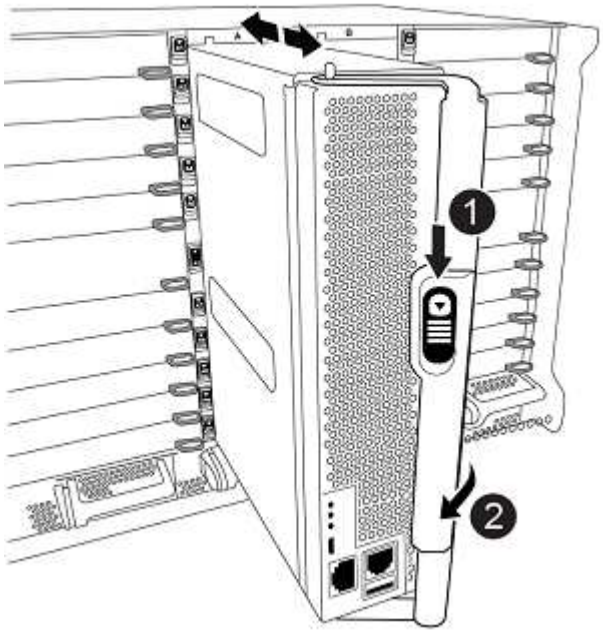
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

Gehen Sie wie folgt vor, um das AFF A700 oder das FAS9000 Controller-Modul zu entfernen

Schritte

1. Trennen Sie gegebenenfalls das Konsolenkabel und das Managementkabel vom Controller-Modul, bevor Sie das Controller-Modul entfernen.
2. Entriegeln und entfernen Sie das Controller-Modul aus dem Gehäuse.

   a. Schieben Sie die orangefarbene Taste am Nockengriff nach unten, bis sie entsperrt ist.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

   a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse. Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul wie folgt:

Hinweis: Das NVS-Modul befindet sich in Steckplatz 6 und ist doppelt so hoch wie andere Module im System.

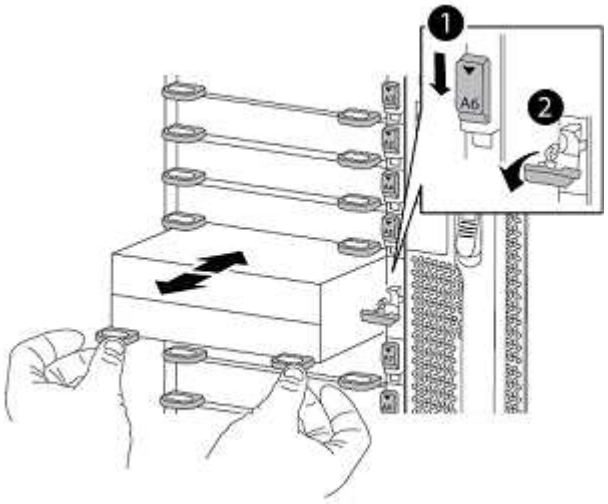
Schritte

1. Entriegeln und entfernen Sie den NVS aus Steckplatz 6.

   a. Drücken Sie die Taste mit den Buchstaben und der nummerierten Nocken. Die Nockentaste bewegt sich vom Gehäuse weg.

   b. Drehen Sie die Nockenverriegelung nach unten, bis sie sich in horizontaler Position befindet. Der NVS löst sich aus dem Gehäuse und bewegt sich ein paar Zentimeter.

   c. Entfernen Sie den NVS aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

2. Wenn Sie zusätzliche Module verwenden, die als Coredump-Geräte bei der AFF A700 oder FAS9000 NVS verwendet werden, übertragen Sie diese nicht auf den AFF A900 oder FAS9500 NVS. Übertragen Sie keine Teile vom AFF A700 oder FAS9000 Controller-Modul und NVS auf das AFF A900 oder FAS9500 Modul.

Installieren Sie die AFF A900- oder FAS9500 NVS- und Controller-Module

Sie müssen das AFF A900 oder FAS9500 NVS und das Controller-Modul installieren, das Sie im Upgrade-Kit auf beiden Knoten bei Site_B. erhalten haben Verschieben Sie das coredump-Gerät nicht vom AFF A700 oder FAS9000 NVS-Modul in das AFF A900 oder FAS9500 NVS Modul.

Über diese Aufgabe

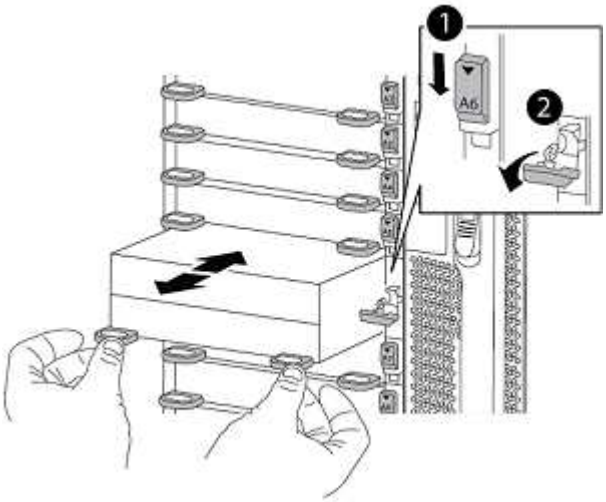
Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Installieren Sie den AFF A900 oder FAS9500 NVS

Gehen Sie wie folgt vor, um den AFF A900 oder FAS9500 NVS in Steckplatz 6 beider Knoten in Site_B. zu installieren

Schritte

1. Richten Sie den NVS an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie den NVS vorsichtig in den Schlitz, bis der vorletzte und nummerierte E/A-Nockenriegel mit dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVS.



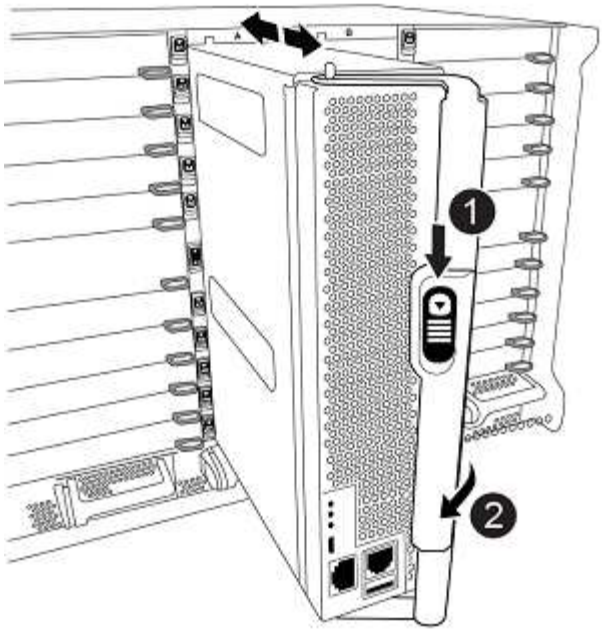
	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

Installieren Sie das AFF A900 oder FAS9500 Controller-Modul.

Gehen Sie wie folgt vor, um das AFF A900 oder FAS9500 Controller-Modul zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
2. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Achtung: Um Schäden an den Anschlüssen zu vermeiden, verwenden Sie keine übermäßige Kraft, wenn Sie das Controller-Modul in das Gehäuse schieben.
3. Verkabeln Sie die Management- und Konsolen-Ports mit dem Controller-Modul.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

4. Installieren Sie die zweite X91146A-Karte in Steckplatz 7 jedes Knotens.
   a. Stellen Sie die e5b-Verbindung auf e7b.
   b. schieben Sie die e5a-Verbindung auf e5b.

> Steckplatz 7 auf allen Knoten des Clusters sollte leer sein, wie in erwähnt Weisen Sie den neuen Nodes Ports von den alten Nodes zu Abschnitt.

5. Schalten Sie das Chassis EIN und verbinden Sie die serielle Konsole.
6. Wenn der Knoten nach der BIOS-Initialisierung Autoboot startet, unterbrechen Sie DEN AUTOBOOT, indem Sie Control-C drücken
7. Nach dem Autoboot wird die Eingabeaufforderung DES LOADERS unterbrochen. Wenn Sie das Autoboot nicht während des Bootens unterbrechen und node1 mit dem Booten startet, warten Sie, bis die Eingabeaufforderung Strg-C drücken, um zum Boot-Menü zu wechseln. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option 8, um den Node neu zu booten und das Autoboot während des Neustarts zu unterbrechen.
8. Legen Sie an der LOADER-Eingabeaufforderung die Standardvariablen für die Umgebung fest: Set-default
9. Speichern Sie die Standardeinstellungen für Umgebungsvariablen: `saveenv`

Netzboot-Nodes an Site_B

Nach Austausch des AFF A900 oder FAS9500 Controller-Moduls und der NVS müssen Sie die AFF A900 oder FAS9500 Nodes als Netzboot einsetzen. Die ONTAP-Version und die Patch-Ebene, die auf dem Cluster ausgeführt werden, müssen dann installiert werden. 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 einen Webserver hinzufügen, auf den das System zugreifen kann.

Es ist nicht möglich, die auf den Boot-Medien eines AFF A900 oder FAS9500 Controller-Moduls installierte ONTAP Version zu prüfen, es sei denn, sie ist in einem Chassis installiert und eingeschaltet. Die ONTAP Version auf dem AFF A900 oder FAS9500 Boot-Medium muss mit der ONTAP Version übereinstimmen, die auf dem AFF A700 oder FAS9000 System ausgeführt wird und bei dem Upgrade der Primär- und der Backup Boot Images übereinstimmen. Sie können die Images konfigurieren, indem Sie einen Netzboot gefolgt vom ausführen `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Sie müssen die erforderlichen Systemdateien für Ihr System sowie die korrekte Version von ONTAP von der NetApp Support-Website herunterladen.

Über diese Aufgabe

Wenn die installierte ONTAP Version nicht mit der auf den ursprünglichen Controllern installierten Version identisch ist, müssen Sie die neuen Controller als Netzboot ausführen. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software im Software Download Bereich der NetApp Support Site herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.
4. Ihre Verzeichnisliste sollte <ontap_version>_image.tgz enthalten.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie sollten den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn das Dynamic Host Configuration Protocol (DCHP)…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`

Nicht Ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` Ist die IP-Adresse des Storage-Systems. `<netmask>` Ist die Netzwerkmaske des Storage-Systems. `<gateway>` Ist das Gateway für das Storage-System. `<dns_addr>` Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. Dieser Parameter ist optional. `<dns_domain>` Der Domain Name (DNS) ist der Domain-Name. Dieser Parameter ist optional. HINWEIS: Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

6. Ausführen eines Netzboots auf Node_B_1: `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>\_image.tgz` In Schritt 2.

   > Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis der Node_B_1 nun auf dem AFF A900 oder FAS9500 Controller-Modul ausgeführt wird, und zeigen Sie die Startmenüoptionen wie unten dargestellt an:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. Wählen Sie im Startmenü Option `(7) Install new software first`.Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert. HINWEIS: Ignorieren Sie die folgende Meldung: `This procedure is not supported for Non-Disruptive Upgrade on an`

`HA pair`. Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades.

Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen.

9. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein: `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>\_image.tgz`
10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird: `Do you want to restore the backup configuration now? {y|n}`
    b. Eingabe `y to reboot when you see the following prompt: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.
11. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium:
    a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`: `This will delete critical system configuration, including cluster membership. Warning: do not run this option on a HA node that has been taken over. Are you sure you want to continue?:`
    b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.
12. Wählen Sie die Option `5` Wechseln Sie vom Boot-Menü zum Wartungsmodus. Antwort `yes` In die -Eingabeaufforderungen, bis der Node im Wartungsmodus beendet wird, und die Eingabeaufforderung *>.
13. Wiederholen Sie diese Schritte zum Netzboot Node_B_2.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:
    a. Überprüfen Sie die aktuellen Einstellungen der Ports:

    ```
    ucadmin show
    ```

    b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*

CNA-Ethernet	`ucadmin modify -mode cna adapter-name`
FC-Ziel	`fcadmin config -t target adapter-name`
FC-Initiator	`fcadmin config -t initiator adapter-name`

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte sein `mccip`.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mccip
   ```

   ```
   ha-config modify chassis mccip
   ```

3. Stoppen Sie den Knoten: `halt`

   Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

4. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `show date`
5. Stellen Sie bei Bedarf das Datum in UTC oder GMT ein: `set date <mm/dd/yyyy>`
6. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`
7. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`
8. Einstellungen speichern: `saveenv`
9. Umgebungsvariablen erfassen: `printenv`

Aktualisieren Sie die RCF-Dateien des Switches, um die neuen Plattformen aufzunehmen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

   Befolgen Sie die im Abschnitt für den Switch-Anbieter aufgeführten Schritte im Abschnitt *MetroCluster IP Installation and Configuration*.

   "Installation und Konfiguration von MetroCluster IP"

   - "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
   - "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"
2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Folgen Sie den Schritten im Abschnitt Ihres Switch-Anbieters vom "Installation und Konfiguration von MetroCluster IP".

   - "Herunterladen und Installieren der Broadcom RCF-Dateien"
   - "Herunterladen und Installieren der Cisco IP RCF-Dateien"

Konfigurieren Sie die neuen Controller

Neue Controller sollten jetzt bereit und verkabelt sein.

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

Für die neuen Controller-Module müssen bestimmte MetroCluster IP-Bootarg-Werte konfiguriert werden. Die Werte müssen mit den auf den alten Controller-Modulen konfigurierten übereinstimmen.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie die UUIDs und System-IDs, die bereits im Upgrade-Verfahren in identifiziert wurden "Sammeln von Informationen vor dem Upgrade".

Schritte

1. Am `LOADER>` Eingabeaufforderung: Legen Sie folgende Bootargs auf den neuen Knoten an Standort_B fest:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   Im folgenden Beispiel werden die Werte für Node_B_1-A900 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   Im folgenden Beispiel werden die Werte für Node_B_2-A900 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. Bei den neuen Nodes `LOADER` Eingabeaufforderung, UUUIDs festlegen:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Legen Sie die UUIDs auf Node_B_1-A900 fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1-A900 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Legen Sie die UUIDs auf Node_B_2-A900 fest:

   Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2-A900 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Wenn die Originalsysteme für ADP konfiguriert wurden, aktivieren Sie an der LOADER-Eingabeaufforderung der Ersatz-Nodes ADP:

   `setenv bootarg.mcc.adp_enabled true`

4. Legen Sie die folgenden Variablen fest:

   `setenv bootarg.mcc.local_config_id` *`original-sys-id`*

   `setenv bootarg.mcc.dr_partner` *`dr-partner-sys-id`*

   > Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls, Node_B_1-A700 gesetzt werden.

   a. Legen Sie die Variablen auf Node_B_1-A900 fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1-A900 angezeigt:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

   b. Legen Sie die Variablen auf Node_B_2-A900 fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2-A900 angezeigt:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu.

Über diese Aufgabe

Diese Schritte werden im Wartungsmodus ausgeführt.

Schritte

1. Starten des Systems in den Wartungsmodus:

   ```
   boot_ontap maint
   ```

2. Zeigen Sie die Laufwerke auf Node_B_1-A900 in der Eingabeaufforderung Wartungsmodus an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (537403322). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. Weisen Sie die Root-Aggregat-Disks in den Laufwerk-Shelfs den neuen Controllern wieder zu.

Wenn Sie ADP verwenden…	Verwenden Sie dann diesen Befehl…
Ja.	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
Nein	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Weisen Sie die Root-Aggregat-Festplatten in den Laufwerk-Shelfs den neuen Controllern neu zu:

   `disk reassign -s old-sysid -d new-sysid`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken in einer nicht-ADP-Konfiguration:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob die Festplatten des Root-Aggregats korrekt neu zugewiesen sind.

   ```
   disk show
   ```

   ```
   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                     OWNER                     POOL   SERIAL NUMBER
HOME                      DR HOME
------------              -------------             -----  -------------
-------------             -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Booten der neuen Controller

Sie müssen die neuen Controller booten, um sicherzustellen, dass die Bootarg-Variablen korrekt sind und, falls erforderlich, die Verschlüsselungswiederherstellungsschritte durchführen.

Schritte

1. Anhalten der neuen Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Überprüfen Sie, ob die Partner-sysid aktuell ist:

```
printenv partner-sysid
```

Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

4. ONTAP-Startmenü anzeigen:

```
boot_ontap menu
```

5. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

6. Wählen Sie im Startmenü die Option `(6) Update flash from backup config`.

> Mit Option 6 wird der Node vor Abschluss zweimal neu gestartet.

Antworten `y` Zu den Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Unterbrechen Sie den AUTOMATISCHEN START, um die Controller am LOADER zu stoppen.

> Überprüfen Sie auf jedem Knoten die in eingestellten Bootargs "Festlegen der MetroCluster-IP-Bootarg-Variablen" Und korrigieren Sie alle falschen Werte. Gehen Sie nur zum nächsten Schritt, nachdem Sie die Bootarg-Werte überprüft haben.

8. Überprüfen Sie doppelt, ob die Partner-Sysid die richtige ist:

```
printenv partner-sysid
```

Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

9. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

Sie müssen den Wiederherstellungsvorgang durchführen, indem Sie die Option 10 oder Option 11 wählen, abhängig von der Einstellung des Schlüsselmanagers und Option 6 an der Eingabeaufforderung des Startmenüs. Um die Knoten vollständig zu booten, müssen Sie eventuell den Wiederherstellungsvorgang mit Option 1 (normaler Start) durchführen.

10. Warten Sie, bis die neuen Knoten Node_B_1-A900 und Node_B_2-A900 gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

    ```
    network port broadcast-domain show
    ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

    "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

c. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

   VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

   "Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs zu Beginn des Upgrade-Vorgangs auf entsprechenden Nodes und Ports gehostet werden, die zugeordnet sind.

Über diese Aufgabe

- Diese Aufgabe wird auf Site_B. ausgeführt
- Sehen Sie sich den Port-Mapping-Plan an, den Sie in erstellt haben "Zuordnen von Ports von den alten Nodes zu den neuen Nodes".

