



Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration

ONTAP MetroCluster

NetApp
February 27, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap-metrocluster/upgrade/concept_choosing_an_upgrade_method_mcc.html on February 27, 2026. 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
Hier starten: Sie haben die Wahl zwischen Controller-Upgrade, Systemaktualisierung oder Erweiterung	1
Wählen Sie ein Controller-Upgrade-Verfahren	2
Auswahl der Methode zur Systemaktualisierung	8
Wählen Sie ein Erweiterungsverfahren aus	13
Controller-Upgrades in MetroCluster IP mit vier Nodes mithilfe von Switchover und Switchback mit Befehlen, die den System-Controller ersetzen (ONTAP 9.13.1 und höher)	13
Workflow für das Upgrade von MetroCluster IP-Controllern mithilfe von Befehlen „System Controller Replace“ (ONTAP 9.13.1 oder höher)	13
Upgrade wird vorbereitet	14
Upgrade Ihrer Controller	27
Schließen Sie das MetroCluster IP-Controller-Upgrade ab	55
Controller-Upgrade in MetroCluster IP durch Switchover und Switchback (ONTAP 9.8 und höher)	56
Workflow für MetroCluster IP-Controller-Upgrades mithilfe von Switchover und Switchback (ONTAP 9.8 und höher)	56
Upgrade wird vorbereitet	57
Upgrade Ihrer Controller	72
Schließen Sie das MetroCluster IP-Controller-Upgrade ab	99
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)	101
Aktivieren Sie die Konsolenprotokollierung	102
Workflow für das Upgrade von Controllern in einer MetroCluster IP-Konfiguration	103
Bereiten Sie sich auf das Upgrade vor	103
Wechseln Sie über die MetroCluster-Konfiguration	109
Entfernen Sie das Controller-Modul der AFF A700 oder FAS9000 Plattform und NVS	111
Installieren Sie die AFF A900- oder FAS9500 NVS- und Controller-Module	112
Aktualisieren Sie die RCF-Dateien des Switches, um die neuen Plattformen aufzunehmen	118
Konfigurieren Sie die neuen Controller	119
Schalten Sie die MetroCluster-Konfiguration zurück	127
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration	129
Aktualisieren Sie die Knoten auf site_A	130
Stellen Sie die Tiebreaker- oder Mediator-Überwachung wieder her	130
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung	131
Aktualisieren Sie Controller in einer MetroCluster FC Konfiguration mithilfe von Switchover und Switchback	131
Unterstützte Plattformkombinationen	131
Über diese Aufgabe	131
Aktivieren Sie die Konsolenprotokollierung	132
Bereiten Sie sich auf das Upgrade vor	133
Wechseln Sie über die MetroCluster-Konfiguration	139
Vorbereiten der Netzwerkkonfiguration der alten Controller	141

Entfernen Sie die alten Plattformen	143
Konfigurieren Sie die neuen Controller	143
Schalten Sie die MetroCluster-Konfiguration zurück	155
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration	157
Aktualisieren Sie die Nodes auf Cluster_A	158
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung	158
Wiederherstellung des Tiebreaker Monitoring	158
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)	158
Aktivieren Sie die Konsolenprotokollierung	160
Bereiten Sie sich auf das Upgrade vor	160
Steckplatz 7 am AFF A700 Controller löschen	160
Wechseln Sie über die MetroCluster-Konfiguration	167
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul und den NVS an Site_B	169
Entfernen Sie das Controller-Modul und den NVS von beiden Nodes an Site_B	169
Installieren Sie das AFF A900 oder FAS9500 NVS und das Controller-Modul	171
Schalten Sie die MetroCluster-Konfiguration zurück	184
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration	185
Aktualisieren Sie die Knoten auf site_A	186
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung	186
Wiederherstellung des Tiebreaker Monitoring	187
Aktualisieren Sie Controller in einer MetroCluster FC-Konfiguration mit vier Knoten mithilfe von Switchover und Switchback mit den Befehlen „System Controller Replace“ (ONTAP 9.10.1 und höher).	187
Unterstützte Plattformkombinationen	187
Über diese Aufgabe	187
Aktivieren Sie die Konsolenprotokollierung	188
Bereiten Sie sich auf das Upgrade vor	188
Ersetzen Sie die alten Controller, und starten Sie die neuen Controller	192
Schließen Sie das Upgrade ab	204
Aktualisieren Sie die Nodes auf Cluster_A	205
Aktualisieren einer MetroCluster FC-Konfiguration mit vier Nodes	205
Aktivieren Sie die Konsolenprotokollierung	205
Führen Sie das Aktualisierungsverfahren durch	206
Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher)	208
Aktivieren Sie die Konsolenprotokollierung	210
Führen Sie das Aktualisierungsverfahren durch	210
Erweitern Sie eine MetroCluster FC Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes.	219
Erweitern einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes	219
Aktivieren Sie die Konsolenprotokollierung	221
Überprüfen des Status der MetroCluster-Konfiguration	221
Senden einer benutzerdefinierten AutoSupport Meldung, bevor Nodes zur MetroCluster Konfiguration hinzugefügt werden	223
Zoning für die neuen Controller-Ports beim Hinzufügen eines Controller-Moduls in einer Fabric-Attached MetroCluster-Konfiguration	224
Fügen Sie jedem Cluster ein neues Controller-Modul hinzu	224

Aktualisierung der MetroCluster Konfiguration durch neue Controller	257
Aktivieren von Storage Failover auf beiden Controller-Modulen und Aktivieren von Cluster HA	260
Starten Sie die SVMs neu	261
Erweitern Sie eine MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes	261
Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes	262
Aktivieren Sie die Konsolenprotokollierung	264
Bestimmen des neuen Verkabelungslayouts	264
Die neue Ausrüstung in den Racks zu bringen	265
Überprüfen des Systemzustands der MetroCluster-Konfiguration	265
Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor	267
Senden einer benutzerdefinierten AutoSupport Meldung vor dem Hinzufügen von Nodes zur MetroCluster Konfiguration	267
Reverkable und Zone A Switch Fabric für die neuen Nodes	268
Konfigurieren Sie ONTAP auf den neuen Controllern	269
Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor	299
Senden einer benutzerdefinierten AutoSupport Meldung nach dem Hinzufügen von Nodes zur MetroCluster Konfiguration	299
Überprüfung von Umschaltung, Reparatur und Wechsel zurück	300
Erweitern Sie eine MetroCluster IP-Konfiguration	300
Aktivieren Sie die Konsolenprotokollierung	302
Beispiel für die Benennung in diesem Verfahren	302
Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe	302
Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung	305
Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe	306
Überprüfen des Systemzustands der MetroCluster-Konfiguration	307
Entfernen der Konfiguration aus Überwachungsanwendungen	311
Vorbereiten der neuen Controller-Module	312
RCF-Dateien aktualisieren	312
Verbinden Sie die neuen Nodes mit den Clustern	314
Konfigurieren von Intercluster-LIFs, Erstellen der MetroCluster-Schnittstellen und Spiegeln von Root-Aggregaten	316
Beenden des Hinzufügung der neuen Nodes	328
Entfernen einer DR-Gruppe aus einer MetroCluster -Konfiguration	334
Aktivieren Sie die Konsolenprotokollierung	334
Entfernen Sie die DR-Gruppenknoten aus jedem Cluster	335
Wo Sie weitere Informationen finden	342
MetroCluster und sonstige Informationen	342

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 Shelves 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 Shelves.

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.



Warten Sie, bis alle Migrationsprozesse abgeschlossen sind, bevor Sie das Controller-Upgrade oder die Systemaktualisierungen initiieren. Starten Sie keine neuen SVM-Migrationsvorgänge während des Upgrade- oder Aktualisierungsprozesses.

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 Shelves 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.

Unterstützte Controller-Upgrades

Erfahren Sie mehr über die unterstützten Kombinationen für MetroCluster IP- und FC-Controller-Upgrades.

Unterstützte MetroCluster IP-Controller-Upgrades mithilfe von Befehlen „System Controller Replace“

Informationen zu unterstützten Plattformen finden Sie in der Tabelle in ["Aktualisieren Sie Controller in einer MetroCluster IP-Konfiguration mit vier Nodes mithilfe von Switchover und Switchback mit Befehlen, die den System-Controller ersetzen \(ONTAP 9.13.1 und höher\)"](#).

Alle anderen unterstützten MetroCluster IP-Controller-Upgrades

Finden Sie Ihre **Source**-Plattform in den MetroCluster Controller-Upgrade-Tabellen in diesem Abschnitt. Wenn die Schnittmenge der Spalte **Source** Plattform und **Target** Plattform leer ist, wird das Upgrade nicht unterstützt.

- 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.

- Auf allen Knoten (alt und neu) in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im ["Hardware Universe"](#).

Unterstützte AFF- und FAS MetroCluster IP-Controller-Upgrades

In den folgenden Tabellen sind die unterstützten Plattformkombinationen für das manuelle Upgrade eines AFF-

oder FAS-Systems in einer MetroCluster IP-Konfiguration in zwei Gruppen aufgeteilt.

- **Gruppe 1** zeigt Kombinationen für Upgrades auf AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF C400, AFF A400, AFF A220, AFF A300, AFF A320 und FAS8700 Systeme.
- **Gruppe 2** zeigt Kombinationen für Upgrades auf AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF, FAS9500, AFF A900, AFF A800 C80, FAS90, AFF A90 und AFF A1K Systeme.

Die folgenden Hinweise gelten für beide Gruppen:

- 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.
- Hinweis 3: Die Zielplattform kann erst nach Abschluss des Controller-Upgrades interne Laufwerke haben. Sie können die internen Laufwerke nach dem Upgrade hinzufügen.
- Hinweis 4: Bei der Aufrüstung integrierter Systeme (Festplatten und Controller im selben Gehäuse) müssen die Controller-Module ausgetauscht werden, während das bestehende Gehäuse und die Festplatten beibehalten werden.
- Hinweis 5: IOM-Module sind erforderlich, um die alten Controller in ein externes SAS-Shelf zu konvertieren. Informationen zu unterstützten IOM-Modulen finden Sie im ["Hardware Universe"](#).

AFF- und FAS-Kombinationen, Gruppe 1

Sehen Sie sich die unterstützten Kombinationen für Upgrades auf AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A400, AFF A220, AFF C400, AFF A320 und FAS8700 an.

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150		Note 5								
	AFF A20										
	FAS2750		Note 5								
	AFF A220										
	FAS500f						Note 4				
	AFF C250										
	AFF A250										
	FAS50										
	AFF C30										
	AFF A30										
	FAS8200										
	AFF A300										
	AFF A320										
	FAS8300										
	AFF C400										
	AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000										
	AFF A700										
	AFF A70										
	AFF C800										
	AFF A800										
	FAS9500										
	AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFF und FAS Kombinationsgruppe 2

Prüfen Sie die unterstützten Kombinationen für Upgrades auf AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

AFF and FAS		Target MetroCluster IP platform										
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150											
	AFF A20											
	FAS2750											
	AFF A220											
	FAS500f											
	AFF C250											
	AFF A250											
	FAS50											
	AFF C30											
	AFF A30											
	FAS8200					Note 3		Note 2			Note 3	
	AFF A300											
	AFF A320											
	FAS8300					Note 3		Note 2	Note 3		Note 3	
	AFF C400											
	AFF A400											
	FAS8700							Note 2				
	AFF C60											
	AFF A50											
	FAS70											
	FAS9000											
	AFF A700					Note 3		Note 1			Note 3	
	AFF A70										Note 4	
	AFF C800								Note 4		Note 4	
	AFF A800											
	FAS9500										Note 3	
	AFF A900											
	AFF C80											
	FAS90											
	AFF A90											
	AFF A1K											

Unterstützte ASA MetroCluster IP-Controller-Upgrades

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für das manuelle Upgrade eines ASA-Systems in einer MetroCluster IP-Konfiguration aufgeführt:

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								Note 1
	ASA C800								
	ASA A800								
	ASA A900								

- Hinweis 1: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.

Unterstützte MetroCluster FC-Controller-Upgrades

Finden Sie Ihre **Source**-Plattform in den MetroCluster Controller-Upgrade-Tabellen in diesem Abschnitt. Wenn die Schnittmenge der Spalte **Source** Plattform und **Target** Plattform leer ist, wird das Upgrade nicht unterstützt.

- 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.

- Auf allen Knoten (alt und neu) in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im "[Hardware Universe](#)".

Unterstützte Upgrades für AFF und FAS MetroCluster FC Controller

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum Upgrade eines AFF oder FAS Systems in einer MetroCluster FC-Konfiguration aufgeführt:

FAS and AFF		Target MetroCluster FC platform									
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF 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
	FAS9000									Note 3	
	AFF A700										Note 3
	FAS9500										
	AFF 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 Folgendes https://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.

Unterstützte ASA MetroCluster FC-Controller-Upgrades

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum Upgrade eines ASA Systems in einer MetroCluster FC-Konfiguration aufgeführt:

Quell-MetroCluster FC-Plattform	Ziel MetroCluster FC-Plattform	Unterstützt?
ASA A400	ASA A400	Ja.
	ASA A900	Nein
ASA A900	ASA A400	Nein
	ASA A900	Ja (siehe Hinweis 1)

- Hinweis 1: Controller-Upgrades werden auf Systemen mit ONTAP 9.14.1 oder höher unterstützt.

Wählen Sie eine Prozedur aus, die den Umschaltvorgang und den Umschaltvorgang verwendet

Nachdem Sie die unterstützten Upgrade-Kombinationen geprüft haben, wählen Sie das richtige Verfahren für das Controller-Upgrade für Ihre Konfiguration aus.

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 <code>system controller replace</code> Befehle	9.8 und höher	"Link zum Verfahren"
FC	Wird Verwendet <code>system controller replace</code> 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 Shelves. 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 aus MetroCluster IP-technischen Aktualisierungen

- 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. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden

Sie im ["Hardware Universe"](#).

- 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 AFF- und FAS MetroCluster IP-Tech Refresh

Die folgende Tabelle zeigt die unterstützten Plattformkombinationen für die Aktualisierung eines AFF- oder FAS-Systems in einer MetroCluster IP-Konfiguration. Die Tabellen sind in zwei Gruppen aufgeteilt:

- **Gruppe 1** zeigt Kombinationen für AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF C400, AFF A400, AFF A220, AFF A300, AFF A320 und FAS8700 Systeme.
- **Gruppe 2** zeigt Kombinationen für AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

Die folgenden Hinweise gelten für beide Gruppen:

- Anmerkung 1: Diese Kombination erfordert ONTAP 9.13.1 oder höher.

AFF- und FAS-Kombinationen, Gruppe 1

Sehen Sie sich die Kombinationen zur Systemaktualisierung für die Systeme AFF A150, FAS500f A20, AFF C250, FAS8300, AFF, FAS2750, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A320, AFF A220, AFF C400, AFF A400 und FAS8700 an.