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Wenn Sie den Befehl zur Änderung der Netzwerkschnittstelle in eingeben `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können das Netzwerk erstellen `interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

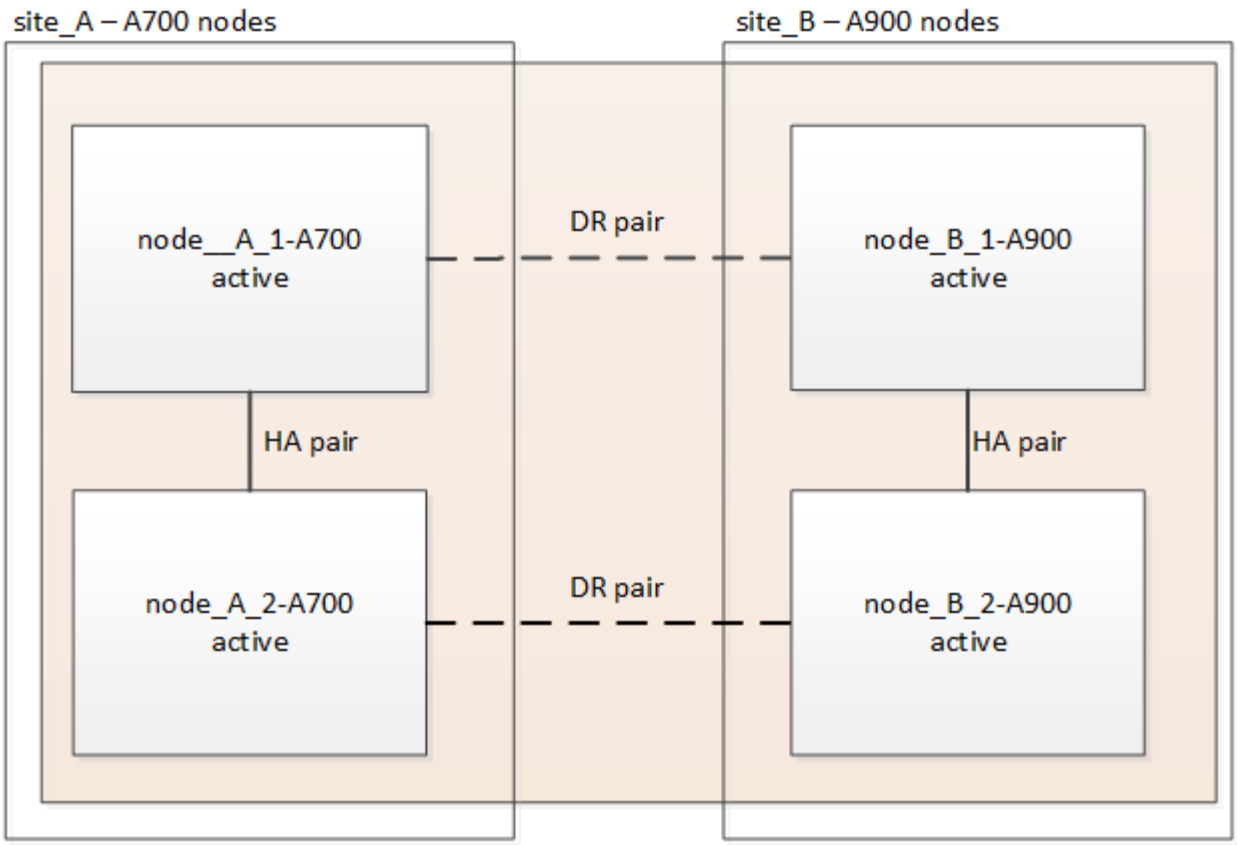
2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   ```
   network interface revert * -vserver vserver-name
   ```

   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Schalten Sie die MetroCluster-Konfiguration zurück

In dieser Aufgabe führen Sie den Vorgang zum zurückwechseln durch, und die MetroCluster-Konfiguration kehrt in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das aus `metrocluster node show` Führen Sie den Befehl von Site_B aus, und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Führen Sie die Reparatur und den Wechsel durch, indem Sie die erforderlichen Befehle von einem beliebigen Node im aktiven Cluster ausführen (das Cluster, das kein Upgrade durchlaufen hat).
   a. Heilen Sie die Datenaggregate:
      `metrocluster heal aggregates`
   b. Heilen Sie die Root-Aggregate:

      ```
      metrocluster heal root
      ```

   c. Zurückwechseln des Clusters:

      ```
      metrocluster switchback
      ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang normal angezeigt wird:

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

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
      `metrocluster show`
   b. Führen Sie eine MetroCluster-Prüfung durch:
      `metrocluster check run`
   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

      ```
      metrocluster check show
      ```

2. Überprüfen Sie die MetroCluster-Konnektivität und den Status.

a. Prüfen Sie die MetroCluster-IP-Verbindungen:

```
storage iscsi-initiator show
```

b. Prüfen Sie, ob die Knoten arbeiten:

```
metrocluster node show
```

c. Überprüfen Sie, ob die MetroCluster IP Schnittstellen aktiv sind:

```
metrocluster configuration-settings interface show
```

d. Überprüfen Sie, ob lokaler Failover aktiviert ist:

```
storage failover show
```

Aktualisieren Sie die Knoten auf site_A

Sie müssen die Upgrade-Aufgaben auf Site_A wiederholen

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Standort_A zu aktualisieren. Beginnen Sie mit "Bereiten Sie sich auf das Upgrade vor".

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Standorten und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von site_A verwendet wird, werden Sie von Site_B. umschalten

Stellen Sie die Tiebreaker- oder Mediator-Überwachung wieder her

Nach Abschluss des Upgrades der MetroCluster-Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

Schritte

1. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen" Im Abschnitt *MetroCluster Tiebreaker Installation and Configuration*.
Mediator	"Konfigurieren des ONTAP Mediator-Dienstes aus einer MetroCluster-IP-Konfiguration" Im Abschnitt *MetroCluster IP-Installation und -Konfiguration*.
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritte

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:
   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Aktualisieren einer MetroCluster FC-Konfiguration mit vier Nodes

Sie können die Controller und den Storage in einer MetroCluster Konfiguration mit vier Nodes aktualisieren, indem Sie die Konfiguration auf eine Konfiguration mit acht Nodes erweitern und anschließend die alte Disaster Recovery-Gruppe (DR) entfernen.

Über diese Aufgabe

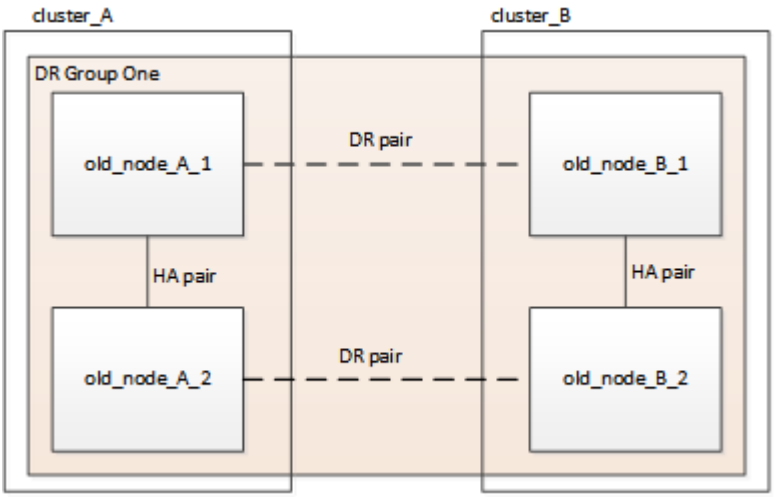
Verweise auf „alte Knoten“ bedeuten die Knoten, die Sie ersetzen möchten.

- Mit diesem Verfahren können Sie nur bestimmte Plattformmodelle in einer MetroCluster FC-Konfiguration aktualisieren.
  - Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster-FC-Aktualisierungstabelle in "Auswahl der Methode zur Systemaktualisierung".

Schritte

1. Erfassung von Informationen von den alten Knoten.

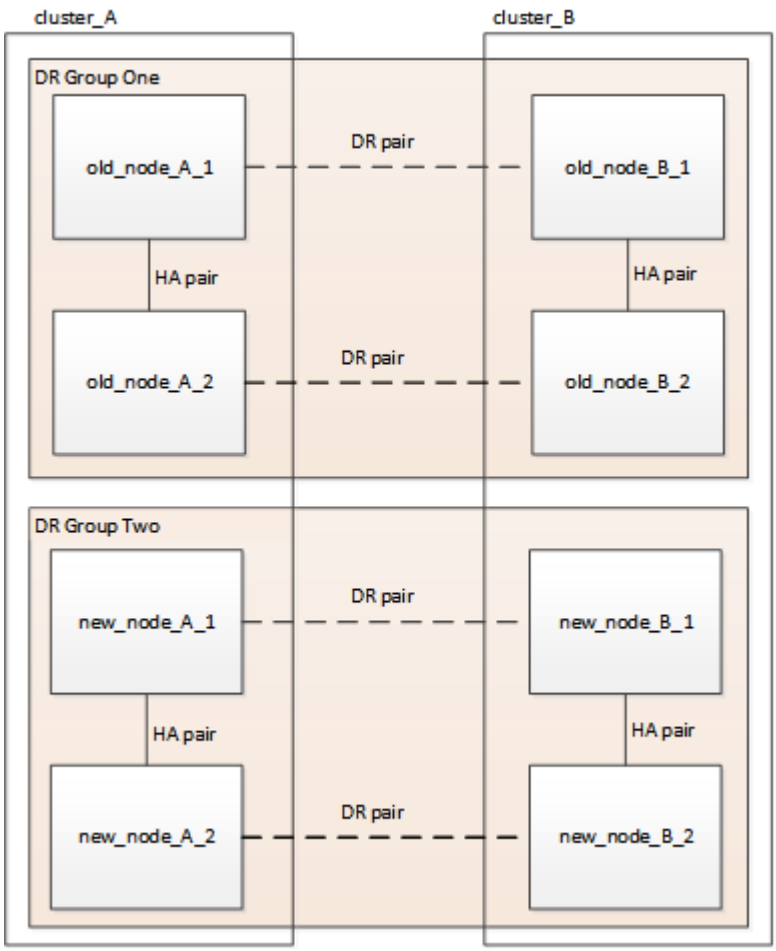
   In dieser Phase wird die Konfiguration mit vier Nodes wie in der folgenden Abbildung dargestellt angezeigt:



2. Führen Sie alle Schritte der Erweiterung mit vier Nodes für Ihren MetroCluster-Typ durch.

   "Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes"

Wenn der Erweiterungsvorgang abgeschlossen ist, wird die Konfiguration wie in der folgenden Abbildung dargestellt angezeigt:



3. Verschieben Sie die CRS-Volumes.

   Führen Sie die Schritte unter aus "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

4. Verschieben Sie die Daten von den alten Knoten auf neue Knoten. Gehen Sie dabei wie folgt vor:
   a. Führen Sie alle Schritte in aus "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes".

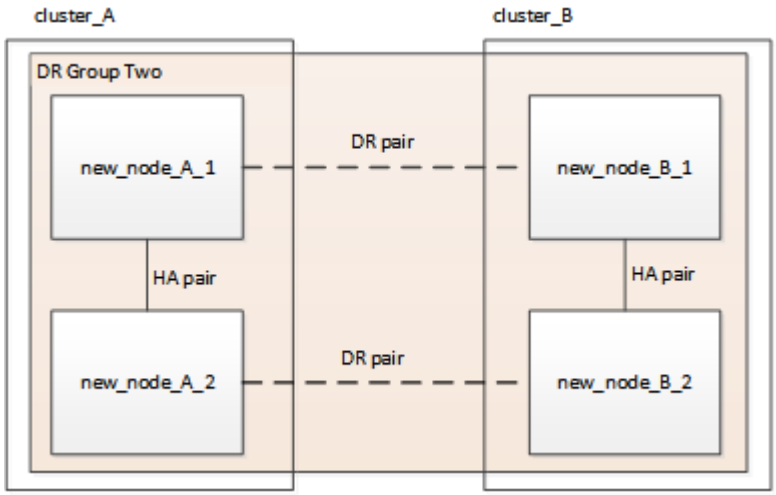
      Sie könnten wählen, um das Aggregat zu spiegeln, wenn oder nachdem es erstellt wurde.

   b. Führen Sie alle Schritte in aus "Verschieben Sie LIFs für nicht-SAN-Daten und Clustermanagement-LIFs auf die neuen Nodes".
   c. Führen Sie alle Schritte in aus "Das Löschen von SAN LIFs ist von den ursprünglichen Nodes nicht mehr erforderlich".
5. Befolgen Sie die Schritte im Verfahren zum Entfernen der alten DR-Gruppe.

   "Entfernen einer Disaster Recovery-Gruppe"

   Nachdem Sie die alte DR-Gruppe (DR-Gruppe 1) entfernt haben, wird die Konfiguration wie im folgenden

Bild dargestellt angezeigt:



Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher)

Mit diesem Verfahren können Sie Controller und Storage in Konfigurationen mit vier oder acht Nodes aktualisieren.

Ab ONTAP 9.13.1 können Sie die Controller und den Speicher in einer MetroCluster IP-Konfiguration mit acht Nodes aktualisieren, indem Sie die Konfiguration zu einer temporären Konfiguration mit zwölf Nodes erweitern und anschließend die alten Disaster Recovery (DR)-Gruppen entfernen.

Ab ONTAP 9.8 können Sie die Controller und den Storage in einer MetroCluster IP-Konfiguration mit vier Nodes aktualisieren, indem Sie die Konfiguration zu einer temporären Konfiguration mit acht Nodes erweitern und dann die alte DR-Gruppe entfernen.

Über diese Aufgabe

- Bei einer Konfiguration mit acht Nodes muss auf dem System ONTAP 9.13.1 oder höher ausgeführt werden.
- Bei einer Konfiguration mit vier Nodes muss auf dem System ONTAP 9.8 oder höher ausgeführt werden.
- Wenn Sie auch die IP-Switches aktualisieren, müssen Sie sie aktualisieren, bevor Sie diese Aktualisierung durchführen.
- In diesem Verfahren werden die Schritte beschrieben, die zum Aktualisieren einer DR-Gruppe mit vier Nodes erforderlich sind. Wenn Sie über eine Konfiguration mit acht Nodes (zwei DR-Gruppen) verfügen, können Sie eine oder beide DR-Gruppen aktualisieren.

  Wenn Sie beide DR-Gruppen aktualisieren, müssen Sie jeweils eine DR-Gruppe aktualisieren.

- Verweise auf „alte Knoten“ bedeuten die Knoten, die Sie ersetzen möchten.
- Bei Konfigurationen mit acht Nodes muss die Kombination aus MetroCluster-Plattform mit acht Quell- und Zielknoten unterstützt werden.

> Wenn Sie beide DR-Gruppen aktualisieren, wird die Plattformkombination möglicherweise nach dem Aktualisieren der ersten DR-Gruppe nicht unterstützt. Sie müssen beide DR-Gruppen aktualisieren, um eine unterstützte Konfiguration mit acht Nodes zu erreichen.

- Sie können nur bestimmte Plattformmodelle aktualisieren, indem Sie dieses Verfahren in einer MetroCluster IP-Konfiguration verwenden.
  - Informationen darüber, welche Plattformupgradekombinationen unterstützt werden, finden Sie in der Tabelle MetroCluster IP-Aktualisierung in "Auswahl der Methode zur Systemaktualisierung".
- Die unteren Limits der Quell- und Zielplattformen gelten. Wenn Sie zu einer höheren Plattform wechseln, gelten die Einschränkungen der neuen Plattform erst nach Abschluss der Technologieaktualisierung für alle DR-Gruppen.
- Wenn Sie eine Technologieaktualisierung für eine Plattform mit niedrigeren Limits als die Quellplattform durchführen, müssen Sie die Grenzwerte anpassen und verringern, um an oder unter den Grenzen der Zielplattform zu liegen, bevor Sie dieses Verfahren durchführen.

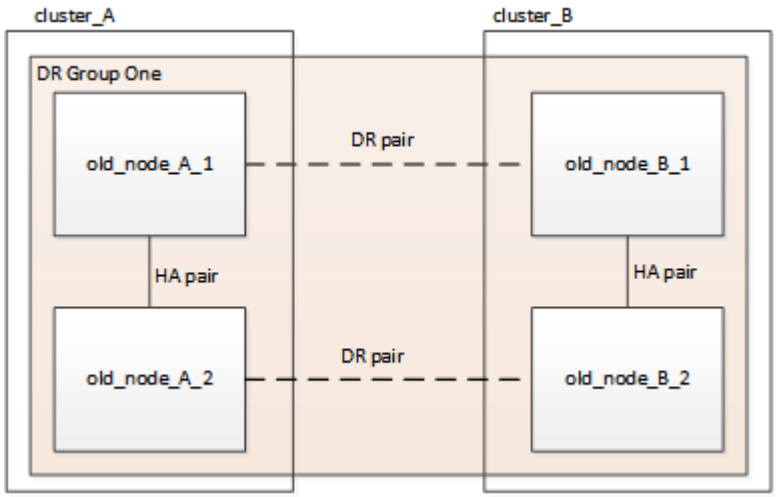
Schritte

1. Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

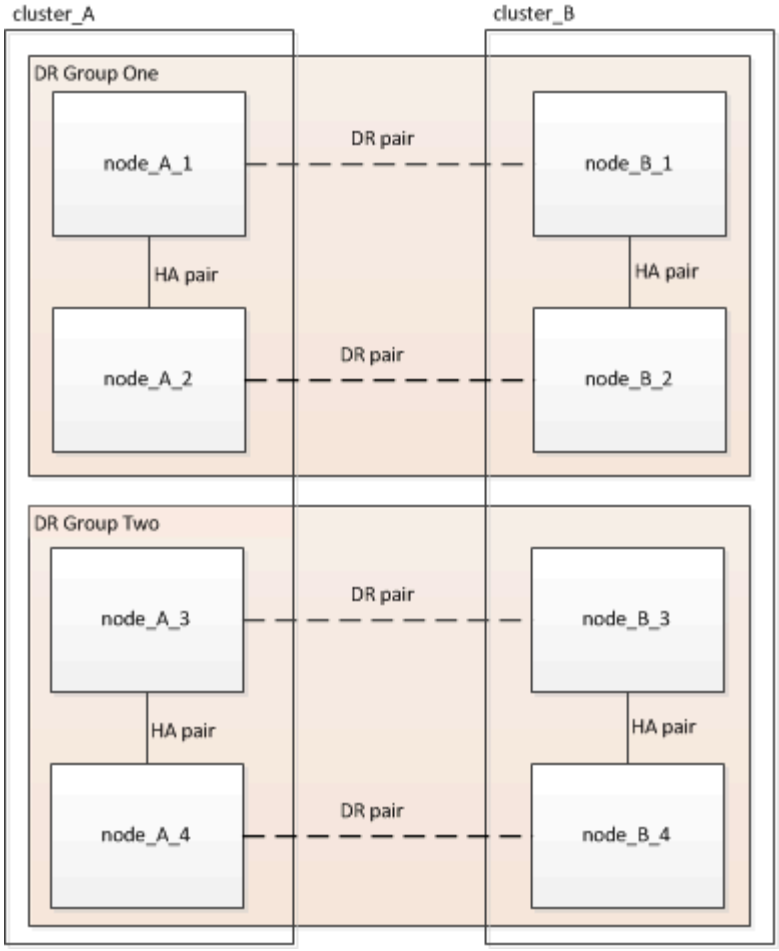
   Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden, sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

2. Erfassung von Informationen von den alten Knoten.

   In dieser Phase wird die Konfiguration mit vier Nodes wie in der folgenden Abbildung dargestellt angezeigt:



   Die Konfiguration mit acht Nodes wird wie im folgenden Bild dargestellt angezeigt:



3. 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 Upgrading old-model to new-model"`

   Das folgende 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.

4. 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	a. Verwenden Sie die Tiebreaker CLI `monitor remove` Befehl zum Entfernen der MetroCluster-Konfiguration.
	
	Im folgenden Beispiel wird „`Cluster_A`“ aus der Software entfernt:
	
	`NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.`
	
	b. Stellen Sie sicher, dass die MetroCluster Konfiguration mithilfe der Tiebreaker CLI ordnungsgemäß entfernt wurde `monitor show -status` Befehl.
	
	`NetApp MetroCluster Tiebreaker :> monitor show -status`

Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

5. Führen Sie alle Schritte in aus "Erweitern einer MetroCluster IP-Konfiguration" Um die neuen Nodes und den neuen Storage zur Konfiguration hinzuzufügen.

   Wenn die Erweiterung abgeschlossen ist, wird die temporäre Konfiguration wie in den folgenden Bildern dargestellt angezeigt:

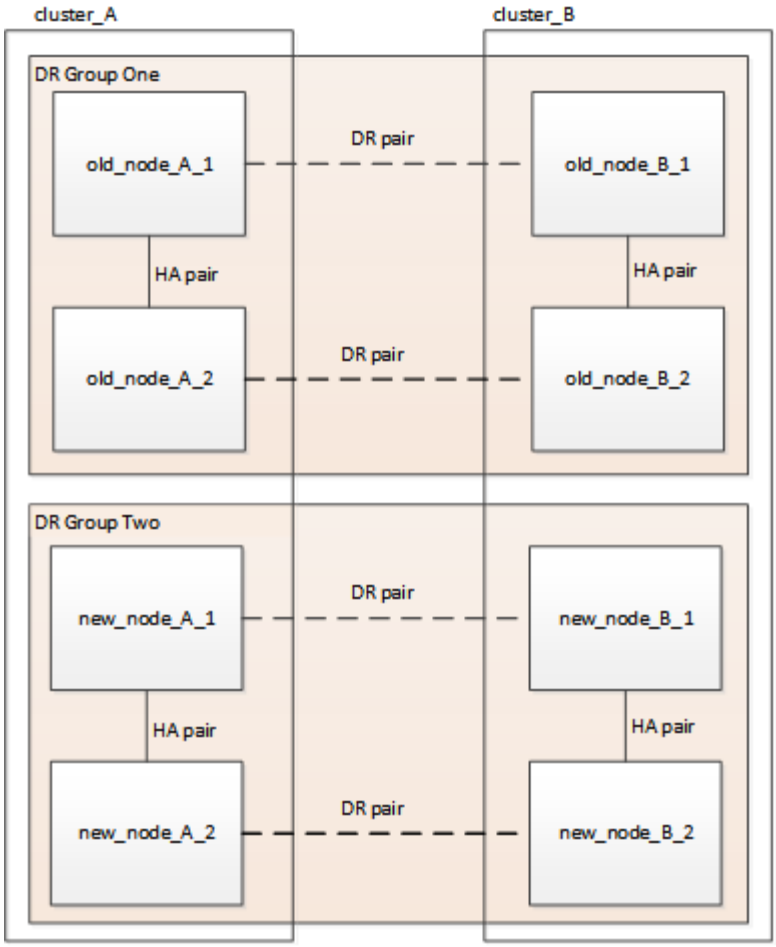


Abbildung 1. Temporäre Konfiguration mit acht Nodes

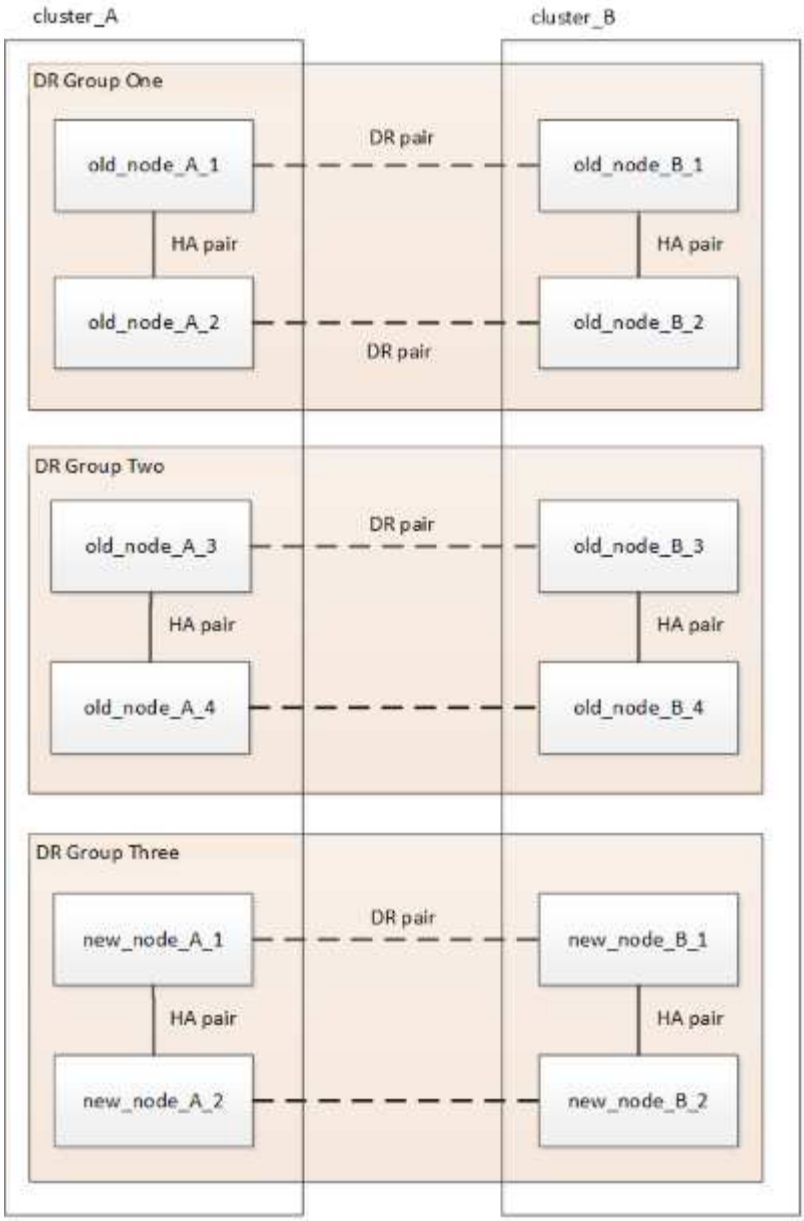


Abbildung 2. Temporäre Konfiguration mit zwölf Nodes

6. Mit dem folgenden Befehl auf beiden Clustern bestätigen Sie, dass ein Takeover möglich ist und die Nodes verbunden sind:

   `storage failover show`