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150	Note 1		Note 1	Note 1					Note 1	Note 1
	AFF A20										
	FAS2750 AFF A220	Note 1		Note 1	Note 1					Note 1	Note 1
	FAS500f AFF C250 AFF A250				Note 1					Note 1	Note 1
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90 AFF A90										
	AFF A1K										

AFF und FAS Kombinationsgruppe 2

Sehen Sie sich die Kombinationen für die Systemaktualisierung für die Systeme AFF C60, AFF A70 A50, FAS70, AFF C800, AFF A800, AFF, FAS9000, AFF A700, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K an.

AFF and FAS		Target MetroCluster IP platform									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150				Note 1		Note 1	Note 1			
	AFF A20										
	FAS2750 AFF A220				Note 1		Note 1	Note 1			
	FAS500f AFF C250 AFF A250				Note 1		Note 1	Note 1			
	FAS50										
	AFF C30 Aff A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90 AFF A90										
	AFF A1K										

Unterstützte ASA MetroCluster IP-Tech Refresh-Kombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für die Aktualisierung eines ASA-Systems in einer MetroCluster IP-Konfiguration aufgeführt:

ASA		Target MetroCluster IP platform							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Source MetroCluster IP platform	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

Unterstützte Kombinationen von MetroCluster FC-Technologie zur Aktualisierung

- 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. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im "[Hardware Universe](#)".
- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielpattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster

neu konfigurieren, damit sie die Grenzen der Zielformat erreichen oder darunter liegen, bevor Sie die neuen Nodes hinzufügen.

- Siehe "[Hardware Universe](#)" Für Plattformgrenzen

Unterstützte Kombinationen aus AFF- und FAS MetroCluster-FC-Technologieaktualisierung

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum Aktualisieren eines AFF oder FAS Systems in einer MetroCluster FC-Konfiguration aufgeführt:

FAS and AFF		Destination MetroCluster FC platform							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8200								
	AFF A300								
	FAS8300								
	AFF A400								
	FAS9000								
	AFF A700								
	FAS9500								
	AFF A900								

Unterstützte Kombinationen aus FC-Technologieaktualisierung von ASA MetroCluster

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum Aktualisieren eines ASA Systems in einer MetroCluster FC-Konfiguration aufgeführt:

Quell-MetroCluster FC-Plattform	Ziel MetroCluster FC-Plattform	Unterstützt?
ASA A400	ASA A400	Ja.
	ASA A900	Nein
ASA A900	ASA A400	Nein
	ASA A900	Ja.

Wählen Sie ein Aktualisierungsverfahren

Wählen Sie aus der folgenden Tabelle das Aktualisierungsverfahren für Ihre Konfiguration aus:

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"

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

Workflow für das Upgrade von MetroCluster IP-Controllern mithilfe von Befehlen „System Controller Replace“ (ONTAP 9.13.1 oder höher)

Sie können diesen geführten automatischen MetroCluster-Switchover-Vorgang verwenden, um ein unterbrechungsfreies Controller-Upgrade auf einer MetroCluster IP-Konfiguration mit vier Nodes auszuführen, bei der ONTAP 9.13.1 später ausgeführt wird. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Informationen zu diesem Workflow

Sie können diesen Workflow verwenden, um MetroCluster IP-Controller mit ONTAP 9.13.1 oder höher mithilfe von Switchover und Switchback mit Befehlen zu aktualisieren `system controller replace`.

1

"Upgrade wird vorbereitet"

Prüfen Sie die unterstützten Upgrade-Kombinationen und -Anforderungen und führen Sie die erforderlichen Aufgaben aus, um das System auf das Controller-Upgrade vorzubereiten. Das automatisierte Controller-Upgrade beginnt mit einer Reihe von Vorabprüfungen, bevor die Konfigurationsinformationen erfasst und vorhandene Monitoring-Software entfernt wird.

2

"Upgrade Ihrer Controller"

Der Automatisierungsvorgang initiiert die Umschaltvorgänge. Nach Abschluss dieser Vorgänge wird der Vorgang angehalten, sodass Sie die Netzwerkkonfiguration der alten Controller vorbereiten, ein Rack erstellen und die neuen Controller installieren, die Root-Aggregat-Festplatten neu zuweisen und die neuen Controller booten können.

3

"Schließen Sie das Upgrade ab"

Führen Sie das automatische Controller-Upgrade durch, indem Sie die Netzwerkfähigkeit überprüfen, die Upgrade-Aufgaben am zweiten Standort wiederholen und die Überwachungskonfiguration wiederherstellen.

Upgrade wird vorbereitet

Unterstützte MetroCluster IP-Controller-Upgrades mithilfe von Befehlen „System Controller Replace“

Bevor Sie mit dem Upgrade des MetroCluster IP-Controllers beginnen, müssen Sie überprüfen, ob Ihre Upgrade-Kombination unterstützt wird.

Finden Sie Ihre **Source**-Plattform in den MetroCluster Controller-Upgrade-Tabellen in diesem Abschnitt. Wenn die Schnittmenge der Spalte **Source** Plattform und **Target** Plattform leer ist, wird das Upgrade nicht unterstützt.

Bevor Sie mit dem Upgrade beginnen, überprüfen Sie die folgenden Überlegungen, um sicherzustellen, dass Ihre Konfiguration unterstützt wird.

- 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 Plattfortmty **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.

- Auf allen Knoten (alt und neu) in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im "[Hardware Universe](#)".

Unterstützte AFF- und FAS MetroCluster IP-Controller-Upgrades

Die folgende Tabelle zeigt die unterstützten Plattformkombinationen zum Upgrade eines AFF- oder FAS-Systems in einer MetroCluster IP-Konfiguration mit Befehlen zum Ersetzen des System-Controllers, aufgeteilt in zwei Gruppen.

- **Gruppe 1** zeigt Kombinationen für Upgrades auf AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF

C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF C400, AFF A400, AFF A220, AFF A300, AFF A320 und FAS8700 Systeme.

- **Gruppe 2** zeigt Kombinationen für Upgrades auf AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF, FAS9500, AFF A900, AFF A800 C80, FAS90, AFF A90 und AFF A1K Systeme.

Die folgenden Hinweise gelten für beide Gruppen:

- Hinweis 1: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.
- Hinweis 2: Die Zielplattform kann erst nach Abschluss des Controller-Upgrades interne Laufwerke haben. Sie können die internen Laufwerke nach dem Upgrade hinzufügen.
- Hinweis 3: Bei der Aufrüstung integrierter Systeme (Festplatten und Controller im selben Gehäuse) müssen die Controller-Module ausgetauscht werden, während das bestehende Gehäuse und die Festplatten beibehalten werden.
- Hinweis 4: Erfordert IOM-Module zur Konvertierung der alten Controller in ein externes SAS-Gehäuse. Siehe "[Hardware Universe](#)" für die unterstützten IOM-Module.
- Hinweis 5: Erfordert ONTAP 9.18.1GA oder später.

AFF- und FAS-Kombinationen, Gruppe 1

Sehen Sie sich die unterstützten Kombinationen für Upgrades auf AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A400, AFF A220, AFF C400, AFF A320 und FAS8700 an.

FAS and AFF		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster IP platform	AFF A150		Note 4								
	AFF A20										
	FAS2750 AFF A220		Note 4								
	FAS500f AFF C250 AFF A250						Note 3				
	FAS50										
	AFF C30 AFF A20										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFF und FAS Kombinationsgruppe 2

Prüfen Sie die unterstützten Kombinationen für Upgrades auf AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

FAS and AFF		Target MetroCluster IP platform										
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90	AFF A90	AFF A1K
Source MetroCluster IP platform	AFF A150											
	AFF A20											
	FAS2750											
	AFF A220											
	FAS500f											
	AFF C250											
	AFF A250											
	FAS50											
	AFF C30											
	AFF A20											
	FAS8200					Note 2		Note 1			Note 2	
	AFF A300											
	AFF A320											
	FAS8300											
	AFF C400					Note 2			Note 2		Note 2	
	AFF A400											
	FAS8700											
	AFF C60											
	AFF A50											
	FAS70									Note 5		
	FAS9000					Note 2					Note 2	
	AFF A700											
	AFF A70										Note 3 and Note 5	
	AFF C800								Note 3		Note 3	
	AFF A800											
	FAS9500										Note 2	
	AFF A900											
	AFF C80											
	FAS90											
	AFF A90											
	AFF A1K											

Unterstützte ASA MetroCluster IP-Controller-Upgrades

Das Upgrade der Controller mithilfe von `system controller replace` Befehlen auf ASA Systemen wird nicht unterstützt.

Weitere Verfahren finden Sie unter ["Wählen Sie eine Upgrade- oder Aktualisierungsmethode aus"](#).

Was kommt als Nächstes?

Lesen Sie die ["Voraussetzungen für die Verwendung dieses Upgrade-Verfahrens"](#).

Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens

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



Sie müssen dieses Verfahren bei jedem Upgrade Ihrer Controller wie beschrieben durchführen. Wenn neue Plattformen veröffentlicht werden, müssen möglicherweise neue oder geänderte Schritte befolgt werden. Wenn Sie beispielsweise auf Plattformen aktualisieren, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie ["Legen Sie das erforderliche Bootarg fest"](#) und führen Sie weitere Schritte für ein erfolgreiches Upgrade aus.

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

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

- Die MetroCluster IP Switches (Switch-Typ, Hersteller und Modell) und die Firmware-Version müssen von den vorhandenen und neuen Controllern in Ihrer Upgrade-Konfiguration unterstützt werden.

Informationen zu unterstützten Switches und Firmware-Versionen finden Sie im ["Hardware Universe"](#) oder

im "IMT" .

- Auf den MetroCluster IP-Systemen muss an beiden Standorten dieselbe ONTAP-Version ausgeführt werden.
- Wenn Sie ein Upgrade von Systemen durchführen, die über mehr Steckplätze oder Ports als das neue System verfügen, müssen Sie überprüfen, ob das neue System über genügend Steckplätze und Ports verfügt.

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

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

- Wenn es auf Ihrem System aktiviert ist, "[End-to-End-Verschlüsselung deaktivieren](#)" bevor Sie das Upgrade durchführen.
- 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:

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

- Node_B_2-neu

Was kommt als Nächstes?

["Aktivieren Sie die Konsolenprotokollierung"](#).

Aktivieren Sie die Konsolenprotokollierung vor dem MetroCluster IP-Upgrade

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

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

Was kommt als Nächstes?

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

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

Wenn Sie auf ein System aktualisieren, das in ONTAP 9.15.1 oder höher eingeführt wurde, müssen Sie normalerweise ein Bootarg auf den alten Controllern festlegen, bevor Sie mit dem Upgrade beginnen können.



Wenn Ihre Upgrade-Kombination betroffen ist, ist für ein erfolgreiches Upgrade das Festlegen eines Bootargs auf allen alten Controllern erforderlich. Lesen Sie die Informationen in diesem Abschnitt sorgfältig durch, um zu prüfen, ob für Ihre Upgrade-Kombination die Festlegung eines Bootargs erforderlich ist und wie Sie das richtige Bootarg für Ihre Kombination festlegen.

Schritt 1: Bestimmen Sie, ob Sie auf den alten Controllern ein Bootarg festlegen müssen

Bevor Sie mit dem Upgrade beginnen, bestimmen Sie anhand der folgenden Informationen, ob Sie auf den alten Controllern ein Bootarg festlegen müssen:

- Sie **müssen** auf den alten Controllern ein Bootarg für unterstützte Upgrades auf die folgenden Systeme festlegen, sofern nicht anders angegeben:
 - AFF A70, AFF A90, AFF A1K
 - FAS70, FAS90
 - AFF C80

- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60
- FAS50
- Sie müssen auf den alten Controllern **kein** Bootarg festlegen, wenn Ihr Upgrade eine der folgenden Kombinationen ist:
 - Von einem AFF A70 -System zu einem AFF A90 -System
 - Von einem FAS70-System zu einem FAS90-System



Wenn Sie für Ihr Upgrade keine Boot-Argumente festlegen müssen, können Sie diesen Schritt überspringen und direkt zu ["Bereiten Sie das System für das Upgrade vor"](#) gehen.

Schritt 2: Bestimmen Sie das Bootarg, das Sie auf den alten Controllern einstellen müssen

Bei den meisten betroffenen Upgrades müssen Sie Folgendes einstellen:

`hw.cxgbe.toe_keepalive_disable` Bootarg auf den alten Controllern. Für bestimmte Upgrade-Pfade müssen Sie jedoch die `bootarg.siw.interop_enabled` bootarg stattdessen.

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

Für dieses Upgrade...	Bootarg festlegen...
Von AFF A250 nach AFF A30	<code>bootarg.siw.interop_enabled</code>
Von AFF C250 nach AFF C30	<code>bootarg.siw.interop_enabled</code>
Von AFF A150 nach AFF A20	<code>bootarg.siw.interop_enabled</code>
Von AFF A220 nach AFF A20	<code>bootarg.siw.interop_enabled</code>
Alle anderen Upgrades für AFF A70, AFF A90, AFF A1K, FAS70-, FAS90-, AFF C80-, AFF A50-, AFF A30-, AFF C30-, AFF C60- oder FAS50-Systeme	<code>hw.cxgbe.toe_keepalive_disable</code>
Hinweis: Sie müssen kein Bootarg festlegen, wenn Ihr Upgrade von einem AFF A70 auf ein AFF A90 -System oder von einem FAS70- auf ein FAS90-System erfolgt.	

Schritt 3: Stellen Sie das erforderliche Bootarg auf den alten Controllern ein

Nachdem Sie das für Ihre Upgrade-Kombination erforderliche bootarg ermittelt haben, befolgen Sie die Schritte, um das bootarg auf den alten Controllern festzulegen.



Sie müssen das Bootarg auf allen alten Knoten an beiden Standorten festlegen, bevor Sie mit dem Upgrade beginnen.

Schritte

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

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

2. Stellen Sie den erforderlichen Bootarg für Ihre Upgrade-Kombination ein. Sie haben bereits den Bootarg festgelegt, den Sie mithilfe der Tabelle in festlegen müssen [Bestimmen Sie, welchen Bootarg Sie einstellen müssen](#).

hw.cxgbe.toe_keepalive_disable

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

```
setenv hw.cxgbe.toe_keepalive_disable 1  
  
saveenv  
  
printenv hw.cxgbe.toe_keepalive_disable
```

bootarg.siw.interop_enabled

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

```
setenv bootarg.siw.interop_enabled 1  
  
saveenv  
  
printenv bootarg.siw.interop_enabled
```

3. Booten des Node:

```
boot_ontap
```

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

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

5. Wiederholen Sie die Schritte für alle vier Nodes in der DR-Gruppe, die Sie aktualisieren.

Wie es weiter geht

["Bereiten Sie das System für das Upgrade vor"](#).