```
cluster_A::> storage failover show
                                      Takeover
Node           Partner                Possible    State Description
-------------- --------------------- ---------   ------------------
Node_FC_1      Node_FC_2                true      Connected to Node_FC_2
Node_FC_2      Node_FC_1                true      Connected to Node_FC_1
Node_IP_1      Node_IP_2                true      Connected to Node_IP_2
Node_IP_2      Node_IP_1                true      Connected to Node_IP_1
```

7. Verschieben Sie die CRS-Volumes.

   Führen Sie die Schritte unter aus "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

8. Verschieben Sie die Daten von den alten Knoten auf die neuen Knoten, indem Sie die folgenden Verfahren durchführen:

   a. Führen Sie alle Schritte in aus "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes".

      Sie könnten wählen, um das Aggregat zu spiegeln, wenn oder nachdem es erstellt wurde.

   b. Führen Sie alle Schritte in aus "Verschieben Sie nicht-SAN-Daten-LIFs und Cluster-Management-LIFs auf die neuen Nodes".

9. Ändern Sie die IP-Adresse für den Cluster-Peer der transitionierten Nodes für jedes Cluster:

   a. Identifizieren Sie den Cluster_A-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

      i. Peer-IP-Adresse „Cluster_A“ ändern:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

   b. Identifizieren Sie den Cluster_B-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

      i. Peer-IP-Adresse für Cluster_B ändern:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

   c. Überprüfen Sie, ob die Cluster-Peer-IP-Adresse für jedes Cluster aktualisiert wurde:

i. Überprüfen Sie mithilfe der, ob die IP-Adresse für jedes Cluster aktualisiert wurde `cluster peer show -instance` Befehl.

   Der `Remote Intercluster Addresses` In den folgenden Beispielen wird die aktualisierte IP-Adresse angezeigt.

   Beispiel für Cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                      Remote Cluster Name: cluster_B
                      Active IP Addresses: 172.21.178.212,
172.21.178.204
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_B_3-IP,
                                          node_B_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+ Beispiel für „Cluster_B“

```
cluster_B::> cluster peer show -instance

                      Peer Cluster Name: cluster_A
           Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. Befolgen Sie die Schritte unter "Entfernen einer Disaster Recovery-Gruppe" Um die alte DR-Gruppe zu entfernen.
11. Wenn Sie beide DR-Gruppen in einer Konfiguration mit acht Nodes aktualisieren möchten, müssen Sie den gesamten Vorgang für jede DR-Gruppe wiederholen.

    Nachdem Sie die alte DR-Gruppe entfernt haben, wird die Konfiguration wie in den folgenden Bildern dargestellt angezeigt:

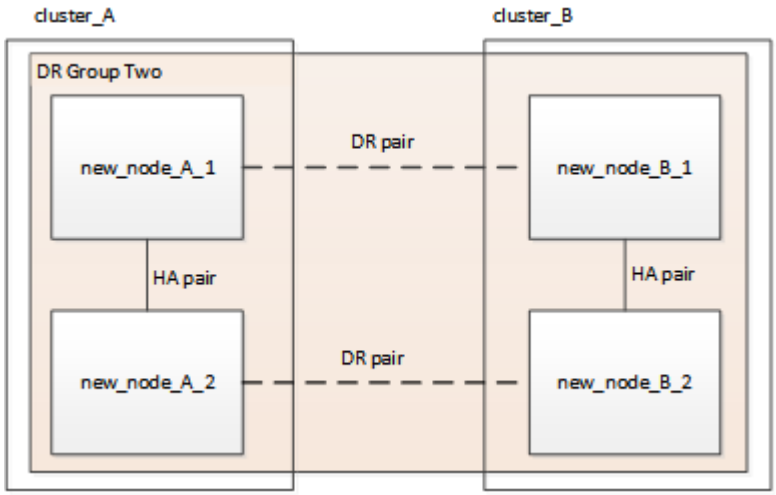


Abbildung 3. Konfiguration mit vier Nodes

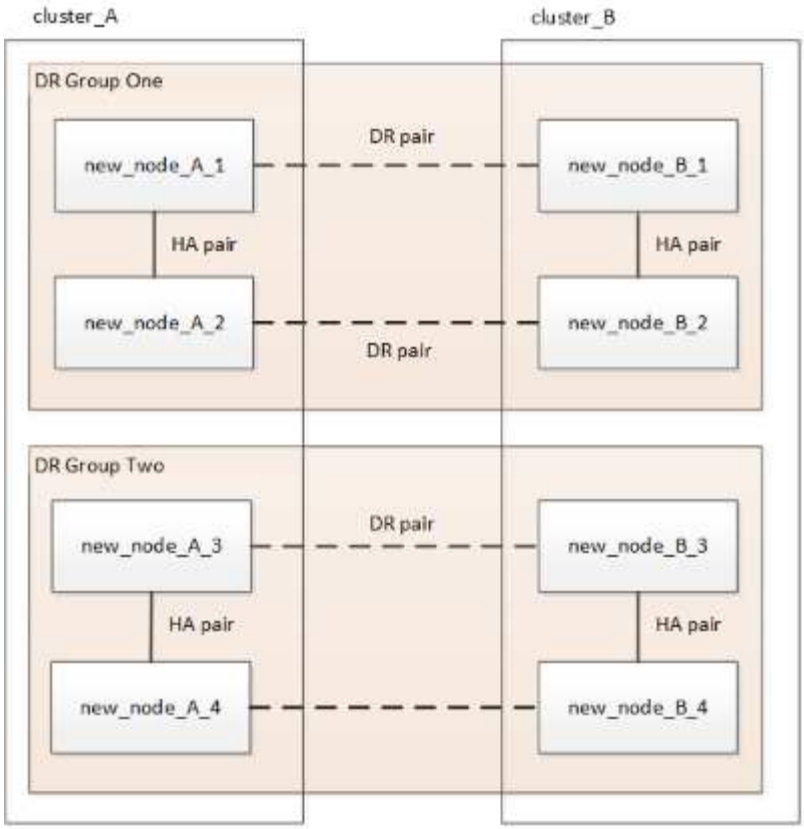


Abbildung 4. Konfiguration mit acht Nodes

12. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.
    a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

    ```
    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
    ```

13. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen" In der *MetroCluster Tiebreaker Installation und Konfiguration*.

Mediator	"Konfigurieren des ONTAP Mediator-Dienstes aus einer MetroCluster-IP-Konfiguration" Im Feld *MetroCluster IP-Installation und -Konfiguration*.
Applikationen von Drittanbietern	Siehe Produktdokumentation.

14. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
    a. Geben Sie den folgenden Befehl ein:

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

    b. Wiederholen Sie den Befehl im Partner-Cluster.

Erweitern Sie eine MetroCluster FC Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes

Erweitern einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes

Wenn Sie eine MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster FC-Konfiguration mit vier Nodes erweitern, muss jedem Cluster ein Controller hinzugefügt werden, um an jedem MetroCluster Standort ein HA-Paar zu bilden, und anschließend die MetroCluster FC-Konfiguration aktualisiert werden.

Bevor Sie beginnen

- Auf den Nodes muss ONTAP 9 oder höher in einer MetroCluster FC-Konfiguration ausgeführt werden.

  Frühere Versionen von ONTAP oder MetroCluster IP-Konfigurationen unterstützen dieses Verfahren nicht.

- Wenn die Plattformen in Ihrer Konfiguration mit zwei Nodes in ONTAP 9.2 nicht unterstützt werden und Sie ein Upgrade auf Plattformen planen, die in ONTAP 9.2 *und* zu einem Cluster mit vier Nodes unterstützt werden, müssen Sie die Plattformen in der Konfiguration mit zwei Nodes _aktualisieren, bevor Sie die MetroCluster FC-Konfiguration erweitern.
- Die vorhandene MetroCluster FC-Konfiguration muss sich in einem ordnungsgemäßen Zustand befindet.
- Die Ausrüstung, die Sie hinzufügen, muss unterstützt werden und alle Anforderungen erfüllen, die in den folgenden Verfahren beschrieben sind:

  "Installation und Konfiguration von Fabric-Attached MetroCluster"

  "Installation und Konfiguration von Stretch MetroCluster"

- Sie benötigen verfügbare FC-Switch-Ports, um die neuen Controller und neue Bridges aufnehmen zu können.
- Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

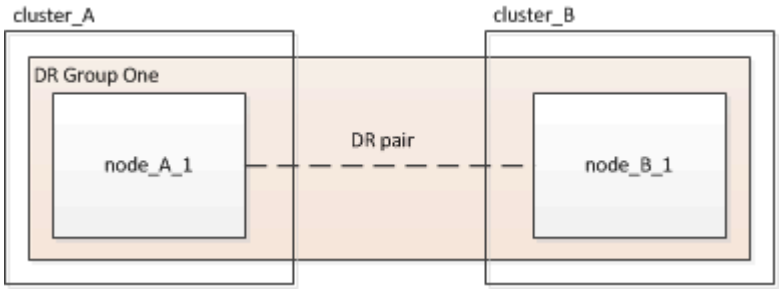
  Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden,

sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

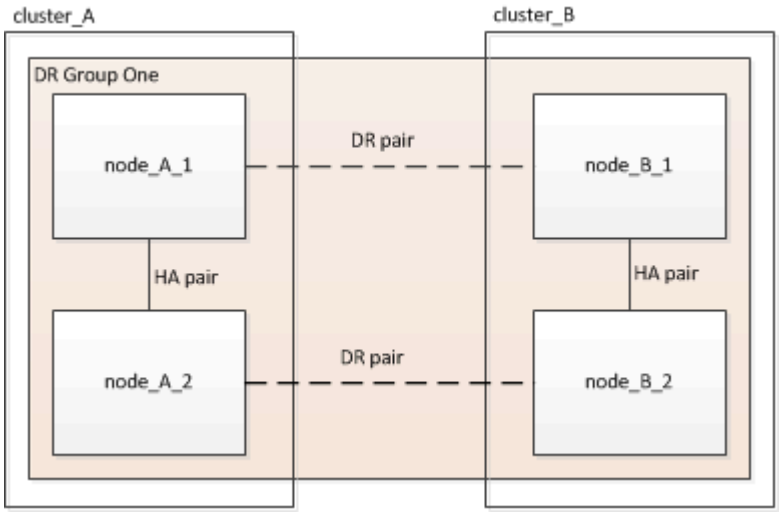
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

Über diese Aufgabe

- Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen.
- Dieser Vorgang ist mit Unterbrechungen verbunden und dauert etwa vier Stunden.
- Bevor Sie dieses Verfahren durchführen, besteht die MetroCluster FC-Konfiguration aus zwei Single-Node-Clustern:



Nach Abschluss dieses Verfahrens besteht die MetroCluster FC-Konfiguration aus zwei HA-Paaren an jedem Standort:



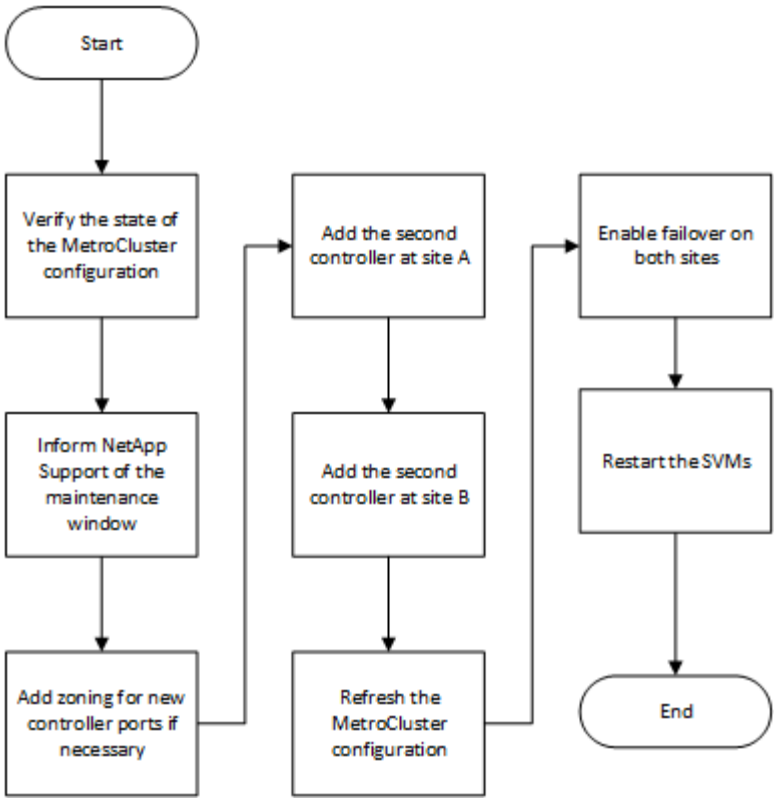
- Beide Standorte müssen gleichermaßen erweitert werden.

  Eine MetroCluster-Konfiguration darf nicht aus einer ungleichmäßigen Anzahl von Nodes bestehen.

- Dieses Verfahren kann pro Standort eine Stunde dauern, wobei zusätzliche Zeit für Aufgaben wie das Initialisieren der Festplatten und das Booten der neuen Nodes ansteht.

  Die Zeit zum Initialisieren der Festplatten hängt von der Größe der Festplatten ab.

- Bei diesem Verfahren wird folgender Workflow verwendet:



Überprüfen des Status der MetroCluster-Konfiguration

Sie sollten die vorhandenen Controller identifizieren und die Disaster Recovery (DR)-Beziehungen zwischen ihnen bestätigen, dass sich die Controller im normalen Modus befinden und die Aggregate gespiegelt werden.

Schritte

1. Zeigt die Details der Nodes in der MetroCluster-Konfiguration von jedem beliebigen Node in der Konfiguration an:

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

   Die folgenden Ausgaben zeigen, dass diese MetroCluster Konfiguration über eine einzelne DR-Gruppe und einen Node pro Cluster verfügt.