Bereiten Sie das MetroCluster IP-System für das Upgrade vor

Um das Controller-Upgrade vorzubereiten, müssen Sie möglicherweise die Switch-Referenzkonfigurationsdateien (RCFs) je nach den alten und neuen Plattformmodellen aktualisieren. Anschließend führen Sie Systemvorprüfungen durch, sammeln die Konfigurationsinformationen und entfernen die vorhandene Überwachungssoftware.

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

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

Upgrade durchführen.

Über diese Aufgabe

Führen Sie diese Aufgabe unter folgenden Umständen aus:

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

Bevor Sie beginnen

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

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

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

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

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



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

Schritte

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

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



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

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

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

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

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

Starten Sie den Controller-Austauschvorgang

Wenn Sie den automatisierten Controller-Austauschvorgang starten, führt der Vorgang eine Reihe von Vorprüfungen durch und hält dann an, damit Sie die konfigurationsbezogenen Informationen manuell erfassen können.

Über diese Aufgabe

Bevor die MetroCluster-Prüfungen beginnen, wird ONTAP Mediator, falls installiert, automatisch erkannt und entfernt. Um das Entfernen zu bestätigen, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wenn Sie das Upgrade abgeschlossen haben, die Vorprüfungen fehlschlagen oder Sie das Upgrade nicht fortsetzen möchten, müssen Sie manuell ["Konfigurieren Sie den ONTAP Mediator-Dienst 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. Führen Sie den folgenden Befehl von Standort A aus, um die Controller an Standort B zu ersetzen:

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



- Wenn Sie die `-nso true` Parameter im Befehl: Das Controller-Upgradeverfahren wählt NSO-basiertes automatisches Umschalten und Zurückschalten als Standardverfahren auf MetroCluster-IP-Systemen.
- Wenn Sie den Vorgang an einem Standort wiederholen, nachdem Sie die Controller am anderen Standort bereits ausgetauscht haben, tritt aufgrund einer Nichtübereinstimmung der Knoten an beiden Standorten ein Fehler auf. Dies ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind.

Wenn nur der Fehler „Mismatch“ zurückgegeben wird, können Sie die `-skip -metrocluster-check true` Option mit der `system controller replace start` Befehl, um die MetroCluster-Prüfungen zu überspringen.

Die Prüfungen werden im automatisierten Betrieb durchgeführt. 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 Quellcontroller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang nach dem Booten der neuen Knoten angehalten und meldet einen Fehler. Führen Sie die manuelle Wiederherstellung durch, um den Cluster wieder in einen fehlerfreien Zustand zu versetzen.

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 Sie vor dem Upgrade Informationen

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
- ° aggr show -r
- ° disk show
- ° system node run <node-name> disk show
- ° vol show -fields type
- ° vol show -fields type , space-guarantee
- ° vservers fcp initiator show
- ° storage disk show
- ° metrocluster configuration-settings interface show

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 Informationen für das Verschlüsselungsmanagement"](#).

a. Wenn Onboard Key Manager konfiguriert ist:

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

Sie benötigen die Passphrase später im Upgrade-Verfahren.

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

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

```
security key-manager key query
```

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

```
system controller replace resume
```

Entfernen Sie die vorhandene Konfiguration aus Tiebreaker oder einer anderen Monitoring-Software

Bevor Sie mit dem Upgrade beginnen, entfernen Sie die vorhandene Konfiguration aus dem Tiebreaker oder einer anderen Überwachungssoftware.

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"](#) aus der 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.

Was kommt als Nächstes?

["Vorbereiten der Netzwerkkonfiguration der alten Controller"](#).

Upgrade Ihrer Controller

Bereiten Sie die Netzwerkkonfiguration der alten MetroCluster IP-Controller vor

Nachdem Sie Informationen gesammelt und den Vorgang fortgesetzt haben, wird die Umschaltung fortgesetzt.

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.

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 starten und die Root-Aggregat-Festplatten dem neuen Controller-Modul aus Flash-Backup mit dem zuvor gesammelten zuweisen können `sysids`.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie verwenden die in gesammelten Informationen "[Sammeln Sie vor dem Upgrade Informationen](#)".

Schritte

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

```
boot_ontap
```

2. Wenn das System, auf das Sie aktualisieren, **Shared Cluster/HA-Ports** verwendet, überprüfen Sie, ob die MetroCluster-IP-Schnittstellen unterstützte IP-Adressen verwenden.

Verwenden Sie die folgenden Informationen, um zu bestimmen, ob das neue System gemeinsam genutzte Cluster/HA-Ports verwendet:

Shared-Cluster-/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte Cluster-/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90

Shared-MetroCluster/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte MetroCluster/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

- a. Überprüfen Sie die IP-Adressen der MetroCluster-Schnittstellen auf den alten Controllern:

```
metrocluster configuration-settings interface show
```

- b. Wenn die MetroCluster-Schnittstellen 169.254.17.x- oder 169.254.18.x-IP-Adressen verwenden, finden Sie unter ["Der Knowledge Base-Artikel „Ändern der Eigenschaften einer MetroCluster IP-Schnittstelle“"](#)

Informationen zum Ändern der Schnittstellen-IP-Adressen, bevor Sie mit dem Upgrade fortfahren.



Ein Upgrade auf ein System mit **Shared Cluster/HA-Ports** wird nicht unterstützt, wenn die MetroCluster-Schnittstellen mit 169.254.17.x- oder 169.254.18.x-IP-Adressen konfiguriert sind.

3. Ändern Sie die Intercluster LIFs auf den alten Controllern, um einen anderen Home Port zu verwenden als die Ports, die für HA Interconnect oder MetroCluster IP DR Interconnect auf den neuen Controllern verwendet werden.



Dieser Schritt ist für ein erfolgreiches Upgrade erforderlich.

Die Intercluster LIFs auf den alten Controllern müssen einen anderen Home Port verwenden als die Ports, die für HA Interconnect oder MetroCluster IP DR Interconnect auf den neuen Controllern verwendet werden. Wenn Sie beispielsweise auf AFF A90 Controller aktualisieren, sind die HA Interconnect-Ports e1a und e7a und die MetroCluster IP DR Interconnect-Ports e2b und e3b. Sie müssen die Intercluster LIFs auf den alten Controllern verschieben, wenn sie auf den Ports e1a, e7a, e2b oder e3b gehostet werden.

Informationen zur Portverteilung und -Zuweisung auf den neuen Knoten finden Sie im "[Hardware Universe](#)".

- a. Sehen Sie sich auf den alten Controllern die Intercluster LIFs an:

```
network interface show -role intercluster
```

Je nachdem, ob die Intercluster LIFs auf den alten Controllern die gleichen Ports verwenden, wie die Ports für HA Interconnect oder den MetroCluster IP DR Interconnect auf den neuen Controllern.

Wenn die Intercluster LIFs...	Gehe zu...
Verwenden Sie denselben Home-Port	Unterschritt b
Verwenden Sie einen anderen Home-Port	Schritt 4

- b. Ändern Sie die Intercluster LIFs, um einen anderen Home Port zu verwenden:

```
network interface modify -vserver <vserver> -lif <intercluster_lif> -home  
-port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-  
nodes>
```

- c. Überprüfen Sie, ob sich alle Intercluster LIFs an ihren neuen Home Ports befinden:

```
network interface show -role intercluster -is-home false
```

Die Befehlsausgabe sollte leer sein und bedeutet, dass sich alle Intercluster LIFs auf ihren jeweiligen Home Ports befinden.

- d. Setzen Sie alle LIFs zurück, die sich nicht auf ihrem Home Port befinden:

```
network interface revert -lif <intercluster_lif>
```

Wiederholen Sie den Befehl für jede Intercluster LIF, die sich nicht im Home Port befindet.

4. Zuweisen Sie den Home-Port aller Daten-LIFs auf dem alten Controller einem gemeinsamen Port, der

sowohl auf den alten als auch auf den neuen Controller-Modulen identisch ist.



Wenn die alten und neuen Controller keinen gemeinsamen Port haben, müssen Sie die Daten-LIFs nicht ändern. Überspringen Sie diesen Schritt und gehen Sie direkt zu [Schritt 5](#).

a. Anzeigen der LIFs:

```
network interface show
```

Alle Daten-LIFs wie SAN und NAS sind admin „up“ und operativ „down“, da diese sich am Umschaltstandort befinden (Cluster_A).

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 der einzelnen Plattformmodelle finden Sie im ["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
```

5. Ändern Sie Broadcast-Domänen, um das zu löschende VLAN und die physischen Ports zu entfernen:

```
broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name>-ports <node-name:port-id>
```

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

6. 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 ala -port e0d
```

a. VLAN- und Schnittstellengruppen-Ports aus der Broadcast-Domäne entfernen:

```
network port broadcast-domain remove-ports -ipSPACE <ipSPACE> -broadcast-domain <broadcast-domain-name>-ports <nodename:portname,nodename:portname>,...
```

b. Ändern Sie die Ports der Schnittstellengruppe, um andere physische Ports als Mitglied zu verwenden:

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

7. Anhalten der Knoten:

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

Dieser Schritt muss auf beiden Knoten durchgeführt werden.

8. Überprüfen Sie, ob die Nodes an der `LOADER` Eingabeaufforderung angezeigt werden, und sammeln und erhalten Sie die aktuellen Umgebungsvariablen.

9. Ermitteln Sie die Bootarg-Werte:

```
printenv
```

10. Schalten Sie die Nodes und Shelves an dem Standort aus, an dem der Controller aktualisiert wird.

Was kommt als Nächstes?

"Richten Sie die neuen Controller ein und booten Sie sie über das Netzwerk".

Richten Sie die neuen MetroCluster IP-Controller ein und booten Sie sie über das Netzwerk

Richten Sie die neuen Controller vor dem Booten der Controller ein, um zu bestätigen, dass auf den neuen Nodes dieselbe Version von ONTAP wie auf den ursprünglichen Nodes ausgeführt wird.

Richten Sie die neuen Controller ein

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

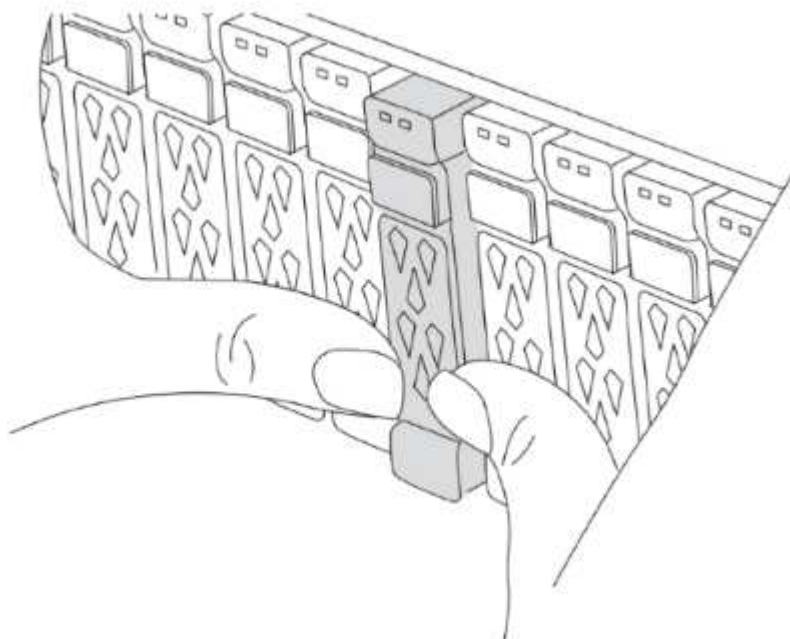
Schritte

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-Shelves in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Wenn Ihr Upgrade den Austausch der Controller-Module erfordert, beispielsweise das Upgrade von einem AFF A800 auf ein AFF A90-System oder von einem AFF C800 auf ein AFF C80-System, müssen Sie das Controller-Modul aus dem Gehäuse entfernen, wenn Sie das Controller-Modul austauschen. Für alle anderen Upgrades fahren sie mit [Schritt 4](#) fort.

Drücken Sie auf der Vorderseite des Gehäuses die Daumen, um jedes Laufwerk fest einzuschieben, bis Sie einen positiven Stopp spüren. Dadurch wird bestätigt, dass die Laufwerke fest an der Mittelplatte des Gehäuses sitzen.



4. Installieren Sie die Controller-Module.

Welche Installationsschritte Sie durchführen, hängt davon ab, ob Ihr Upgrade den Austausch der Controller-Module erfordert oder ob IOM-Module zur Konvertierung der alten Controller in ein externes Shelf erforderlich sind.

Wenn Sie ein Upgrade durchführen...	Folgen Sie den Schritten für ...
• Ein AFF A150 auf ein AFF A20-System • Ein AFF A220 auf ein AFF A20-System	Konvertierung von Controller zu externem Shelf
• Ein AFF A800 auf ein AFF A90 System • Ein AFF C800 auf ein AFF C80-System • Ein AFF A250 zu einem AFF A30 System • Ein AFF C250 zu einem AFF C30 System • Ein AFF A70 zu einem AFF A90 System	Austausch des Controller-Moduls
Beliebige andere Kombinationen für Controller-Upgrades	Alle anderen Upgrades

Konvertierung von Controller zu externem Shelf

Bei ursprünglichen MetroCluster IP-Controllern handelt es sich um AFF A150- oder AFF A220-Modelle, können Sie das AFF A150 oder AFF A220 HA-Paar in ein DS224C Laufwerk-Shelf konvertieren und dann zu den neuen Nodes hinzufügen.

Wenn Sie beispielsweise ein Upgrade von einem AFF A150 oder AFF A220 System zu einem AFF A20 System durchführen, können Sie das AFF A150 oder AFF A220 HA-Paar in ein DS224C Shelf konvertieren, indem Sie die AFF A150 oder AFF A220 Controller-Module durch IOM12-Module austauschen.

Schritte

- a. Ersetzen Sie die Controller-Module im Node, den Sie mit IOM12 Shelf-Modulen konvertieren.

"Hardware Universe"

- b. Legen Sie die Festplatten-Shelf-ID fest.