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

   dr-group-id  cluster         node            dr-partner      dr-partner-
   systemid
   -----------  -------------   -------         ----------
   -------------------
   1            cluster_A       controller_A_1  controller_B_1  536946192
   1            cluster_B       controller_B_1  controller_A_1  536946165
   2 entries were displayed.
   ```

2. Zeigt den Status der MetroCluster-Konfiguration an:

   ```
   metrocluster show
   ```

   Die folgende Ausgabe zeigt, dass sich die vorhandenen Nodes in der MetroCluster Konfiguration im normalen Modus befinden:

   ```
   cluster_A::> metrocluster show

   Configuration: two-node-fabric

   Cluster                         Entry Name             State
   ------------------------------- -----------------------
   ---------------------
   Local: cluster_A                Configuration State    configured
                                   Mode                   normal
                                   AUSO Failure Domain    auso-on-cluster-
   disaster
   Remote: controller_B_1_siteB
                                   Configuration State    configured
                                   Mode                   normal
                                   AUSO Failure Domain    auso-on-cluster-
   disaster
   ```

3. Überprüfen Sie den Status der Aggregate auf jedem Node in der MetroCluster Konfiguration:

   ```
   storage aggregate show
   ```

   Die folgende Ausgabe zeigt, dass die Aggregate auf Cluster_A online und gespiegelt sind:

   ```
   cluster_A::> storage aggregate show


   Aggregate                 Size     Available Used%  State   #Vols  Nodes
   RAID Status
   ---------                 -------- --------- -----  ------- ------
   ---------------- ------------
   aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
   controller_A_1   raid_dp,mirrored
   controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
   controller_A_1   raid_dp,mirrored
   controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
   controller_A_1   raid_dp,mirrored
   3 entries were displayed.

   cluster_A::>
   ```

Senden einer benutzerdefinierten AutoSupport Meldung, bevor Nodes zur MetroCluster Konfiguration hinzugefügt werden

Sie sollten 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 Site_A beim 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` Der Parameter gibt die Länge des Wartungsfensters an und kann maximal 72 Stunden betragen. Wenn Sie die Wartung vor Ablauf der Zeit abgeschlossen haben, können Sie den folgenden Befehl eingeben, um anzugeben, dass der Wartungszeitraum beendet wurde:

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

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Zoning für die neuen Controller-Ports beim Hinzufügen eines Controller-Moduls in einer Fabric-Attached MetroCluster-Konfiguration

Das FC-Switch-Zoning muss die neuen Controller-Verbindungen aufnehmen. Wenn Sie die von NetApp zur Konfiguration der Switches bereitgestellten Referenzkonfigurationsdateien (RCFs) verwendet haben, ist das Zoning vorkonfiguriert und Sie müssen keine Änderungen vornehmen.

Wenn Sie Ihre FC-Switches manuell konfiguriert haben, müssen Sie sicherstellen, dass das Zoning für die Initiator-Verbindungen der neuen Controller-Module richtig ist. Siehe Abschnitte zum Zoning in "Installation und Konfiguration von Fabric-Attached MetroCluster".

Fügen Sie jedem Cluster ein neues Controller-Modul hinzu

Hinzufügen eines neuen Controller-Moduls zu jedem Cluster

Sie müssen jedem Standort ein neues Controller-Modul hinzufügen, wodurch an jedem Standort ein HA-Paar erstellt wird. Dies ist ein mehrstufiger Prozess, der sowohl Hardware- als auch Softwareänderungen einschließt, die in der richtigen Reihenfolge an jedem Standort durchgeführt werden müssen.

Über diese Aufgabe

- Das neue Controller-Modul muss von NetApp im Rahmen des Upgrade Kits eingehen.

Sie sollten überprüfen, ob PCIe-Karten im neuen Controller-Modul kompatibel sind und vom neuen Controller-Modul unterstützt werden.

"NetApp Hardware Universe"

- Ihr System muss beim Upgrade auf ein HA-Paar in einem Chassis über einen leeren Steckplatz für das neue Controller-Modul verfügen (ein HA-Paar, in dem sich beide Controller-Module im selben Chassis befinden).

  Diese Konfiguration wird nicht auf allen Systemen unterstützt. In ONTAP 9 unterstützte Plattformen mit Einzel-Chassis sind AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080 UND FAS9000.

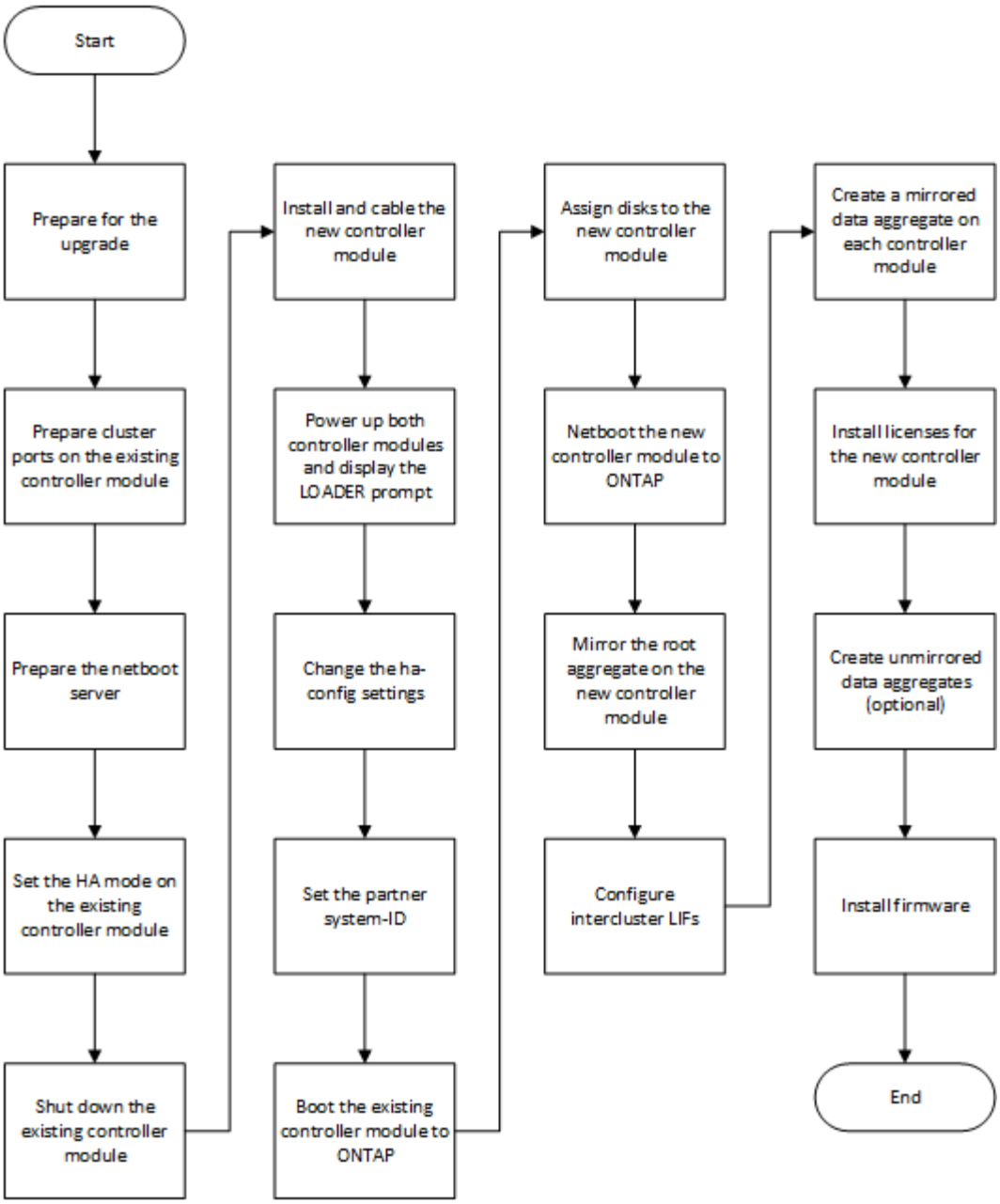
- Bei einem Upgrade auf ein HA-Paar mit zwei Chassis (ein HA-Paar, in dem sich die Controller-Module in einem separaten Chassis befinden) müssen Sie Rack-Platz und Kabel für das neue Controller-Modul haben.

  Diese Konfiguration wird nicht auf allen Systemen unterstützt.

- Sie müssen jedes Controller-Modul über seinen e0a Port mit dem Management-Netzwerk verbinden, oder, wenn Ihr System einen hat, können Sie als Management-Port eine Verbindung mit dem E0M Port herstellen.
- Diese Aufgaben müssen an jedem Standort wiederholt werden.
- Die bestehenden Controller-Module werden als *vorhandene* Controller-Module bezeichnet.

  Die Beispiele in diesem Verfahren enthalten die Konsolenaufforderung `existing_ctlr>`.

- Die hinzugefügten Controller-Module werden als *neue* Controller-Module bezeichnet; die Beispiele in diesem Verfahren haben die Konsolenaufforderung `new_ctlr>`.
- Diese Aufgabe verwendet den folgenden Workflow:



Vorbereitung auf das Upgrade

Vor dem Upgrade auf ein HA-Paar müssen Sie sicherstellen, dass das System alle Anforderungen erfüllt und alle erforderlichen Informationen enthält.

Schritte

1. Identifizieren Sie nicht zugewiesene Festplatten oder Ersatzfestplatten, die Sie dem neuen Controller-Modul mithilfe folgender Befehle zuweisen können:
   - `storage disk show -container-type spare`
   - `storage disk show -container-type unassigned`
2. Führen Sie die folgenden Teilschritte durch:
   a. Ermitteln Sie, wo sich die Aggregate für den vorhandenen Node befinden:

```
storage aggregate show
```

b. Wenn die automatische Zuweisung für die Festplatteneigentümer aktiviert ist, deaktivieren Sie sie:

```
storage disk option modify -node node_name -autoassign off
```

c. Entfernen Sie sich auf Festplatten, die über keine Aggregate verfügen:

```
storage disk removeowner disk_name
```

d. Wiederholen Sie den vorherigen Schritt für so viele Festplatten wie für den neuen Node.

3. Stellen Sie sicher, dass die Kabel für die folgenden Anschlüsse bereit sind:
   - Cluster-Verbindungen

     Wenn Sie einen 2-Node-Cluster ohne Switches erstellen, müssen Sie die Controller-Module mit zwei Kabeln verbinden. Andernfalls sind mindestens vier Kabel erforderlich, zwei für jede Controller-Modulverbindung zum Cluster-Netzwerk-Switch. Andere Systeme (wie die 80xx Serie) verfügen standardmäßig über vier oder sechs Cluster-Verbindungen.

   - HA Interconnect-Verbindungen, wenn sich das System in einem HA-Paar mit Dual-Chassis befindet
4. Überprüfen Sie, ob eine serielle Port-Konsole für die Controller-Module verfügbar ist.
5. Vergewissern Sie sich, dass die Umgebung den Standort- und Systemanforderungen entspricht.

   "NetApp Hardware Universe"

6. Sammeln Sie alle IP-Adressen und anderen Netzwerkparameter für das neue Controller-Modul.

Löschen der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   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.

Vorbereiten von Cluster-Ports auf einem vorhandenen Controller-Modul

Vor dem Installieren eines neuen Controller-Moduls müssen Sie Cluster-Ports auf dem vorhandenen Controller-Modul konfigurieren, damit die Cluster-Ports mit dem neuen Controller-Modul kommunizieren können.

Über diese Aufgabe

Wenn Sie einen 2-Node-Cluster ohne Switches erstellen (ohne Cluster-Netzwerk-Switches), müssen Sie den Switch-freien Cluster-Netzwerkmodus aktivieren.

Ausführliche Informationen zur Port-, LIF- und Netzwerkkonfiguration in ONTAP finden Sie unter "Netzwerkmanagement".

Schritte

1. Legen Sie fest, welche Ports als Cluster-Ports des Node verwendet werden sollen.

   Eine Liste der Standard-Portrollen für Ihre Plattform finden Sie im "Hardware Universe"

   Die Anweisungen *Installation and Setup* für Ihre Plattform auf der NetApp Support Site enthalten Informationen zu den Ports für Cluster-Netzwerkverbindungen.

2. Geben Sie für jeden Cluster-Port die Port-Rollen an:

   ```
   network port show
   ```

   Im folgenden Beispiel müssen die Ports „`e0a`“, „`e0b`“, „`e0c`“ und „`e0d`“ in Cluster-Ports geändert werden:

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. Ändern Sie für alle Daten-LIFs, die einen Cluster-Port als Home-Port oder aktuellen Port verwenden, die LIF, um einen Daten-Port als Home-Port zu verwenden:

   `network interface modify`

   Im folgenden Beispiel wird der Home-Port einer Daten-LIF auf einen Daten-Port geändert:

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. Setzen Sie für jede geänderte LIF auf ihren neuen Home-Port zurück:

   `network interface revert`

   Das folgende Beispiel setzt das LIF „`datalif1`“ auf seinen neuen Home-Port „`e1b`“ zurück:

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und ifgrps, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:
      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

   `network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

   Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN und Interface Group Ports aus Broadcast-Domäne:

   `network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname,..`*

b. Ändern Sie die Schnittstellen-Gruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden.:
   `ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

6. Vergewissern Sie sich, dass sich die Portrollen geändert haben:

   `network port show`

   Das folgende Beispiel zeigt, dass die Ports „`e0a`“, „`e0b`“, „`e0c`“ und „`e0d`“ nun Cluster-Ports sind:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Fügen Sie die Ports zur Cluster Broadcast Domain hinzu:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id, port-id, port-id…`*

   Beispiel:

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. Wenn Ihr System Teil eines geswitchten Clusters ist, erstellen Sie Cluster-LIFs auf den Cluster-Ports: `network interface create`

   Im folgenden Beispiel wird eine Cluster-LIF auf einem der Cluster-Ports des Node erstellt. Der `-auto` Mit dem Parameter wird das LIF so konfiguriert, dass eine Link-lokale IP-Adresse verwendet wird.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. Wenn Sie einen 2-Node-Cluster ohne Switches erstellen, aktivieren Sie den Cluster-Netzwerkmodus ohne Switch:

   a. Ändern Sie von jedem Node auf die erweiterte Berechtigungsebene:

      `set -privilege advanced`

Sie können antworten `y` Wenn Sie gefragt werden, ob Sie den erweiterten Modus fortsetzen möchten. Die Eingabeaufforderung für den erweiterten Modus wird angezeigt (`*>`).

a. Aktivieren Sie den Cluster-Netzwerkmodus ohne Switches:

```
network options switchless-cluster modify -enabled true
```

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

> Die Erstellung der Cluster-Schnittstelle für den vorhandenen Node in einem 2-Node-Cluster-System ohne Switches wird abgeschlossen, nachdem das Cluster-Setup per Netzboot des neuen Controller-Moduls abgeschlossen wurde.

Vorbereiten des Netzboots-Servers zum Herunterladen des Images

Wenn Sie den Netzboot-Server vorbereiten möchten, müssen Sie das korrekte ONTAP-Netzboot-Image von der NetApp Support Site auf den Netzboot-Server herunterladen und die IP-Adresse beachten.

Über diese Aufgabe

- Sie müssen vor und nach dem Hinzufügen des neuen Controller-Moduls auf einen HTTP-Server aus dem System zugreifen können.
- Sie müssen auf die NetApp Support-Website zugreifen können, um die erforderlichen Systemdateien für Ihre Plattform und Ihre Version von ONTAP herunterzuladen.

  "NetApp Support Website"

- Beide Controller-Module im HA-Paar müssen dieselbe Version von ONTAP ausführen.

Schritte

1. 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.

   Der `<ontap_version>_image.tgz` Die Datei wird zum Ausführen eines Netzboots des Systems verwendet.

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

Für…	Dann…

SYSTEME DER FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 SERIE	Extrahieren Sie den Inhalt der Datei <ontap_version>_image.tgz in das Zielverzeichnis:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz` Der Dateiinhalt muss nicht extrahiert werden.

3. Ermitteln Sie die IP-Adresse des vorhandenen Controller-Moduls.

   Diese Adresse wird später in diesem Verfahren als bezeichnet *ip-address-of-existing controller*.

4. Ping *ip-address-of-existing controller* Um zu überprüfen, ob die IP-Adresse erreichbar ist.

Einstellen des HA-Modus auf dem vorhandenen Controller-Modul

Sie müssen den Befehl Storage Failover modify verwenden, um den Modus des vorhandenen Controller-Moduls einzustellen. Der Modus-Wert wird später aktiviert, nachdem Sie das Controller-Modul neu gebootet haben.

Schritte

1. Setzen Sie den Modus auf HA:

   ```
   storage failover modify -mode ha -node existing_node_name
   ```

Herunterfahren des vorhandenen Controller-Moduls

Sie müssen das vorhandene Controller-Modul sauber herunterfahren, um zu überprüfen, ob alle Daten auf die Festplatte geschrieben wurden. Sie müssen auch die Netzteile trennen.

Über diese Aufgabe

Sie müssen ein sauberes System herunterfahren, bevor Sie die Systemkomponenten ersetzen, um zu vermeiden, dass die nicht geschriebenen Daten in NVRAM oder NVMEM verloren gehen.

Schritte

1. Stoppen Sie den Knoten von der vorhandenen Eingabeaufforderung für das Controller-Modul:

   ```
   halt local -inhibit-takeover true
   ```

   Wenn Sie aufgefordert werden, den Vorgang zum Anhalten fortzusetzen, geben Sie ein `y` Wenn Sie dazu aufgefordert werden, und warten Sie, bis das System an der LOADER-Eingabeaufforderung angehalten wird.

   In einem 80xx-System befindet sich die NVRAM-LED auf dem Controller-Modul rechts neben den Netzwerkports, die mit einem Batteriesymbol gekennzeichnet sind.

   Diese LED blinkt, wenn nicht geschriebene Daten im NVRAM vorhanden sind. Wenn diese LED gelb blinkt, nachdem Sie den Befehl zum Anhalten eingegeben haben, müssen Sie das System neu booten und versuchen, das System erneut zu stoppen.

2. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
3. Schalten Sie die Netzteile aus und trennen Sie die Stromversorgung mit der richtigen Methode für Ihr System und Ihren Netzteiltyp:

Setzt Ihr System Folgendes ein:	Dann…
Netzteile	Ziehen Sie die Netzkabel von der Stromversorgung ab, und entfernen Sie anschließend die Netzkabel.
Gleichstromnetzteile	Trennen Sie die Stromversorgung an der Gleichstromquelle, und entfernen Sie ggf. die Gleichstromkabel.

Installieren und verkabeln Sie das neue Controller-Modul

Installieren und Verkabeln des neuen Controller-Moduls

Sie müssen das neue Controller-Modul physisch im Chassis installieren und anschließend verkabeln.

Schritte

1. Wenn Sie ein I/O-Erweiterungsmodul (IOXM) in Ihrem System haben und ein HA-Paar mit einem Chassis erstellen, müssen Sie das IOXM aufheben und entfernen.

   Anschließend können Sie den leeren Schacht für das neue Controller-Modul verwenden. Allerdings bietet die neue Konfiguration nicht die zusätzliche I/O-Leistung des IOXM.

2. Installieren Sie das neue Controller-Modul physisch und installieren Sie bei Bedarf weitere Lüfter:

Wenn Sie ein Controller-Modul hinzufügen…	Führen Sie dann folgende Schritte aus…

Bei einem leeren Schacht für das Erstellen eines HA-Paars mit einem Chassis gehört das System zu einer der folgenden Plattformen:	a. Entfernen Sie die leere Platte auf der Rückseite des Gehäuses, die den leeren Schacht, der das neue Controller-Modul enthält, abdeckt. b. Schieben Sie das Controller-Modul vorsichtig zur Hälfte in das Gehäuse. Um zu verhindern, dass das Controller-Modul automatisch gebootet werden kann, setzen Sie es erst später in diesem Verfahren vollständig im Chassis ein.
In einem separaten Chassis vom HA-Partner zur Erstellung eines HA-Paares mit Dual-Chassis, wenn sich die vorhandene Konfiguration in einer Controller-IOX-Modul-Konfiguration befindet. • FAS8200 • 80xx	Installieren Sie das neue System im Rack oder Systemschrank.

3. Netzwerkkabel des Clusters nach Bedarf verkabeln:

   a. Identifizieren Sie die Ports auf dem Controller-Modul für die Cluster-Verbindungen.

      "AFF A320-Systeme: Installation und Einrichtung"

      "Installations- und Setup-Anleitung für AFF A220/FAS2700 Systeme"

      "Installations- und Setup-Anleitung für AFF A800 Systeme"

      "Installations- und Setup-Anleitung für AFF A300 Systeme"

      "FAS8200 Systems Installation and Setup instructions"

   b. Wenn Sie ein Switch-Cluster konfigurieren, geben Sie die Ports an, die Sie auf den Cluster-Netzwerk-Switches verwenden möchten.

      Siehe "Konfigurationsleitfaden für Clustered Data ONTAP Switches für Cisco Switches", "^NetApp 10G Cluster-Mode-Switch Installationshandbuch" Oder "Installationshandbuch für den NetApp 1G Cluster-Mode Switch", Je nachdem, welche Schalter Sie verwenden.

   c. Verbinden Sie die Kabel mit den Cluster-Ports:

Falls das Cluster…	Dann…
Zwei-Node-Cluster ohne Switches	Verbinden Sie die Cluster-Ports des vorhandenen Controller-Moduls direkt mit den entsprechenden Cluster-Ports des neuen Controller-Moduls.
Cluster mit Switches	Verbinden Sie die Cluster-Ports an jedem Controller mit den Ports auf den in Unterschritt B angegebenen Cluster-Netzwerk-Switches

Verkabelung der FC-VI- und HBA-Ports des neuen Controller-Moduls an die FC-Switches

Die FC-VI-Ports und HBAs (Host Bus Adapter) des neuen Controller-Moduls müssen mit den FC-Switches am Standort verbunden sein.

Schritte

1. Verkabeln Sie die FC-VI-Ports und HBA-Ports mit der Tabelle für Ihre Konfiguration und Ihr Switch-Modell.
   - "Port-Zuweisungen für FC-Switches bei Verwendung von ONTAP 9.1 und höher"
   - "Port-Zuweisungen für FC-Switches bei Verwendung von ONTAP 9.0"
   - "Port-Zuweisungen für Systeme mit zwei Initiator-Ports"

Verkabelung der Cluster-Peering-Verbindungen des neuen Controller-Moduls

Sie müssen das neue Controller-Modul mit dem Cluster-Peering-Netzwerk verkabeln, damit es eine Verbindung mit dem Cluster am Partnerstandort hat.

Über diese Aufgabe

Mindestens zwei Ports auf jedem Controller-Modul sollten für Cluster-Peering verwendet werden.

Die empfohlene minimale Bandbreite für die Ports und Netzwerkkonnektivität ist 1 GbE.

Schritte

1. Identifizieren und verkabeln Sie mindestens zwei Ports für Cluster-Peering und vergewissern Sie sich, dass sie über eine Netzwerkverbindung mit dem Partner-Cluster verfügen.

Einschalten beider Controller-Module und Anzeigen der LOADER-Eingabeaufforderung

Sie schalten das vorhandene Controller-Modul und das neue Controller-Modul ein, um die LOADER-Eingabeaufforderung anzuzeigen.

Schritte

Schalten Sie die Controller-Module aus und unterbrechen Sie den Bootvorgang, indem Sie die Schritte für Ihre Konfiguration verwenden:

Wenn die Controller-Module…	Dann…

Im gleichen Chassis	1. Vergewissern Sie sich, dass das neue Controller-Modul **nicht** vollständig in den Schacht eingesetzt ist. Das vorhandene Controller-Modul sollte vollständig in den Schacht eingesetzt werden, da es nie aus dem Chassis entfernt wurde, das neue Controller-Modul jedoch nicht sein sollte. 2. Schließen Sie das Netzteil an, und schalten Sie die Netzteile ein, sodass das vorhandene Controller-Modul mit Strom versorgt wird. 3. Unterbrechen Sie den Boot-Vorgang des vorhandenen Controller-Moduls, indem Sie Strg-C drücken 4. Drücken Sie das neue Controller-Modul fest in den Schacht. Wenn das neue Controller-Modul voll eingesetzt ist, wird es mit Strom versorgt und wird automatisch gestartet. 5. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken 6. Ziehen Sie ggf. die Daumenschraube am Nockengriff fest. 7. Installieren Sie das Kabelverwaltungsgerät, falls vorhanden. 8. Verbinden Sie die Kabel mit dem Haken- und Schlaufenband mit dem Kabelmanagement-Gerät.
In einem separaten Chassis	1. Schalten Sie die Netzteile des vorhandenen Controller-Moduls ein. 2. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken 3. Wiederholen Sie diese Schritte für das neue Controller-Modul

Jedes Controller-Modul sollte die LOADER-Eingabeaufforderung anzeigen (`LOADER>`, `LOADER-A>`, Oder `LOADER-B>`).

> Wenn keine LOADER-Eingabeaufforderung angezeigt wird, notieren Sie die Fehlermeldung. Wenn das Startmenü angezeigt wird, starten Sie den Neustart neu, und versuchen Sie erneut, den Bootvorgang zu unterbrechen.

Ändern der HA-Konfigurationseinstellung für die vorhandenen und neuen Controller-Module

Wenn Sie eine MetroCluster-Konfiguration erweitern, müssen Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls und des neuen Controller-Moduls aktualisieren. Sie müssen außerdem die System-ID des neuen Controller-Moduls bestimmen.

Über diese Aufgabe

Diese Aufgabe wird sowohl bei vorhandenen als auch bei neuen Controller-Modulen im Wartungsmodus ausgeführt.

Schritte

1. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls:

a. Zeigen Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls und des Gehäuses an:

```
ha-config show
```

Die HA-Konfigurationseinstellung ist für alle Komponenten „`mcc-2n`“, da sich das Controller-Modul in einer MetroCluster-Konfiguration mit zwei Knoten befand.

b. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls in „`mcc`“:
`ha-config modify controller mcc`

c. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Gehäuses in „`mcc`“:

```
ha-config modify chassis mcc
```

d. Rufen Sie die System-ID für das vorhandene Controller-Modul ab:

```
sysconfig
```

Notieren Sie die System-ID. Sie benötigen es, wenn Sie die Partner-ID auf dem neuen Controller-Modul einstellen.

a. Beenden Sie den Wartungsmodus, um zur LOADER-Eingabeaufforderung zurückzukehren:

```
halt
```

2. Ändern Sie die HA-Konfigurationseinstellung und rufen Sie die System-ID des neuen Controller-Moduls ab:

a. Wenn sich das neue Controller-Modul nicht bereits im Wartungsmodus befindet, starten Sie es in den Wartungsmodus:

```
boot_ontap maint
```

b. Ändern Sie die HA-Konfigurationseinstellung des neuen Controller-Moduls in „`mcc`“:

```
ha-config modify controller mcc
```

c. Ändern Sie die HA-Konfigurationseinstellung des neuen Chassis in mcc:

```
ha-config modify chassis mcc
```

d. Rufen Sie die System-ID für das neue Controller-Modul ab:

```
sysconfig
```

Notieren Sie die System-ID. Sie benötigen es, wenn Sie die Partner-ID festlegen und dem neuen Controller-Modul Festplatten zuweisen.

a. Beenden Sie den Wartungsmodus, um zur LOADER-Eingabeaufforderung zurückzukehren:

```
halt
```

Festlegen der Partner-System-ID für beide Controller-Module

Sie müssen die Partner-System-ID auf beiden Controller-Modulen festlegen, damit sie ein HA-Paar bilden können.

Über diese Aufgabe

Dieser Task wird an der LOADER-Eingabeaufforderung mit beiden Controller-Modulen ausgeführt.

Schritte

1. Legen Sie im vorhandenen Controller-Modul die Partner-System-ID auf die des neuen Controller-Moduls fest:

   ```
   setenv partner-sysid sysID_of_new_controller
   ```

2. Stellen Sie bei dem neuen Controller-Modul die Partner-System-ID auf die des vorhandenen Controller-Moduls ein:

   ```
   setenv partner-sysid sysID_of_existing_controller
   ```

Booten des vorhandenen Controller-Moduls

Sie müssen das vorhandene Controller-Modul bei ONTAP booten.

Schritte

1. Booten Sie an der LOADER-Eingabeaufforderung das vorhandene Controller-Modul in ONTAP:

   ```
   boot_ontap
   ```

Zuweisen von Festplatten zum neuen Controller-Modul

Bevor Sie die Konfiguration des neuen Controller-Moduls über einen Netzboot ausführen, müssen Sie ihm Festplatten zuweisen.

Über diese Aufgabe

Sie müssen sicherstellen, dass genügend Ersatzteile, nicht zugewiesene Festplatten oder zugewiesene Festplatten nicht Teil eines vorhandenen Aggregats sind.

"Vorbereitung auf das Upgrade"

Diese Schritte werden am vorhandenen Controller-Modul durchgeführt.

Schritte

1. Weisen Sie die Root-Festplatte dem neuen Controller-Modul zu:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

   Wenn Ihr Plattformmodell die ADP-Funktion (Advanced Drive Partitioning) verwendet, müssen Sie den Parameter -root true angeben:

   ```
   storage disk assign -disk disk_name -root true -sysid new_controller_sysID
   -force true
   ```

2. Weisen Sie dem neuen Controller-Modul die verbleibenden erforderlichen Festplatten zu, indem Sie für jede Festplatte den folgenden Befehl eingeben:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

3. Vergewissern Sie sich, dass die Festplattenzuordnungen korrekt sind:

   ```
   storage disk show -partitionownership*
   ```

   Stellen Sie sicher, dass Sie alle Laufwerke zugewiesen haben, die Sie dem neuen Knoten zuweisen möchten.

Booten und Einrichten von ONTAP auf dem neuen Controller-Modul

Sie müssen eine bestimmte Sequenz von Schritten zum Netzboot ausführen und das ONTAP Betriebssystem auf dem neuen Controller-Modul installieren, wenn Sie einer vorhandenen MetroCluster Konfiguration Controller-Module hinzufügen.

Über diese Aufgabe

- Diese Aufgabe wird bei der LOADER-Eingabeaufforderung des neuen Controller-Moduls gestartet.
- Diese Aufgabe umfasst die Initialisierung von Datenträgern.

  Die Dauer, die zur Initialisierung der Festplatten benötigt wird, hängt von der Größe der Festplatten ab.

- Das System weist dem neuen Controller-Modul automatisch zwei Festplatten zu.

  "Festplatten- und Aggregatmanagement"

Schritte

1. Konfigurieren Sie an der LOADER-Eingabeaufforderung die IP-Adresse des neuen Controller-Moduls basierend auf der DHCP-Verfügbarkeit:

DHCP ist…	Geben Sie dann den folgenden Befehl ein…
Verfügbar	**`ifconfig e0M -auto`**

Nicht verfügbar	`ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Storage-Systems. *`netmask`* Ist die Netzwerkmaske des Storage-Systems. *`gateway`* Ist das Gateway für das Storage-System. *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Verwenden Sie für Details den `help ifconfig` Befehl an der LOADER-Eingabeaufforderung.

2. An der LOADER-Eingabeaufforderung „Netzboot“ des neuen Node:

Für…	Geben Sie diesen Befehl aus…
SYSTEME DER FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 SERIE	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Alle anderen Systeme	`netboot http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

Der *`path_to_the_web-accessible_directory`* Befindet sich der Speicherort des heruntergeladenen `<ontap_version>_image.tgz` Datei:

3. Wählen Sie im angezeigten Menü die Option **Neue Software zuerst installieren** aus.

   Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

   - Sie sollten „`y`“ eingeben, wenn Sie dazu aufgefordert werden, dass dieses Verfahren nicht für ein unterbrechungsfreies Upgrade auf einem HA-Paar unterstützt wird.
   - Sie sollten „`y`“ eingeben, wenn Sie darauf hingewiesen werden, dass dieser Prozess die vorhandene ONTAP-Software durch neue Software ersetzt.
   - Sie sollten bei der Aufforderung zur URL der Datei image.tgz den Pfad wie folgt eingeben:

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Geben Sie „`y`“ ein, wenn Sie dazu aufgefordert werden, ein unterbrechungsfreies Upgrade oder Austausch der Software zu starten.

5. Geben Sie den Pfad zur Datei image.tgz ein, wenn Sie zur URL des Pakets aufgefordert werden.

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. Geben Sie „n“ ein, um die Backup-Wiederherstellung zu überspringen, wenn Sie dazu aufgefordert werden, die Backup-Konfiguration wiederherzustellen.

```
*****************************************************************
*             Restore Backup Configuration                      *
*  This procedure only applies to storage controllers that      *
*  are configured as an HA pair.                                *
*                                                               *
*  Choose Yes to restore the "varfs" backup configuration       *
*  from the SSH server.  Refer to the Boot Device Replacement   *
*  guide for more details.                                      *
*  Choose No to skip the backup recovery and return to the      *
*  boot menu.                                                   *
*****************************************************************

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

7. Geben Sie „y“ ein, wenn Sie dazu aufgefordert werden, den Neustart jetzt durchzuführen.

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

8. Wählen Sie bei Bedarf die Option **Clean Configuration aus und initialisieren Sie alle Festplatten**, nachdem der Knoten gestartet wurde.

   Da Sie ein neues Controller-Modul konfigurieren und die Festplatten des neuen Controller-Moduls leer sind, können Sie „y“ antworten, wenn das System Sie darauf warnt, dass alle Festplatten gelöscht werden.

   > Die Zeit, die zum Initialisieren von Festplatten benötigt wird, hängt von der Größe der Festplatten und der Konfiguration ab.

9. Nachdem die Festplatten initialisiert wurden und der Setup-Assistent für das Cluster gestartet wurde, richten Sie den Node ein:

   Geben Sie die LIF-Informationen zum Node-Management auf der Konsole ein.

10. Melden Sie sich bei dem Node an, und geben Sie den ein `cluster setup` Und geben Sie dann „`join`“ ein, wenn Sie dazu aufgefordert werden, dem Cluster beizutreten.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. Beantworten Sie die verbleibenden Eingabeaufforderungen für Ihren Standort.

    Der "Einrichtung von ONTAP" Für Ihre Version von ONTAP enthält zusätzliche Details.

12. Wenn sich das System in einer 2-Node-Konfiguration ohne Switches befindet, erstellen Sie die Cluster-Schnittstellen auf dem vorhandenen Node. Verwenden Sie dabei den Befehl „Network Interface create“, um Cluster LIFs auf den Cluster-Ports zu erstellen.

    Der folgende Befehl ist ein Beispiel zum Erstellen einer Cluster-LIF auf einem der Cluster-Ports des Node. Der Parameter -Auto konfiguriert das LIF so, dass eine Link-lokale IP-Adresse verwendet wird.

    ```
    cluster_A::> network interface create -vserver Cluster -lif clus1 -role
    cluster -home-node node_A_1 -home-port e1a -auto true
    ```

13. Nach Abschluss der Einrichtung vergewissern Sie sich, dass der Node sich in einem ordnungsgemäßen Zustand befindet und berechtigt ist, am Cluster teilzunehmen:

    ```
    cluster show
    ```

    Das folgende Beispiel zeigt einen Cluster, nachdem der zweite Node (cluster1-02) damit verbunden wurde:

    ```
    cluster_A::> cluster show
    Node                  Health  Eligibility
    --------------------- ------- ------------
    node_A_1              true    true
    node_A_2              true    true
    ```

    Sie können mit dem Cluster Setup-Assistenten einen der Werte, die Sie für die SVM (Admin Storage Virtual Machine) oder Node-SVM eingegeben haben, über den Cluster-Setup-Befehl ändern.

14. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

    ```
    network port show
    ```

    Das folgende Beispiel zeigt die Ausgabe für zwei Controller-Module in „Cluster_A“:

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

Spiegelung des Root-Aggregats auf dem neuen Controller

Sie müssen das Root-Aggregat spiegeln, um Datensicherung zu ermöglichen, wenn Sie einer MetroCluster-Konfiguration einen Controller hinzufügen.

Diese Aufgabe muss am neuen Controller-Modul ausgeführt werden.

1. Root-Aggregat spiegeln:

   `storage aggregate mirror` *`aggr_name`*

   Der folgende Befehl spiegelt das Root-Aggregat für Controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

Konfigurieren Sie Intercluster LIFs

Konfigurieren von Intercluster-LIFs auf dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

   ```
   cluster01::> network port show
                                                                    Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   ```
   network interface show -fields home-port,curr-port
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Das folgende Beispiel weist den Failover-Gruppe „intercluster01“ auf der System-SVM „cluster01“ die Ports „e0e“ und „e0f“ zu:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   `network interface failover-groups show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

ONTAP-Version	Befehl
9.6 und höher	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 und früher	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic02“ in der Failover-Gruppe „intercluster01“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem SVM „e0e“-Port an den „e0f“-Port scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                            Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

Im ONTAP 9.6 und höher:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 und früher:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern wird.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

  In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

> Es wird empfohlen, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

```
storage disk show -spare -owner node_name
```

2. Erstellen Sie das Aggregat:

```
storage aggregate create -mirror true
```

Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um sicherzustellen, dass das Aggregat auf einem bestimmten Node erstellt wird, verwenden Sie die `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

Sie können die folgenden Optionen angeben:

- Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
- Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
- Anzahl der zu einführenden Laufwerke

> In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

- Prüfsummenstil, den Sie für das Aggregat verwenden möchten
- Typ der zu verwendenden Laufwerke
- Die Größe der zu verwendenden Laufwerke
- Fahrgeschwindigkeit zu verwenden
- RAID-Typ für RAID-Gruppen auf dem Aggregat
- Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
- Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

  Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

  Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

```
storage aggregate show-status -aggregate aggregate-name
```

Installieren von Lizenzen für das neue Controller-Modul

Lizenzen für das neue Controller-Modul müssen für alle ONTAP Services hinzugefügt werden, die Standard-Lizenzen (mit Nodes gesperrt) erfordern. Bei Standardlizenzen

muss jeder Node im Cluster über seinen eigenen Schlüssel für die Funktion verfügen.

Ausführliche Informationen zur Lizenzierung finden Sie in der Knowledge Base-Artikel 3013749: Übersicht über die Data ONTAP 8.2 Lizenzierung und Referenzen auf der NetApp Support Site und *System Administration Reference*.

Schritte

1. Falls erforderlich, beziehen Sie Lizenzschlüssel für den neuen Node auf der NetApp Support Site im Abschnitt „My Support“ unter „Software-Lizenzen“.

   Weitere Informationen zum Austausch von Lizenzen finden Sie im Knowledge Base-Artikel "Verfahren zum Austausch der Hauptplatine zur Aktualisierung der Lizenzierung auf einem All Flash FAS/FAS System"

2. Geben Sie den folgenden Befehl ein, um jeden Lizenzschlüssel zu installieren:

   ```
   system license add -license-code license_key
   ```

   Der *license_key* Ist 28 Ziffern lang.

3. Wiederholen Sie diesen Schritt für jede erforderliche Standard-Lizenz (Node-locked).

Erstellen von nicht gespiegelten Datenaggregaten

Optional können Sie nicht gespiegelte Datenaggregate für Daten erstellen, für die keine redundante Spiegelung von MetroCluster-Konfigurationen erforderlich ist.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke oder Array LUNs im neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie überprüfen können, ob der richtige Laufwerkstyp ausgewählt ist.

> In MetroCluster IP-Konfigurationen können Remote-Aggregate nach einem Switchover nicht zugänglich gemacht werden

> Die nicht gespiegelten Aggregate müssen sich lokal an dem Node halten, auf dem sie sich enthalten.

- Laufwerke und Array-LUNs sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat Eigentum desselben Node sein, der zum Home Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- *Festplatten- und Aggregatmanagement* enthält weitere Informationen zur Spiegelung von Aggregaten.

Schritte

1. Installieren und verkabeln Sie die Festplatten-Shelfs, die die nicht gespiegelten Aggregate enthalten.

   Sie können die Verfahren in der Dokumentation *Installation and Setup* für Ihre Plattform und Platten-Shelfs verwenden.

   "Dokumentation zu ONTAP Hardwaresystemen"

2. Weisen Sie alle Festplatten auf dem neuen Shelf dem entsprechenden Node manuell zu:

   `disk assign -disk disk-id -owner owner-node-name`

3. Erstellen Sie das Aggregat:

   `storage aggregate create`

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Node erstellt wird, sollten Sie das verwenden `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

   Darüber hinaus müssen Sie sicherstellen, dass Sie nur Laufwerke in das nicht gespiegelte Shelf zum Aggregat aufnehmen.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste bestimmter Laufwerke oder Array LUNs, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken oder Array-LUNs, die in einer RAID-Gruppe enthalten sein können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

     Mit dem folgenden Befehl wird ein nicht gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

4. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate aggregate-name`

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Installieren der Firmware nach dem Hinzufügen eines Controller-Moduls

Nach dem Hinzufügen des Controller-Moduls müssen Sie die aktuelle Firmware auf dem neuen Controller-Modul installieren, damit das Controller-Modul ordnungsgemäß mit ONTAP funktioniert.

Schritte

1. Laden Sie die aktuelle Firmware-Version für Ihr System herunter und befolgen Sie die Anweisungen zum Herunterladen und Installieren der neuen Firmware.

   "NetApp Downloads: System-Firmware und -Diagnose"

Aktualisierung der MetroCluster Konfiguration durch neue Controller

Sie müssen die MetroCluster Konfiguration aktualisieren, wenn Sie sie von einer Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes erweitern.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Rufen Sie den erweiterten Berechtigungsmodus auf:
      `set -privilege advanced`

   b. Aktualisieren Sie die MetroCluster-Konfiguration:
      `metrocluster configure -refresh true -allow-with-one-aggregate true`

      Mit dem folgenden Befehl wird die MetroCluster-Konfiguration auf allen Nodes in der DR-Gruppe aktualisiert, die Controller_A_1 enthält:

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

   a. Zurück zum Admin-Berechtigungsmodus:

      `set -privilege admin`

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

   `network port show`

   Im folgenden Beispiel wird die Verwendung von Netzwerkports in einer MetroCluster Konfiguration mit vier Nodes angezeigt:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

   a. Überprüfen Sie die Konfiguration von Standort A:

   ```
   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. Überprüfen Sie die Konfiguration von Standort B:

   ```
   metrocluster show
   ```

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

c. Überprüfen Sie, ob die DR-Beziehungen korrekt erstellt wurden:

   `metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner`

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Aktivieren von Storage Failover auf beiden Controller-Modulen und Aktivieren von Cluster HA

Nachdem Sie der MetroCluster Konfiguration neue Controller-Module hinzugefügt haben, müssen Sie Storage Failover auf beiden Controller-Modulen aktivieren und die separat aktiviert werden.

Bevor Sie beginnen

Die MetroCluster Konfiguration muss zuvor mit dem aktualisiert worden sein `metrocluster configure -refresh true` Befehl.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Storage-Failover:

   ```
   storage failover modify -enabled true -node existing-node-name
   ```

   Der einzelne Befehl ermöglicht ein Storage Failover beider Controller-Module.