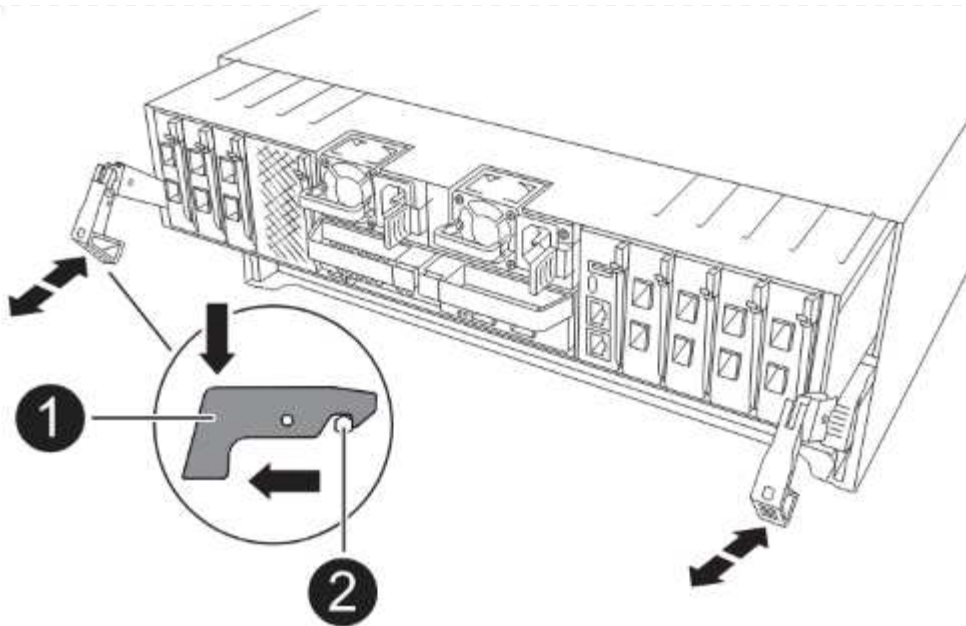
Jedes Festplatten-Shelf, einschließlich des Chassis, erfordert eine eindeutige ID.

- c. Setzen Sie andere Festplatten-Shelf-IDs bei Bedarf zurück.
- d. Schalten Sie die Shelves aus.
- e. Verkabeln Sie das umgewandelte Festplatten-Shelf mit einem SAS-Port auf dem neuen System und bei Verwendung von Out-of-Band-ACP-Verkabelung zum ACP-Port auf dem neuen Node.
- f. Schalten Sie das umgewandelte Laufwerk-Shelf und alle anderen an die neuen Nodes angeschlossenen Laufwerk-Shelves ein.
- g. Schalten Sie die neuen Nodes ein und unterbrechen Sie dann den Boot-Prozess auf jedem Node, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Austausch des Controller-Moduls

Die separate Installation der neuen Controller ist bei Upgrades integrierter Systeme mit Festplatten und Controllern im selben Chassis, beispielsweise von einem AFF A800 System auf ein AFF A90 System, nicht möglich. Sie müssen die neuen Controller-Module und I/O-Karten nach dem Ausschalten der alten Controller austauschen, wie in der Abbildung unten gezeigt.

Das folgende Beispielbild dient nur zur Darstellung. Die Controller-Module und E/A-Karten können zwischen den Systemen variieren.



Alle anderen Upgrades

Installieren Sie die Controller-Module im Rack oder Schrank.

5. Verkabeln Sie die Stromversorgungs-, seriellen Konsolen- und Managementverbindungen der Controller wie in beschrieben "[MetroCluster IP-Switches verkabeln](#)"

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 Aufforderung Strg-C, um die Eingabeaufforderung anzuzeigen `LOADER`.

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

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 im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten 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 einer Kernel-Datei enthalten: `ontap-`

```
version_image.tgz
```

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

4. Konfigurieren Sie an der `LOADER` Eingabeaufforderung 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.

```
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. Eingeben `n` Überspringen Sie die Backup-Wiederherstellung, wenn Sie eine ähnliche Aufforderung wie die folgende sehen:

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



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

```
halt
```

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

```
set-defaults
```

3. Umgebung speichern:

```
saveenv
```

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

```
boot_ontap menu
```

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

```
wipeconfig
```

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

Was kommt als Nächstes?

["Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status fest"](#).

Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status des MetroCluster IP-Controllers und -Gehäuses fest

Konfigurieren Sie die HBA-Karten im Controller-Modul, und überprüfen und legen Sie den HA-Status des Controllers und des Gehäuses fest.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration von HBA-Karten im Controller-Modul müssen Sie sie für Ihren Standort korrekt 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	<code>ucadmin modify -m fc -t initiator <adapter-name></code>
CNA-Ethernet	<code>ucadmin modify -mode cna <adapter-name></code>
FC-Ziel	<code>fcadmin config -t target <adapter-name></code>
FC-Initiator	<code>fcadmin config -t initiator <adapter-name></code>

2. Beenden des Wartungsmodus:

```
halt
```

Warten Sie nach dem Ausführen des Befehls, bis der Node an der Eingabeaufforderung angehalten `LOADER` wird.

3. Booten Sie den Node wieder im Wartungsmodus, um die Konfigurationsänderungen anzuwenden:

```
boot_ontap maint
```

4. Überprüfen Sie die Änderungen:

Wenn Sie über diese Art von HBA verfügen...	Befehl
CNA	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

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. Überprüfen und ändern Sie die Ethernet-Ports, die mit NS224-Shelfs oder Speicher-Switches verbunden sind.

- a. Überprüfen Sie die Ethernet-Ports, die mit NS224-Shelfs oder Speicher-Switches verbunden sind:

```
storage port show
```

- b. Setzen Sie alle mit Ethernet-Shelfs oder Storage-Switches verbundenen Ethernet-Ports, einschließlich gemeinsam genutzter Switches für Storage und Cluster, auf den `storage` Modus:

```
storage port modify -p <port> -m storage
```

Beispiel:

```
*> storage port modify -p e5b -m storage
Changing NVMe-oF port e5b to storage mode
```



Dies muss für alle betroffenen Ports festgelegt werden, damit ein Upgrade erfolgreich durchgeführt werden kann.

Festplatten aus den an die Ethernet-Ports angeschlossenen Shelfs werden in der Ausgabe gemeldet `sysconfig -v`.

Informationen zu den Speicherports für das System, auf das Sie aktualisieren, finden Sie im "[Hardware Universe](#)".

- a. Überprüfen Sie, ob `storage` der Modus festgelegt ist, und vergewissern Sie sich, dass die Ports den Status „Online“ aufweisen:

```
storage port show
```

4. Stoppen Sie den Knoten: `halt`

Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

5. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `show date`

6. Stellen Sie bei Bedarf das Datum in UTC oder GMT ein: `set date <mm/dd/yyyy>`

7. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`

8. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`

9. Einstellungen speichern: `saveenv`

10. Umgebungsvariablen erfassen: `printenv`

Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers

Wenn Sie ein Upgrade von einem System mit ausschließlich externen Laufwerken auf ein System mit externen und internen Laufwerken (Festplatten und Controller im selben Gehäuse) durchführen, müssen Sie alle internen Laufwerke aus dem neuen System entfernen oder ausbauen, bis Sie das Upgrade abgeschlossen haben.



Diese Aufgabe ist für ein erfolgreiches Controller-Upgrade auf betroffenen Systemen zwingend erforderlich.

1. Wenn Ihre Upgrade-Kombination mit **Hinweis 2** gekennzeichnet ist, müssen Sie die internen Laufwerke aus dem neuen System entfernen oder aus dem Sitz lösen

Nach Abschluss dieser Aufgabe sollten keine internen Laufwerke mehr zugänglich sein. Sie fügen die Laufwerke später im Verfahren zum neuen Controller hinzu.

Was kommt als Nächstes?

["Aktualisieren Sie die Switch-RCF-Dateien und legen Sie die MetroCluster IP-Bootarg-Werte fest"](#).

Aktualisieren Sie die Switch-RCFs und legen Sie die MetroCluster IP-Bootarg-Werte fest

Aktualisieren Sie die Switch-Referenzkonfigurationsdateien (RCFs) für die neuen Plattformen und legen Sie die MetroCluster IP-Bootarg-Werte auf den Controller-Modulen fest.

Aktualisieren Sie die Switch-RCFs, 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-Switches auf die Anwendung der neuen RCFs vor.

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

- ["Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"](#)

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

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

- ["Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"](#)

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

- Sie benötigen die UUIDs und System-IDs, die zuvor im Upgrade-Verfahren in identifiziert "[Sammeln Sie vor dem Upgrade Informationen](#)" wurden.
- Je nach Plattformmodell können Sie die VLAN-ID mit dem Parameter angeben `-vlan-id`. Die folgenden Plattformen unterstützen den Parameter nicht `-vlan-id`:
 - FAS8200 UND AFF A300
 - AFF A320
 - FAS9000 und AFF A700
 - AFF C800, ASA C800, AFF A800 und ASA A800

Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.

- Die von Ihnen festgelegten MetroCluster Bootarg-Werte hängen davon ab, ob Ihr neues System gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet.

Shared-Cluster-/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte Cluster-/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90

Shared-MetroCluster/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte MetroCluster/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

Schritte

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

Die Schritte, die Sie befolgen, hängen von den Ports ab, die vom neuen Plattformmodell verwendet werden.

Systeme, die Shared Cluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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



Wenn die Schnittstellen eine Standard-VLAN-ID verwenden, ist der `vlan-id` Parameter nicht erforderlich.

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

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

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

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

Im folgenden Beispiel werden die Werte für Node_B_1-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen festgelegt:

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

Im folgenden Beispiel werden die Werte für Node_B_2-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen festgelegt:

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

Systeme, die gemeinsam genutzte MetroCluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs 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 eine Standard-VLAN-ID verwenden, ist der `vlan-id` Parameter nicht erforderlich.

Im folgenden Beispiel werden die Werte für Node_B_1-New 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-New 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
```