2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   ```
   storage failover show
   ```

   Die Ausgabe sollte wie folgt aussehen:

   ```
   Node           Partner        Possible State Description
   -------------- -------------- -------- ----------------------
   old-ctlr        new-ctlr      true      Connected to new-ctlr
   new-ctlr        old-ctlr      true      Connected to old-ctlr
   2 entries were displayed.
   ```

3. Cluster-HA aktivieren:

   ```
   cluster ha modify -configured true
   ```

   Cluster High Availability (HA) muss in einem Cluster konfiguriert werden, wenn es nur zwei Nodes enthält und sich von der durch Storage Failover gelieferten HA unterscheidet.

Starten Sie die SVMs neu

Nach erweitern der MetroCluster Konfiguration müssen Sie die SVMs neu starten.

Schritte

1. Identifizieren Sie die SVMs, die neu gestartet werden müssen:

   ```
   metrocluster vserver show
   ```

   Dieser Befehl zeigt die SVMs auf beiden MetroCluster Clustern.

2. Starten Sie die SVMs auf dem ersten Cluster neu:

   a. Rufen Sie den erweiterten Berechtigungsmodus auf, und drücken Sie **y** Wenn Sie dazu aufgefordert werden:

      ```
      set -privilege advanced
      ```

   b. Starten Sie die SVMs neu:

      ```
      vserver start -vserver SVM_name -force true
      ```

   c. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

3. Wiederholen Sie den vorherigen Schritt im Partner-Cluster.
4. Vergewissern Sie sich, dass sich die SVMs in einem ordnungsgemäßen Zustand befinden:

```
metrocluster vserver show
```

Erweitern Sie eine MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes

Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes

Um eine MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes zu erweitern, müssen jedem Cluster zwei Controller hinzugefügt werden. So bilden sie an jedem MetroCluster Standort ein zweites HA-Paar, und anschließend werden der MetroCluster FC-Konfigurationsvorgang ausgeführt.

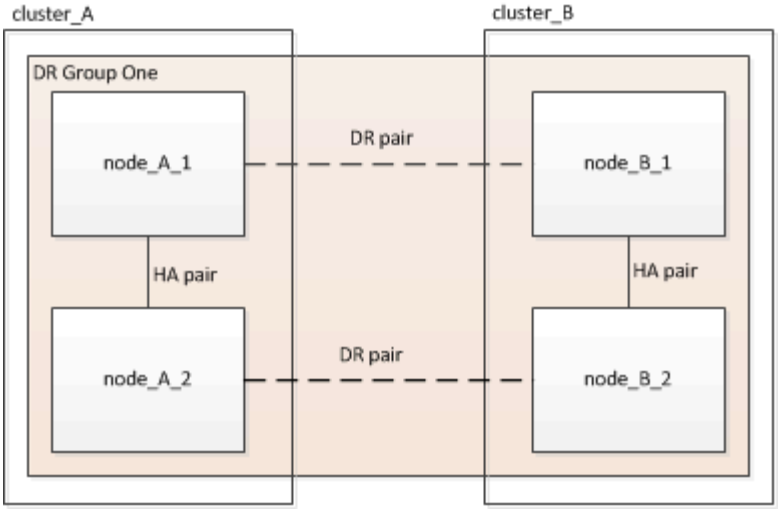
Über diese Aufgabe

- Die Knoten müssen ONTAP 9 in einer MetroCluster FC-Konfiguration ausführen.

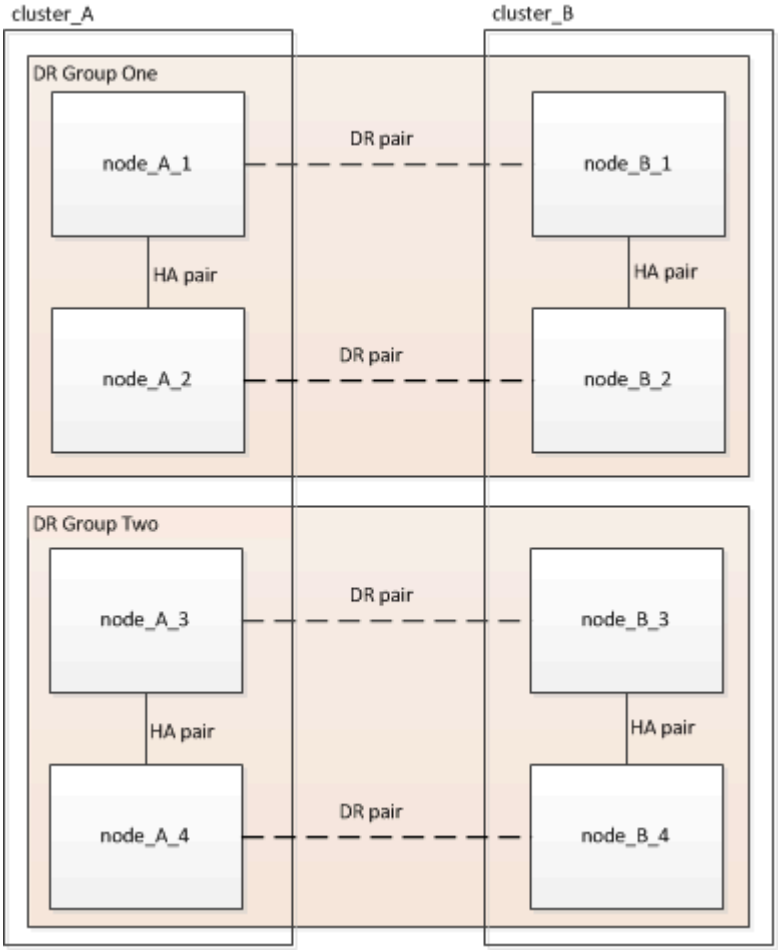
  Frühere Versionen von ONTAP oder MetroCluster IP-Konfigurationen unterstützen dieses Verfahren nicht.

- Die vorhandene MetroCluster FC-Konfiguration muss sich in einem ordnungsgemäßen Zustand befindet.
- Die Geräte, die Sie hinzufügen, müssen unterstützt werden und alle in beschriebenen Anforderungen erfüllen "Installation und Konfiguration von Fabric-Attached MetroCluster"
- Sie benötigen verfügbare FC-Switch-Ports, um die neuen Controller und neue Bridges aufnehmen zu können.
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.
- Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen.
- Diese Vorgehensweise verursacht keine Unterbrechungen und dauert etwa einen Tag (ausgenommen Rack und Stack), wenn Festplatten gelöscht werden.

Bevor Sie dieses Verfahren durchführen, besteht die MetroCluster FC-Konfiguration aus vier Nodes mit einem HA-Paar an jedem Standort:



Nach Abschluss dieses Verfahrens besteht die MetroCluster FC-Konfiguration aus zwei HA-Paaren an jedem Standort:



Beide Standorte müssen gleichermaßen erweitert werden. Eine MetroCluster FC-Konfiguration darf nicht aus einer ungleichmäßigen Anzahl von Nodes bestehen.

Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe

In der folgenden Tabelle werden die unterstützten Plattformkombinationen für MetroCluster FC-Konfigurationen mit acht Nodes aufgeführt.

- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen.
- Die Kombinationen in dieser Tabelle gelten nur für normale oder permanente Konfigurationen mit acht Nodes.
- Die Plattformkombinationen in dieser Tabelle **nicht** gelten, wenn Sie die Umstiegs- oder Aktualisierungsverfahren verwenden.
- Alle Nodes in einer DR-Gruppe müssen vom gleichen Typ und von derselben Konfiguration sein.

		8Node DrGroup 2									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
8Node DrGroup 1	FAS8200										
	AFF A300										
	FAS8300										
	AFF A400										
	ASA A400										
	FAS9000										
	AFF A700										
	FAS9500										
	AFF A900										
	ASA A900										

Bestimmen des neuen Verkabelungslayouts

Sie müssen die Verkabelung der neuen Controller-Module und aller neuen Platten-Shelfs zu den vorhandenen FC-Switches bestimmen.

Über diese Aufgabe

Diese Aufgabe muss an jedem MetroCluster Standort ausgeführt werden.

Schritte

1. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um ein Verkabelungslayout für Ihren Switch-Typ zu erstellen, verwenden Sie die Portnutzung für eine MetroCluster-Konfiguration mit acht Nodes.

   Die Verwendung des FC-Switch-Ports muss mit der in dem Verfahren beschriebenen Verwendung übereinstimmen, sodass die RCFs (Reference Configuration Files) verwendet werden können.

   Wenn Ihre Umgebung nicht so verkabelt werden kann, dass RCF-Dateien verwendet werden können, müssen Sie das System manuell gemäß den Anweisungen in konfigurieren "Installation und Konfiguration von Fabric-Attached MetroCluster". Verwenden Sie dieses Verfahren nicht, wenn die Verkabelung keine RCF-Dateien verwenden kann.

Die neue Ausrüstung in den Racks zu bringen

Sie müssen die Geräte für die neuen Nodes im Rack unterbringen.

Schritte

1. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um neue Storage-Systeme, Platten-Shelfs und FC-to-SAS-Bridges Rack zu bilden.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie sollten den Systemzustand der MetroCluster-Konfiguration überprüfen, um einen ordnungsgemäßen Betrieb zu gewährleisten.

Schritte

1. 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
   ```

2. 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.
   ```

3. 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.
```

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

   `system health alert show`

5. Simulation eines Switchover-Vorgangs:
   a. Ändern Sie in der Eingabeaufforderung eines beliebigen Nodes die erweiterte Berechtigungsebene: `set -privilege advanced`

      Sie müssen mit reagieren **`y`** Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*>) anzuzeigen.

   b. Führen Sie den Umschaltvorgang mit dem Parameter -Simulate: + aus `metrocluster switchover -simulate`
   c. Zurück zur Administrator-Berechtigungsebene: `set -privilege admin`

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor

Sie können die NetApp Support-Website besuchen und das Config Advisor-Tool herunterladen, um häufige Konfigurationsfehler zu überprüfen.

Über diese Aufgabe

Config Advisor ist ein Tool zur Konfigurationsvalidierung und Statusüberprüfung. Sie können die Lösung sowohl an sicheren Standorten als auch an nicht sicheren Standorten zur Datenerfassung und Systemanalyse einsetzen.

> Der Support für Config Advisor ist begrenzt und steht nur online zur Verfügung.

Schritte

1. Rufen Sie die Config Advisor Download-Seite auf und laden Sie das Tool herunter.

   "NetApp Downloads: Config Advisor"

2. Führen Sie Config Advisor aus, überprüfen Sie die Ausgabe des Tools und folgen Sie den Empfehlungen in der Ausgabe, um erkannte Probleme zu beheben.

Senden einer benutzerdefinierten AutoSupport Meldung vor dem Hinzufügen von Nodes zur MetroCluster Konfiguration

Sie sollten 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 Site_A beim 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` Der Parameter gibt die Länge des Wartungsfensters an und kann maximal 72 Stunden betragen. Wenn die Wartung vor Ablauf der Zeit abgeschlossen ist, können Sie den folgenden Befehl eingeben, um anzugeben, dass der Wartungszeitraum beendet ist:

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

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Reverkable und Zone A Switch Fabric für die neuen Nodes

Bestehende DR-Gruppe von der Fabric trennen

Sie müssen die vorhandenen Controller-Module von den FC-Switches in der Fabric trennen.

Über diese Aufgabe

Diese Aufgabe muss an jedem MetroCluster Standort ausgeführt werden.

Schritte

1. Deaktivieren Sie die HBA-Ports, die die vorhandenen Controller-Module mit der zu Wartungszwecken laufenden Switch-Fabric verbinden:

   ```
   storage port disable -node node-name -port port-number
   ```

2. Entfernen Sie bei den lokalen FC-Switches die Kabel von den Ports für die HBA-, FC-VI- und ATTO-Brücken des vorhandenen Controller-Moduls.

Sie sollten die Kabel so kennzeichnen, dass sie sich leicht identifizieren lassen, wenn Sie sie erneut verkabeln. Nur die ISL-Ports sollten verkabelt bleiben.

Die Switches können neu konfiguriert und neu konfiguriert werden

Sie müssen die RCF-Dateien anwenden, um das Zoning neu zu konfigurieren, um die neuen Nodes aufzunehmen.

Wenn Sie die RCF-Dateien nicht zur Konfiguration der Switches verwenden können, müssen Sie die Switches manuell konfigurieren. Siehe:

- "Konfigurieren Sie die Brocade FC-Switches manuell"
- "Konfigurieren Sie Cisco FC-Switches manuell"

Schritte

1. Suchen Sie die RCF-Dateien für Ihre Konfiguration.

   Sie müssen die RCF-Dateien für eine Konfiguration mit acht Nodes verwenden, die Ihrem Switch-Modell entspricht.

2. Wenden Sie die RCF-Dateien an, indem Sie den Anweisungen auf der Download-Seite folgen und die ISL-Einstellungen nach Bedarf anpassen.
3. Stellen Sie sicher, dass die Switch-Konfiguration gespeichert ist.
4. Starten Sie die FC-Switches neu.
5. Verkabelung der vorhandenen und der neuen FC-to-SAS-Bridges zu den FC-Switches, wobei Sie das zuvor erstellte Verkabelungslayout verwenden.

   Die Verwendung von FC-Switch-Ports muss mit der in beschriebenen Verwendung von acht MetroCluster-Nodes übereinstimmen "Installation und Konfiguration von Fabric-Attached MetroCluster" Damit die Referenzkonfigurationsdateien (RCfs) verwendet werden können.

6. Überprüfen Sie, ob die Ports online sind, indem Sie den korrekten Befehl für Ihren Switch verwenden.

Switch-Anbieter	Befehl
Brocade	switchshow
Cisco	Schnittstellenübersicht anzeigen

7. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um die FC-VI-Ports mithilfe des zuvor erstellten Verkabelungslayouts von den vorhandenen und neuen Controllern zu verkabeln.

   Die Verwendung von FC-Switch-Ports muss mit der in beschriebenen Verwendung von acht MetroCluster-Nodes übereinstimmen "Installation und Konfiguration von Fabric-Attached MetroCluster" Damit die Referenzkonfigurationsdateien (RCfs) verwendet werden können.

8. Vergewissern Sie sich von den vorhandenen Nodes, dass die FC-VI-Ports online sind:

   ```
   metrocluster interconnect adapter show
   ```

```
metrocluster interconnect mirror show
```

9. Verkabeln Sie die HBA-Ports der aktuellen und der neuen Controller.
10. Aktivieren Sie bei den vorhandenen Controller-Modulen die Ports, die im Rahmen der Wartung an die Switch-Fabric angeschlossen sind:

    ```
    storage port enable -node node-name -port port-ID
    ```

11. Starten Sie die neuen Controller, und starten Sie sie in den Wartungsmodus:

    ```
    boot_ontap maint
    ```

12. Vergewissern Sie sich, dass nur Storage sichtbar ist, der von der neuen DR-Gruppe verwendet wird.

    Keiner der Storage, der von der anderen DR-Gruppe verwendet wird, sollte sichtbar sein.

13. Kehren Sie zu Beginn dieses Prozesses zurück, um die zweite Switch-Fabric wieder zu verkabeln.

Konfigurieren Sie ONTAP auf den neuen Controllern

Löschen der 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 gegebenenfalls den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

    ```
    halt
    ```

2. Legen Sie an der Loader-Eingabeaufforderung die Umgebungsvariablen auf Standardwerte fest:

    ```
    set-defaults
    ```

3. Umgebung speichern:

    ```
    saveenv
    ```

4. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

    ```
    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.

Zuweisung der Festplatteneigentümer für AFF Systeme

Wenn Sie in einer Konfiguration mit AFF Systemen und gespiegelten Aggregaten einsetzen und die Nodes die Festplatten (SSDs) nicht korrekt zugewiesen sind, sollten Sie den HA-Partner-Node jeweils halb so viele Festplatten an jedem Shelf einem lokalen Node und der anderen Hälfte der Festplatten zuweisen. Sie sollten eine Konfiguration erstellen, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Über diese Aufgabe

Die Storage Controller müssen sich im Wartungsmodus befinden.

Dies gilt nicht für Konfigurationen mit nicht gespiegelten Aggregaten, einer aktiv/Passiv-Konfiguration oder einer ungleichen Anzahl von Festplatten in lokalen und Remote-Pools.

Dieser Task ist nicht erforderlich, wenn Festplatten beim Empfang vom Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören, während Pool 1 immer die Festplatten enthält, die sich dem Speichersystem, dem sie gehören, fernhalten.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Festplatten den Nodes des ersten Standorts (Standort A) zu:

   Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

   a. Weisen Sie beim ersten Knoten systematisch die Hälfte der Disks jedem Shelf zu, um 0 und die andere Hälfte dem Pool des HA-Partners 0: + zuzuweisen `disk assign -disk disk-name -p pool -n number-of-disks`

      Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
      ```

   b. Wiederholen Sie den Vorgang für den zweiten Knoten am lokalen Standort, indem Sie in jedem Shelf systematisch die Hälfte der Festplatten dem Pool 1 und der anderen Hälfte dem Pool des HA-Partners 1: + zuweisen `disk assign -disk disk-name -p pool`

      Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Weisen Sie die Festplatten den Nodes des zweiten Standorts (Standort B) zu:

   Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

   a. Weisen Sie auf dem ersten Knoten am Remote-Standort systematisch die Hälfte der Festplatten auf jedem Shelf zu Pool 0 und die andere Hälfte dem Pool des HA-Partners 0: + zu `disk assign -disk disk-name -p pool`

      Wenn der Storage Controller Controller_B_1 vier Shelves mit jeweils 8 SSDs hat, geben Sie die folgenden Befehle ein:

      ```
      *> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
      *> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

      *> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
      *> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
      ```

   b. Wiederholen Sie diesen Vorgang für den zweiten Node am Remote-Standort, indem Sie in jedem Shelf systematisch die Hälfte der Festplatten dem Pool 1 und der anderen Hälfte dem Pool des HA-Partners 1 zuweisen:

      `disk assign -disk disk-name -p pool`

      Wenn der Storage Controller Controller_B_2 vier Shelfs mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Bestätigen Sie die Festplattenzuordnungen:

   `storage show disk`

5. Beenden des Wartungsmodus:

   `halt`

6. Anzeigen des Startmenüs:

```
boot_ontap menu
```

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

Zuweisung der Festplatteneigentümer in anderen Systemen außerhalb von All Flash FAS

Wenn auf den MetroCluster Nodes die Festplatten nicht korrekt zugewiesen sind oder wenn Sie in Ihrer Konfiguration DS460C Platten-Shelfs verwenden, müssen Sie jedem der Nodes der MetroCluster Konfiguration Shelf-einzeln Festplatten zuweisen. Sie erstellen eine Konfiguration, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Über diese Aufgabe

Die Storage Controller müssen sich im Wartungsmodus befinden.

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs nicht umfasst, ist diese Aufgabe nicht erforderlich, wenn die Festplatten bereits im Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören.
>
> Pool 1 enthält immer die Festplatten, die sich dem Speichersystem, zu dem sie gehören, fernhalten.

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs umfasst, sollten Sie die Festplatten anhand der folgenden Richtlinien für jedes Laufwerk mit 12 Festplatten manuell zuweisen:

Diese Festplatten in der Schublade zuweisen…	Zu diesem Knoten und Pool…
0-2	Pool des lokalen Node 0
3 - 5	Pool 0 des HA-Partner-Node
6 - 8	DR-Partner des lokalen Knotens Pool 1
9 - 11	DR-Partner des HA-Partners Pool 1

Mit diesem Zuweisungsmuster wird sichergestellt, dass ein Aggregat minimal beeinträchtigt wird, wenn ein Einschub offline geht.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Platten-Shelfs den Nodes des ersten Standorts (Standort A) zu:

   Festplatten-Shelfs an demselben Standort wie der Node werden Pool 0 zugewiesen, und Festplatten-Shelfs, die sich am Standort des Partners befinden, werden Pool 1 zugewiesen.

   Sie sollten jedem Pool die gleiche Anzahl von Shelfs zuweisen.

   a. Weisen Sie beim ersten Knoten systematisch die lokalen Festplatten-Shelfs dem Pool 0 und den

Remote-Festplatten-Shelfs zu, und Pool 1:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

Wenn der Storage Controller Controller_A_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

b. Wiederholen Sie den Vorgang für den zweiten Node am lokalen Standort, indem Sie den Pool 0 und die Remote-Festplatten-Shelfs systematisch den Pool 1 zuweisen:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

Wenn der Storage Controller Controller_A_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Weisen Sie die Platten-Shelfs den Nodes am zweiten Standort (Standort B) zu:

Festplatten-Shelfs an demselben Standort wie der Node werden Pool 0 zugewiesen, und Festplatten-Shelfs, die sich am Standort des Partners befinden, werden Pool 1 zugewiesen.

Sie sollten jedem Pool die gleiche Anzahl von Shelfs zuweisen.

a. Weisen Sie beim ersten Knoten am Remote-Standort systematisch seine lokalen Festplatten-Shelfs dem Pool 0 und seinen Remote-Festplatten-Shelfs zu 1:

```
disk assign -shelf local-switch-nameshelf-name -p pool
```

Wenn der Storage Controller_B_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. Wiederholen Sie den Vorgang für den zweiten Node am Remote-Standort, indem Sie seine lokalen Festplatten-Shelfs systematisch dem Pool 0 und den Remote-Festplatten-Shelfs Pool 1 zuordnen:

```
disk assign -shelf shelf-name -p pool
```

Wenn der Storage Controller_B_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Bestätigen Sie die Shelf-Zuweisungen:

   ```
   storage show shelf
   ```

5. Beenden des Wartungsmodus:

   ```
   halt
   ```

6. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

Überprüfen des HA-Konfigurationsstatus von Komponenten

In einer MetroCluster-Konfiguration muss der HA-Konfigurationszustand des Controller-Moduls und der Gehäusekomponenten auf **mcc** eingestellt sein, damit sie ordnungsgemäß hochfahren.

Über diese Aufgabe

- Das System muss sich im Wartungsmodus befinden.
- Diese Aufgabe muss an jedem neuen Controller-Modul ausgeführt werden.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte „mcc“ sein.

2. Wenn der angezeigte Systemzustand des Controllers nicht korrekt ist, setzen Sie den HA-Status für das Controller-Modul ein:

   ```
   ha-config modify controller mcc
   ```

3. Wenn der angezeigte Systemzustand des Chassis nicht korrekt ist, setzen Sie den HA-Status für das Chassis ein:

   ```
   ha-config modify chassis mcc
   ```

4. Wiederholen Sie diese Schritte auf dem anderen Ersatzknoten.

Booten der neuen Controller und Verbinden der Controller mit dem Cluster

Damit Sie die neuen Controller dem Cluster beitreten können, müssen Sie jedes neue Controller-Modul booten und den ONTAP Cluster Setup-Assistenten verwenden, um zu ermitteln, dass der Cluster Beitritt.

Bevor Sie beginnen

Sie müssen die MetroCluster-Konfiguration verkabelt haben.

Sie müssen den Service-Prozessor nicht konfiguriert haben, bevor Sie diese Aufgabe ausführen.

Über diese Aufgabe

Diese Aufgabe muss für jeden der neuen Controller bei beiden Clustern in der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Falls noch nicht geschehen, schalten Sie jeden Knoten ein und lassen Sie ihn vollständig booten.

   Wenn sich das System im Wartungsmodus befindet, geben Sie den aus `halt` Befehl zum Beenden des Wartungsmodus und geben Sie dann den folgenden Befehl von der LOADER-Eingabeaufforderung aus:

   ```
   boot_ontap
   ```

   Das Controller-Modul wechselt in den Node-Setup-Assistenten.

   Die Ausgabe sollte wie folgt aussehen:

   ```
   Welcome to node setup

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
                  Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.
   .
   .
   .
   ```

2. Aktivieren Sie das AutoSupport-Tool, indem Sie den vom System bereitgestellten Anweisungen folgen.
3. Befolgen Sie die Aufforderungen zur Konfiguration der Node-Managementoberfläche.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Sicherstellen, dass die Nodes im Hochverfügbarkeits-Modus konfiguriert sind:

   `storage failover show -fields mode`

   Wenn dies nicht der Fall ist, müssen Sie für jeden Node den folgenden Befehl eingeben und dann den Node neu booten:

   `storage failover modify -mode ha -node localhost`

   Dieser Befehl konfiguriert den Hochverfügbarkeits-Modus, ermöglicht jedoch kein Storage Failover. Storage-Failover wird automatisch aktiviert, wenn Sie das ausgeben `metrocluster configure` Befehl später im Konfigurationsprozess.

5. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

   `network port show`

   Im folgenden Beispiel wird die Ausgabe für zwei Controller in „Cluster_A“ angezeigt Wenn es sich um eine MetroCluster-Konfiguration mit zwei Nodes handelt, wird in der Ausgabe nur ein Node angezeigt.

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Da Sie das Cluster mit der CLI einrichten, beenden Sie den Node Setup-Assistenten:

   `exit`

7. Loggen Sie sich mit dem beim Administratorkonto ein `admin` Benutzername:
8. Starten Sie den Cluster Setup-Assistenten und fügen Sie ihn dem vorhandenen Cluster hinzu:

   `cluster setup`

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`
```

9. Nachdem Sie den **Cluster Setup**-Assistenten abgeschlossen und beendet haben, überprüfen Sie, ob der Cluster aktiv ist und der Knoten ordnungsgemäß ist:

   `cluster show`

   Das folgende Beispiel zeigt ein Cluster, in dem der erste Node (cluster1-01) sich in einem ordnungsgemäßen Zustand befindet und zur Teilnahme berechtigt ist:

```
cluster_A::> cluster show
Node                Health  Eligibility
------------------ ------- ------------
node_A_1            true    true
node_A_2            true    true
node_A_3            true    true
```

   Wenn eine der Einstellungen, die Sie für die Admin-SVM oder Node-SVM eingegeben haben, geändert werden muss, können Sie über den auf den Assistenten * Cluster Setup* zugreifen `cluster setup command`.

Konfigurieren Sie die Cluster in einer MetroCluster-Konfiguration

Konfigurieren Sie Intercluster LIFs

Konfigurieren von Intercluster-LIFs auf dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

   ```
   cluster01::> network port show
                                                                    Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   ```
   network interface show -fields home-port,curr-port
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Das folgende Beispiel weist den Failover-Gruppe „intercluster01“ auf der System-SVM „cluster01“ die Ports „e0e“ und „e0f“ zu:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   `network interface failover-groups show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

ONTAP-Version	Befehl
9.6 und höher	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 und früher	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic02“ in der Failover-Gruppe „intercluster01“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem SVM „e0e“-Port an den „e0f“-Port scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                            Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

Im ONTAP 9.6 und höher:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 und früher:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern wird.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Spiegelung der Root-Aggregate

Um Datensicherung zu ermöglichen, müssen Sie die Root-Aggregate spiegeln.

Standardmäßig wird das Root-Aggregat als RAID-DP Typ Aggregat erstellt. Sie können das Root-Aggregat von RAID-DP zu einem Aggregat des RAID4-Typs ändern. Mit dem folgenden Befehl wird das Root-Aggregat für das RAID4-Typ-Aggregat modifiziert:

```
storage aggregate modify –aggregate aggr_name -raidtype raid4
```

> Auf Systemen anderer Hersteller kann der RAID-Typ des Aggregats von dem Standard RAID-DP zu RAID4 vor oder nach der Spiegelung des Aggregats geändert werden.

Schritte

1. Root-Aggregat spiegeln:

   `storage aggregate mirror` *`aggr_name`*

   Der folgende Befehl spiegelt das Root-Aggregat für Controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

2. Wiederholen Sie den vorherigen Schritt für jeden Node in der MetroCluster-Konfiguration.

Implementieren der MetroCluster-Konfiguration

Sie müssen den ausführen `metrocluster configure -refresh true` Befehl zum

Starten der Datensicherung auf den Nodes, die Sie einer MetroCluster-Konfiguration hinzugefügt haben.

Über diese Aufgabe

Sie stellen das aus `metrocluster configure -refresh true` Befehl einmal auf einem der neu hinzugefügten Nodes, um die MetroCluster-Konfiguration zu aktualisieren. Sie müssen den Befehl nicht an jedem Standort bzw. jeder Node ausgeben.

Der `metrocluster configure -refresh true` Befehl koppelt die beiden Nodes automatisch mit den niedrigsten System-IDs in jedem der beiden Cluster als Disaster Recovery (DR) Partner. In einer MetroCluster Konfiguration mit vier Nodes gibt es zwei DR-Partnerpaare. Das zweite DR-Paar wird aus den beiden Knoten mit höheren System-IDs erstellt.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Wechseln Sie in den erweiterten Berechtigungsmodus:

      ```
      set -privilege advanced
      ```

   b. Aktualisieren Sie die MetroCluster Konfiguration auf einem der neuen Nodes:
      `metrocluster configure -refresh true`

      Im folgenden Beispiel wird die auf beiden DR-Gruppen aktualisierte MetroCluster Konfiguration angezeigt:

```
controller_A_2::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

+

```
controller_A_4::*> metrocluster configure -refresh true

[Job 740] Job succeeded: Configure is successful.
```

   a. Zurück zum Admin-Berechtigungsmodus:

      ```
      set -privilege admin
      ```

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

   ```
   network port show
   ```

   Im folgenden Beispiel wird die Verwendung von Netzwerkports in einer MetroCluster Konfiguration mit vier Nodes angezeigt:

```
cluster_A::> network port show
                                                            Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration:

   a. Überprüfen Sie die Konfiguration von Standort A:

      `metrocluster show`

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

   a. Überprüfen Sie die Konfiguration von Standort B:
      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

  In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

> Es wird empfohlen, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   `storage disk show -spare -owner` *`node_name`*

2. Erstellen Sie das Aggregat:

```
storage aggregate create -mirror true
```

Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um sicherzustellen, dass das Aggregat auf einem bestimmten Node erstellt wird, verwenden Sie die `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

Sie können die folgenden Optionen angeben:

- Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
- Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
- Anzahl der zu einführenden Laufwerke

> In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

- Prüfsummenstil, den Sie für das Aggregat verwenden möchten
- Typ der zu verwendenden Laufwerke
- Die Größe der zu verwendenden Laufwerke
- Fahrgeschwindigkeit zu verwenden
- RAID-Typ für RAID-Gruppen auf dem Aggregat
- Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
- Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

  Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

  Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

```
storage aggregate show-status -aggregate aggregate-name
```

Konfiguration von FC-to-SAS-Bridges für das Monitoring des Systemzustands

Über diese Aufgabe

- SNMP-Überwachungstools anderer Anbieter werden für FibreBridge-Brücken nicht unterstützt.
- Ab ONTAP 9.8 werden FC-to-SAS-Bridges standardmäßig über in-Band-Verbindungen überwacht, keine zusätzliche Konfiguration erforderlich.

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

Schritt

1. Fügen Sie von der ONTAP Cluster-Eingabeaufforderung die Bridge zur Statusüberwachung hinzu:

   a. Fügen Sie die Bridge mit dem Befehl für Ihre ONTAP-Version hinzu:

ONTAP-Version	Befehl
9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 und früher	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   b. Überprüfen Sie, ob die Bridge hinzugefügt und richtig konfiguriert wurde:

   ```
   storage bridge show
   ```

   Es kann bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „Status“ „ok“ lautet und weitere Informationen, z. B. der weltweite Name (WWN), angezeigt werden.

   Das folgende Beispiel zeigt, dass die FC-to-SAS-Bridges konfiguriert sind:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen

Sie können ein Metadaten-Volume in eine MetroCluster Konfiguration von einem Aggregat zu einem anderen Aggregat verschieben. Unter Umständen möchten Sie ein Metadaten-Volume verschieben, wenn das Quellaggregat deaktiviert oder nicht gespiegelt wird, oder aus anderen Gründen, aus denen das Aggregat nicht mehr berechtigt ist.

Über diese Aufgabe

- Um diese Aufgabe ausführen zu können, müssen Sie über Cluster-Administratorrechte verfügen.
- Das Zielaggregat muss gespiegelt werden und darf nicht im eingeschränkten Zustand sein.
- Der verfügbare Speicherplatz im Zielaggregat muss größer sein als das zu bewegende Metadaten-Volume.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Identifizierung des zu verschiebenden Metadaten-Volumes:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Ermittlung eines geeigneten Zielaggregats:

   `metrocluster check config-replication show-aggregate-eligibility`

   Mit dem folgenden Befehl werden die Aggregate in „Cluster_A“ identifiziert, die zum Hosten von Metadaten-Volumes geeignet sind:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

In dem vorherigen Beispiel können Node_A_1_aggr2 und Node_A_2_aggr2 ausgewählt werden.

4. Starten Sie die Volume-Verschiebung:

   `volume move start -vserver` *`svm_name`* `-volume` *`metadata_volume_name`* `-destination -aggregate` *`destination_aggregate_name`*`*`

   Der folgende Befehl verschiebt Metadaten-Volume „MDV_CRS_14c00d4ac9f311e7922800a0984395f1“ von „Aggregate Node_A_1_aggr1“ in „Aggregate Node_A_1_aggr2“:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Überprüfung des Status der Verschiebung eines Volumes:

   ```
   volume move show -volume vol_constituent_name
   ```

6. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Überprüfen der MetroCluster-Konfiguration

Sie können überprüfen, ob die Komponenten und Beziehungen in der MetroCluster Konfiguration ordnungsgemäß funktionieren. Nach der Erstkonfiguration und nach sämtlichen Änderungen an der MetroCluster-Konfiguration sollten Sie einen Check durchführen. Sie sollten auch vor einer ausgehandelten (geplanten) Umschaltung oder einem Switchback prüfen.

Über diese Aufgabe

Wenn der `metrocluster check run` Befehl wird zweimal innerhalb kürzester Zeit auf einem oder beiden Clustern ausgegeben. Ein Konflikt kann auftreten, und der Befehl erfasst möglicherweise nicht alle Daten. Danach `metrocluster check show` Befehle zeigen nicht die erwartete Ausgabe an.

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

   Der Befehl wird als Hintergrundjob ausgeführt und wird möglicherweise nicht sofort ausgeführt.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Zeigen Sie detailliertere Ergebnisse der letzten Zeit an `metrocluster check run` Befehl:

   ```
   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

   Der `metrocluster check show` Befehle zeigen die Ergebnisse der letzten `metrocluster check run` Befehl. Sie sollten immer den ausführen `metrocluster check run` Befehl vor Verwendung des `metrocluster check show` Befehle, sodass die angezeigten Informationen aktuell sind.

   Das folgende Beispiel zeigt die `metrocluster check aggregate show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
```

```
                      controller_A_1_aggr1
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_1_aggr2
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_2_aggr1
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_2_aggr2
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok

18 entries were displayed.
```

Das folgende Beispiel zeigt die `metrocluster check cluster show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes. Sie zeigt an, dass die Cluster bei Bedarf bereit sind, eine ausgehandelte Umschaltung durchzuführen.

```
Last Checked On: 9/13/2017 20:47:04

Cluster                 Check                            Result
--------------------- -------------------------------- ---------
mccint-fas9000-0102
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
mccint-fas9000-0304
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
10 entries were displayed.
```

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor

Sie können die NetApp Support-Website besuchen und das Config Advisor-Tool herunterladen, um häufige Konfigurationsfehler zu überprüfen.

Über diese Aufgabe

Config Advisor ist ein Tool zur Konfigurationsvalidierung und Statusüberprüfung. Sie können die Lösung sowohl an sicheren Standorten als auch an nicht sicheren Standorten zur Datenerfassung und Systemanalyse einsetzen.

> Der Support für Config Advisor ist begrenzt und steht nur online zur Verfügung.

Schritte

1. Rufen Sie die Config Advisor Download-Seite auf und laden Sie das Tool herunter.

   "NetApp Downloads: Config Advisor"

2. Führen Sie Config Advisor aus, überprüfen Sie die Ausgabe des Tools und folgen Sie den Empfehlungen in der Ausgabe, um erkannte Probleme zu beheben.

Senden einer benutzerdefinierten AutoSupport Meldung nach dem Hinzufügen von Nodes zur MetroCluster Konfiguration

Sie sollten eine Meldung von AutoSupport senden, um den technischen Support von NetApp über die Wartung zu informieren.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei Site_A beim Cluster an
2. Rufen Sie eine AutoSupport-Meldung auf, die das Ende der Wartung angibt:

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

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Überprüfung von Umschaltung, Reparatur und Wechsel zurück

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

Schritte

1. Verwenden Sie die Verfahren für die ausgehandelte Umschaltung, Heilung und zurückwechseln "MetroCluster Management und Disaster Recovery".

Erweitern einer MetroCluster IP-Konfiguration

Je nach ONTAP Version können Sie Ihre MetroCluster IP-Konfiguration erweitern, indem Sie vier neue Nodes als neue DR-Gruppe hinzufügen.

Ab ONTAP 9.13.1 können Sie eine MetroCluster Konfiguration mit acht Nodes vorübergehend erweitern, um die Controller und Storage zu aktualisieren. Siehe "Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher)" Finden Sie weitere Informationen.

Ab ONTAP 9.9 können Sie der MetroCluster IP-Konfiguration vier neue Nodes als zweite DR-Gruppe hinzufügen. Dadurch wird eine MetroCluster-Konfiguration mit acht Nodes erstellt.

Bevor Sie beginnen

- Die alten und neuen Nodes müssen dieselbe Version von ONTAP ausführen.
- In diesem Verfahren werden die Schritte beschrieben, die erforderlich sind, um eine DR-Gruppe mit vier Nodes einer vorhandenen MetroCluster IP-Konfiguration hinzuzufügen. Wenn Sie eine Konfiguration mit acht Nodes aktualisieren, müssen Sie den gesamten Vorgang für jede DR-Gruppe wiederholen und nacheinander hinzufügen.
- Stellen Sie sicher, dass die alten und neuen Plattformmodelle für die gemeinsame Verwendung der Plattformen unterstützt werden.

  "NetApp Hardware Universe"

- Überprüfen Sie, ob die alten und die neuen Plattformmodelle von den IP-Switches unterstützt werden.

  "NetApp Hardware Universe"

- Wenn Sie es sind "Aktualisieren einer MetroCluster-IP-Konfiguration mit vier oder acht Nodes", Die neuen Knoten müssen über genügend Speicher verfügen, um die Daten der alten Knoten aufzunehmen, zusammen mit geeigneten Platten für Root-Aggregate und freie Platten.
- Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

  Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden,

sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

Beispiel für die Benennung in diesem Verfahren

Bei diesem Verfahren werden durchgängig Beispielnamen verwendet, um die involvierten DR-Gruppen, Nodes und Switches zu identifizieren.

DR-Gruppen	Cluster_A an Standort_A	Cluster_B an Standort_B
dr_Group_1-alt	• Node_A_1-alt • Node_A_2-alt	• Node_B_1-alt • Node_B_2-alt
dr_Group_2-neu	• Node_A_3-neu • Node_A_4-neu	• Node_B_3-neu • Node_B_4-neu

Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für IP-Konfigurationen mit acht Nodes aufgeführt.

- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen.
- Die Kombinationen in dieser Tabelle gelten nur für reguläre oder permanente Konfigurationen mit 8 Nodes.
- Die Plattformkombinationen in dieser Tabelle **nicht** gelten, wenn Sie die Umstiegs- oder Aktualisierungsverfahren verwenden.
- Alle Nodes in einer DR-Gruppe müssen vom gleichen Typ und von derselben Konfiguration sein.

		8Node DrGroup 2									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
8Node DrGroup 1	AFF A150 ASA A150	Note 2									
	FAS2750 AFF A220										
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250										
	FAS8200 AFF A300				Note 1						
	AFF A320					Note 1					
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										
	FAS8700										
	FAS9000 AFF A700								Note 1		
	AFF C800 ASA A800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

- **Hinweis 1**: Für diese Kombinationen ist ONTAP 9.9.1 oder höher (oder die minimale ONTAP-Version, die auf der Plattform unterstützt wird) erforderlich.
- **Hinweis 2**: Für diese Kombinationen ist ONTAP 9.13.1 oder höher (oder die minimale ONTAP-Version, die auf der Plattform unterstützt wird) erforderlich.

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
   Upgrading old-model to new-model"
   ```

   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
   ```

   ```
   cluster_A::> cluster show
   Node            Health  Eligibility
   --------------- ------  -----------
   node_A_1        true    true
   node_A_2        true    true

   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::>
```

Entfernen der Konfiguration aus Überwachungsanwendungen

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Software, dem ONTAP Mediator oder anderen Anwendungen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster-Konfiguration vor dem Upgrade von der Monitoring-Software entfernen.

Schritte

1. 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.

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Vorbereiten der neuen Controller-Module

Sie müssen die vier neuen MetroCluster-Knoten vorbereiten und die korrekte ONTAP-Version installieren.

Über diese Aufgabe

Diese Aufgabe muss auf jedem der neuen Knoten ausgeführt werden:

- Node_A_3-neu
- Node_A_4-neu
- Node_B_3-neu
- Node_B_4-neu

Löschen Sie in diesen Schritten die Konfiguration auf den Knoten und löschen Sie den Mailbox-Bereich auf neuen Laufwerken.

Schritte

1. Für die neuen Controller
2. Schließen Sie die neuen MetroCluster IP-Knoten wie in der Installation und Konfiguration *MetroCluster gezeigt an die IP-Switches an.*

   "Verkabeln der IP-Switches"

3. Konfigurieren Sie die MetroCluster IP-Knoten mithilfe der folgenden Abschnitte der Installation und Konfiguration *MetroCluster.*
   a. "Sammeln der erforderlichen Informationen"
   b. "Systemeinstellungen auf einem Controller-Modul werden wiederhergestellt"
   c. "Überprüfen des HA-Konfigurationsstatus von Komponenten"
   d. "Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.4 und höher)"
4. Geben Sie im Wartungsmodus den Befehl stop ein, um den Wartungsmodus zu beenden, und geben Sie dann den Boot_ontap-Befehl aus, um das System zu booten und zum Cluster-Setup zu gelangen.

   Schließen Sie derzeit den Cluster-Assistenten oder den Node-Assistenten nicht ab.

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.

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          warning
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:

- "Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen"
- "Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen"

3. Laden Sie je nach Switch-Anbieter die IP RCF-Datei herunter, und installieren Sie sie.

> Aktualisieren Sie die Schalter in folgender Reihenfolge: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

- "Herunterladen und Installieren der Broadcom IP RCF-Dateien"
- "Herunterladen und Installieren der Cisco IP RCF-Dateien"

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.

Verbinden der neuen Nodes mit den Clustern

Sie müssen die vier neuen MetroCluster IP-Nodes der bestehenden MetroCluster-Konfiguration hinzufügen.

Über diese Aufgabe

Sie müssen diese Aufgabe für beide Cluster ausführen.

Schritte

1. Fügen Sie die neuen MetroCluster IP-Knoten zur bestehenden MetroCluster-Konfiguration hinzu.
   a. Fügen Sie den ersten neuen MetroCluster-IP-Knoten (Node_A_1-New) der bestehenden MetroCluster-IP-Konfiguration hinzu.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: 172.17.8.93
```

```
172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Fügen Sie den zweiten neuen MetroCluster-IP-Knoten (Node_A_2-New) der bestehenden MetroCluster-IP-Konfiguration hinzu.

2. Wiederholen Sie diese Schritte, um Node_B_1-New und Node_B_2-New zu Cluster_B. zu verbinden

Konfigurieren von Intercluster-LIFs, Erstellen der MetroCluster-Schnittstellen und Spiegeln von Root-Aggregaten

Sie müssen Cluster-Peering-LIFs erstellen, die MetroCluster-Schnittstellen auf den neuen MetroCluster IP-Nodes erstellen.

Über diese Aufgabe

Der in den Beispielen verwendete Home-Port ist plattformspezifisch. Sie sollten den entsprechenden Home Port für die MetroCluster IP-Node-Plattform verwenden.

Schritte

1. Konfigurieren Sie auf den neuen MetroCluster IP-Nodes die Intercluster-LIFs wie folgt:

   "Konfigurieren von Intercluster-LIFs auf dedizierten Ports"

   "Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports"

2. Vergewissern Sie sich an jedem Standort, dass Cluster-Peering konfiguriert ist:

   ```
   cluster peer show
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. Erstellen der DR-Gruppe für die MetroCluster IP-Knoten:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   Weitere Informationen zu den MetroCluster-Konfigurationseinstellungen und -Verbindungen finden Sie im Folgenden:

   "Überlegungen für MetroCluster IP-Konfigurationen"

"Erstellen der DR-Gruppe"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Vergewissern Sie sich, dass die DR-Gruppe erstellt wurde.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                     Node                DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                        node_A_1-old        node_B_1-old
                                        node_A_2-old        node_B_2-old
            cluster_B
                                        node_B_1-old        node_A_1-old
                                        node_B_2-old        node_A_2-old
2           cluster_A
                                        node_A_1-new        node_B_1-new
                                        node_A_2-new        node_B_2-new
            cluster_B
                                        node_B_1-new        node_A_1-new
                                        node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Konfigurieren Sie die MetroCluster IP-Schnittstellen für die neu verbundenen MetroCluster IP-Knoten:

   `metrocluster configuration-settings interface create -cluster-name`

- Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20. Sie können auch ein anderes (nicht standardmäßiges) VLAN angeben, das höher als 100 (zwischen 101 und 4095) ist `-vlan-id parameter` Im `metrocluster configuration-settings interface create` Befehl.
- Ab ONTAP 9.9 müssen Sie auch die angeben, wenn Sie eine Layer 3-Konfiguration verwenden `-gateway` Parameter beim Erstellen von MetroCluster-IP-Schnittstellen. Siehe "Überlegungen für Layer 3-Weitbereichs-Netzwerke".

Die folgenden Plattformmodelle können der vorhandenen MetroCluster Konfiguration hinzugefügt werden, wenn die verwendeten VLANs 10/20 oder mehr als 100 sind. Werden weitere VLANs verwendet, können diese Plattformen nicht zur vorhandenen Konfiguration hinzugefügt werden, da die MetroCluster Schnittstelle nicht konfiguriert werden kann. Wenn Sie eine andere Plattform verwenden, ist die VLAN-Konfiguration nicht relevant, da dies in ONTAP nicht erforderlich ist.

AFF Plattformen	FAS Plattformen
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

Sie können die MetroCluster-IP-Schnittstellen von beiden Clustern konfigurieren.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Überprüfen Sie, ob die MetroCluster-IP-Schnittstellen erstellt wurden:

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                 Home Port: e1a
                      172.17.28.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                 Home Port: e1a
                      172.17.28.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                 Home Port: e1a
                      172.17.28.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Verbinden Sie die MetroCluster IP-Schnittstellen:

   `metrocluster configuration-settings connection connect`

   Dieser Befehl kann einige Minuten dauern.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Überprüfen Sie, ob die Verbindungen ordnungsgemäß aufgebaut sind: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_1-new
                Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Überprüfen der automatischen Zuweisung und Partitionierung der Festplatte:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Root-Aggregate spiegeln:

```
storage aggregate mirror -aggregate aggr0_node_A_1-new
```

Diesen Schritt müssen Sie bei jedem MetroCluster IP Node abschließen.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Überprüfen Sie, ob die Root-Aggregate gespiegelt wurden:

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Beenden des Hinzufügung der neuen Nodes

Sie müssen die neue DR-Gruppe in die MetroCluster Konfiguration einbinden und gespiegelte Datenaggregate auf den neuen Nodes erstellen.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Wechseln Sie in den erweiterten Berechtigungsmodus:

      ```
      set -privilege advanced
      ```

   b. Aktualisieren Sie die MetroCluster-Konfiguration auf einem der neuen Nodes:

```
metrocluster configure
```

Im folgenden Beispiel wird die auf beiden DR-Gruppen aktualisierte MetroCluster Konfiguration angezeigt:

```
cluster_A::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

a. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

2. Erstellen von gespiegelten Datenaggregaten auf jedem der neuen MetroCluster Nodes:

```
storage aggregate create -aggregate aggregate-name -node node-name -diskcount
no-of-disks -mirror true
```

> Sie müssen mindestens ein gespiegeltes Datenaggregat pro Standort erstellen. Es wird empfohlen, zwei gespiegelte Datenaggregate pro Standort auf MetroCluster IP-Knoten zu haben, um die MDV-Volumes zu hosten. Allerdings wird ein einzelnes Aggregat pro Standort unterstützt (jedoch nicht empfohlen). Es wird unterstützt, dass ein Standort der MetroCluster ein einziges gespiegeltes Datenaggregat hat und der andere Standort mehr als ein gespiegeltes Datenaggregat hat.

Das folgende Beispiel zeigt die Erstellung eines Aggregats auf Node_A_1-New.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
```

```
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                              Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. Vergewissern Sie sich, dass die Nodes zu ihrer DR-Gruppe hinzugefügt werden.

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Verschieben Sie die MDV_CRS-Volumes von den alten Knoten auf die neuen Knoten in der erweiterten Berechtigung.

   a. Anzeigen der Volumes zur Identifizierung der MDV-Volumes:

   > Wenn Sie ein einzelnes gespiegeltes Datenaggregat pro Standort haben, dann verschieben Sie beide MDV-Volumen zu diesem einzigen Aggregat. Wenn Sie zwei oder mehr gespiegelte Datenaggregate haben, dann verschieben Sie jedes MDV-Volume zu einem anderen Aggregat.

   Das folgende Beispiel zeigt die MDV-Volumes im `volume show` Ausgabe:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Legen Sie die erweiterte Berechtigungsebene fest:

   `set -privilege advanced`

c. Verschieben Sie die MDV-Volumes nacheinander:

   `volume move start -volume` *`mdv-volume`* `-destination-aggregate` *`aggr-on-new-node`* `-vserver` *`vserver-name`*

   Das folgende Beispiel zeigt den Befehl und die Ausgabe für das Verschieben von "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A", um "Data_a3" auf "Node_A_3" zu aggregieren.

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Überprüfen Sie mit dem Befehl Volume show, ob das MDV-Volume erfolgreich verschoben wurde:

   `volume show mdv-name`

   Die folgende Ausgabe zeigt, dass das MDV-Volume erfolgreich verschoben wurde.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

5. Verschieben Sie Epsilon von einem alten Knoten auf einen neuen Knoten:

   a. Identifizieren Sie, welcher Knoten derzeit über Epsilon verfügt:

      `cluster show -fields epsilon`

```
cluster_B::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Stellen Sie das Epsilon auf „false“ auf dem alten Knoten (Node_A_1-old) ein:

   ```
   cluster modify -node old-node -epsilon false*
   ```

c. Setzen Sie das Epsilon auf „true“ (Node_A_3-New):

   ```
   cluster modify -node new-node -epsilon true
   ```

d. Vergewissern Sie sich, dass sich das Epsilon auf den richtigen Knoten bewegt hat:

   ```
   cluster show -fields epsilon
   ```

```
cluster_A::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

Entfernen einer Disaster Recovery-Gruppe

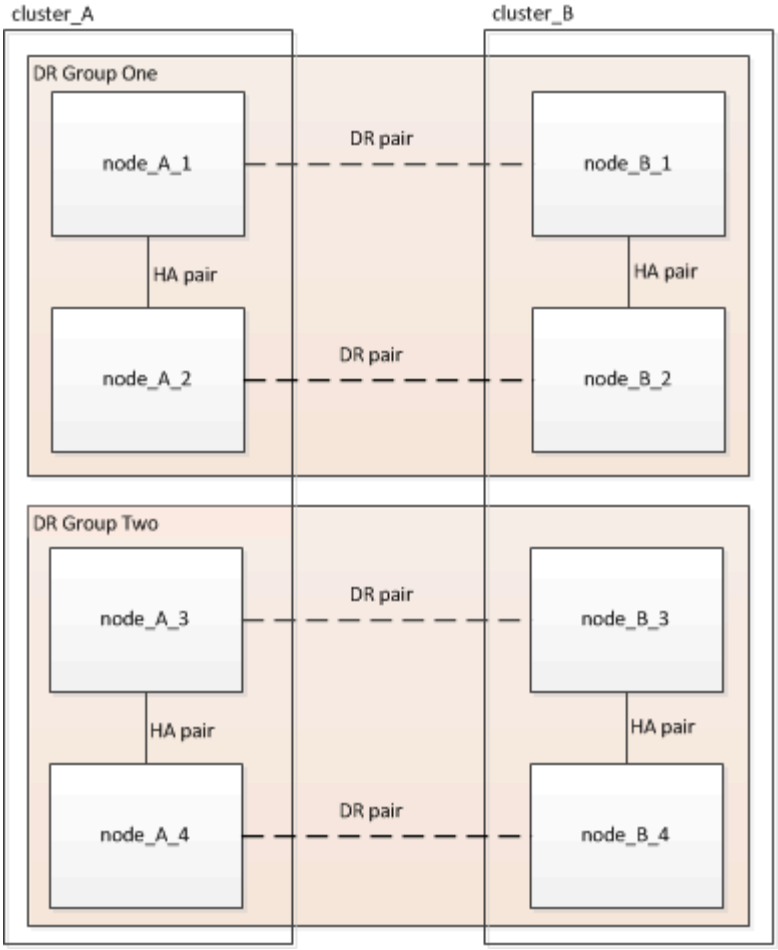
Ab ONTAP 9.8 können Sie eine DR-Gruppe aus einer MetroCluster Konfiguration mit acht Nodes entfernen, um eine MetroCluster Konfiguration mit vier Nodes zu erstellen.

Dieses Verfahren wird unter ONTAP 9.8 und höher unterstützt. Informationen zu Systemen mit ONTAP 9.7 oder einer älteren Version finden Sie im Knowledge Base-Artikel

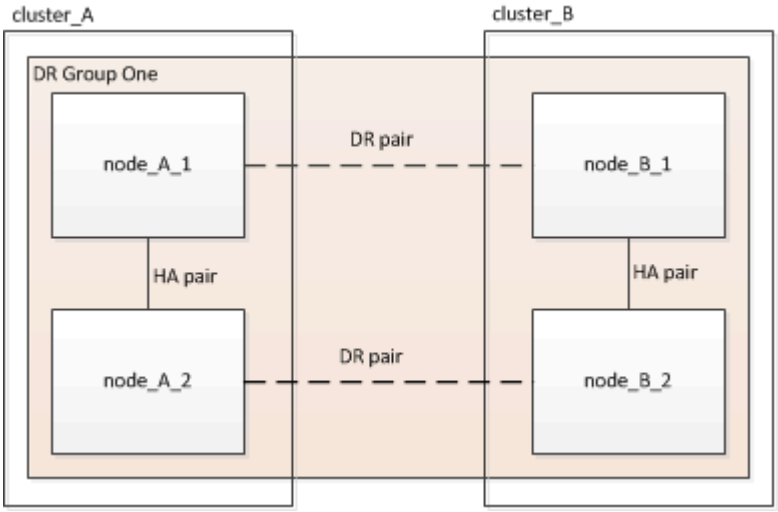
"So entfernen Sie eine DR-Gruppe aus einer MetroCluster-Konfiguration"

"NetApp Support"

Eine Konfiguration mit acht Nodes umfasst acht Nodes, die als zwei DR-Gruppen mit vier Nodes organisiert sind.



Durch Entfernen einer DR-Gruppe verbleiben vier Knoten in der Konfiguration.



Entfernen der DR-Gruppen-Nodes aus jedem Cluster

Bevor Sie beginnen

- Sie müssen diesen Schritt auf beiden Clustern durchführen.
- Der `metrocluster remove-dr-group` Befehl wird nur auf ONTAP 9.8 und höher unterstützt.

Schritte

1. Bereiten Sie sich auf das Entfernen der DR-Gruppe vor, falls noch nicht.

   a. Verschieben Sie alle Daten-Volumes in eine andere DR-Gruppe.

   b. Wenn die zu entfernende DR-Gruppe Spiegelvolumes mit der Lastverteilung enthält, können sie nicht verschoben werden. Erstellen Sie alle Spiegelvolumes mit Lastenfreigabe in einer anderen DR-Gruppe erneut, und löschen Sie dann die Spiegelvolumes mit Lastenfreigabe in der zu entfernenden DR-Gruppe.

   c. Verschieben Sie alle MDV_CRS-Metadaten-Volumes in eine andere DR-Gruppe, indem Sie die befolgen "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen" Verfahren.

   d. Löschen Sie alle MDV_aud-Metadaten-Volumes, die in der zu entfernenden DR-Gruppe vorhanden sein könnten.

   e. Löschen Sie alle Datenaggregate in der DR-Gruppe, die entfernt werden sollen, wie im folgenden Beispiel gezeigt:

```
ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
-fields aggregate ,node
ClusterA::> aggr delete -aggregate aggregate_name
ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
-fields aggregate ,node
ClusterB::> aggr delete -aggregate aggregate_name
```

   Root-Aggregate werden nicht gelöscht.

   f. Verschieben Sie die Daten-LIFs offline. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin down`

   g. Migrieren Sie alle Daten-LIFs auf Home Nodes in einer anderen DR-Gruppe.
   `network interface show -home-node` *`old_node`*

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-node` *`new_node`* `-home-port` *`port-id`*

   h. Verschieben Sie die Daten-LIFs wieder online. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin up`

   i. Migrieren Sie die Cluster-Management-LIF auf einen Home-Node in einer anderen DR-Gruppe.

   `network interface show -role cluster-mgmt`

   `network interface modify -vserver` *`svm-name`* `-lif` *`cluster_mgmt`* `-home-node` *`new_node`* `-home-port` *`port-id`*

   Das Node-Management und logische Schnittstellen zwischen Clustern werden nicht migriert.

   a. Übertragen Sie Epsilon auf einen Node in einer anderen DR-Gruppe, falls erforderlich.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identifizieren und entfernen Sie die DR-Gruppe.

   a. Identifizieren Sie die richtige DR-Gruppe für das Entfernen:

      ```
      metrocluster node show
      ```

   b. Entfernen Sie die Knoten der DR-Gruppe:
      ```
      metrocluster remove-dr-group -dr-group-id 1
      ```

      Im folgenden Beispiel wird das Entfernen der Konfiguration der DR-Gruppe auf „Cluster_A“ gezeigt

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B"to remove the remote nodes in the DR
group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not completed
on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Wiederholen Sie den vorherigen Schritt im Partner-Cluster.
4. Entfernen Sie bei einer MetroCluster IP-Konfiguration die MetroCluster-Verbindungen auf den Nodes der alten DR-Gruppe.

   Diese Befehle können von beiden Clustern ausgegeben werden und gelten für die gesamte DR-Gruppe, die beide Cluster abdeckt.

   a. Trennen Sie die Verbindungen:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Löschen Sie die MetroCluster-Schnittstellen auf den Knoten der alten DR-Gruppe:

```
metrocluster configuration-settings interface delete
```

c. Löschen Sie die Konfiguration der alten DR-Gruppe.
```
metrocluster configuration-settings dr-group delete
```

5. Heben Sie die Verbindung zu den Knoten in der alten DR-Gruppe auf.

   Sie müssen diesen Schritt für jedes Cluster durchführen.

   a. Legen Sie die erweiterte Berechtigungsebene fest:

   ```
   set -privilege advanced
   ```

   b. Deaktivieren des Speicher-Failover:

   ```
   storage failover modify -node node-name -enable false
   ```

   c. Heben Sie die Verbindung zum Knoten auf:
   ```
   cluster unjoin -node node-name
   ```

   Wiederholen Sie diesen Schritt für den anderen lokalen Knoten in der alten DR-Gruppe.

   d. Legen Sie die Administrator-Berechtigungsebene fest:
   ```
   set -privilege admin
   ```

6. Cluster-HA in der neuen DR-Gruppe erneut aktivieren:

   ```
   cluster ha modify -configured true
   ```

   Sie müssen diesen Schritt für jedes Cluster durchführen.

7. Halten Sie den Vorgang an, schalten Sie ihn aus und entfernen Sie die alten Controller-Module und Storage-Shelfs.

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen

"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management und Disaster Recovery"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln • Disaster Recovery
"Warten von MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes

"MetroCluster: Upgrade, Transition und Erweiterung"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"Installation und Konfiguration der MetroCluster Tiebreaker Software"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Dokumentation zu ONTAP Hardwaresystemen" In MetroCluster IP-Konfigurationen können Standardwartungsverfahren für Storage Shelves verwendet werden.	• Hot-Adding eines Festplatten-Shelfs • Hot-entfernen eines Festplatten-Shelfs
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.