Im folgenden Beispiel werden die Werte für Node_B_1-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen 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
```

Im folgenden Beispiel werden die Werte für Node_B_2-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen 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
```

2. Legen Sie an DER LOADER-Eingabeaufforderung der neuen Nodes die UUIDs 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
```

3. Bestimmen Sie, ob die ursprünglichen Systeme für die erweiterte Laufwerkpartitionierung (Advanced Drive Partitioning, ADP) konfiguriert wurden, indem Sie den folgenden Befehl vom Standort aus ausführen:

```
disk show
```

In der Spalte „Containertyp“ wird in der Ausgabe „freigegeben“ angezeigt `disk show`, wenn ADP konfiguriert ist. Wenn „Containertyp“ einen anderen Wert hat, ist ADP auf dem System nicht konfiguriert. Die folgende Beispielausgabe zeigt ein mit ADP konfiguriertes System:

```
::> disk show
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
Info: This cluster has partitioned disks. To get a complete list of spare disk capacity use "storage aggregate show-spare-disks".						
1.11.0 node_A_1	894.0GB	11	0	SSD	shared	testaggr
1.11.1 node_A_1	894.0GB	11	1	SSD	shared	testaggr
1.11.2 node_A_1	894.0GB	11	2	SSD	shared	testaggr

4. Wenn die ursprünglichen Systeme mit partitionierten Laufwerken für ADP konfiguriert wurden, aktivieren Sie diese an der `LOADER` Eingabeaufforderung für jeden Ersatz-Node:

```
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
```

Was kommt als Nächstes?

"[Weisen Sie die Root-Aggregat-Festplatten neu zu](#)".

Weisen Sie die Festplatten des Root-Aggregats dem neuen MetroCluster IP-Controller-Modul neu zu

Weisen Sie die Festplatten des Stammaggregats dem neuen Controller-Modul unter Verwendung der zuvor zusammengetragenen System-IDs neu zu.

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "[Sammeln Sie vor dem Upgrade Informationen](#)".

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. Verkabeln Sie alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.).
2. Halten Sie das System an und starten Sie von der in den Wartungsmodus `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). Dieses Beispiel zeigt keine Laufwerke an, die anderen Nodes in der MetroCluster-Konfiguration gehören.



Bevor Sie mit der Neuuzuweisung der Festplatte fortfahren, überprüfen Sie, ob die zum Root-Aggregat des Node gehörenden Pool0- und Pool1-Festplatten in der Ausgabe angezeigt werden `disk show`. Im folgenden Beispiel werden in der Ausgabe die Laufwerke pool0 und pool1 aufgelistet, die sich im Besitz von Node_B_1-old 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 SOM1J2CF
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254) Pool0 SOM0CQM5
node_B_1-old(4068741254) node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254) Pool0 SOM1PSDW
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 Befehl ausführen `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid`.

Das folgende Beispiel zeigt die Neuuzuweisung 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)   Pool11 PZHYN0MD
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool11 PPG3J5HA
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool11 PZHTDSZD
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool10 SOM1J2CF
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool10 SOM0CQM5
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool10 SOM1PSDW
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).

Was kommt als Nächstes?

["Booten der neuen Controller und Wiederherstellen der LIF-Konfiguration".](#)

Starten Sie die neuen MetroCluster IP-Controller und stellen Sie die LIF-Konfiguration wieder her

Starten Sie die neuen Controller und überprüfen Sie, ob LIFs auf den entsprechenden Nodes und Ports gehostet werden, bevor Sie den Vorgang mit dem Befehl fortsetzen
`system controller replace resume`.

Starten Sie die neuen Controller

Starten Sie die neuen Controller, überprüfen Sie, ob die Bootarg-Variablen korrekt sind und führen Sie bei Bedarf die Schritte zur Wiederherstellung der Verschlüsselung durch.

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. Prüfen Sie, ob die Partner-Sysid korrekt ist:

```
printenv partner-sysid
```

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

```
setenv partner-sysid <partner-sysID>
```

4. Anzeigen des Startmenüs:

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



Mit der Option „6“ wird der Knoten zweimal neu gebootet, bevor der Prozess abgeschlossen ist.

Reagieren Sie mit „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}`. Eingabe `y`.

7. Überprüfen Sie an der `LOADER` Eingabeaufforderung die Bootarg-Werte, und aktualisieren Sie die Werte bei Bedarf.

Verwenden Sie die Schritte in ["Legen Sie die MetroCluster-IP-Bootarg-Variablen fest"](#).

8. Überprüfen Sie, ob die Partner-Sysid korrekt 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“ 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.

10. Starten der Knoten:

```
boot_ontap
```

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

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

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

- a. Broadcast-Domänen anzeigen:

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

- b. Wenn für die Datenports auf den neu aktualisierten Controllern eine neue Broadcast-Domäne erstellt wird, löschen Sie die Broadcast-Domäne:



Löschen Sie nur die neue Broadcast-Domäne. Löschen Sie keine der Broadcast-Domänen, die vor dem Start des Upgrades vorhanden waren.

```
broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

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

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

- d. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast-Domäne hostet.
- e. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.
- f. Sobald die Intercluster-LIFs aktiv sind, überprüfen Sie den Cluster-Peer-Status und stellen Sie das Cluster-Peering bei Bedarf wieder her.

Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

"Erstellen einer Cluster-Peer-Beziehung"

- g. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

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

"Erstellen Sie eine VLAN"

"Kombinieren Sie physische 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
```

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

Sie verwenden...	Befehl
Integriertes Verschlüsselungsmanagement	<pre>security key-manager onboard sync</pre> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	<pre>`security key-manager external restore -vserver <svm-name> -node <node-name> -key-server <host_name</pre>

14. Vergewissern Sie sich, dass 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

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs auf den entsprechenden Nodes gehostet werden, bevor Sie mit dem

automatischen Switchback fortfahren.

Über diese Aufgabe

- Diese Aufgabe wird auf Site_B. ausgeführt



Sie müssen vor dem Wechsel zurück überprüfen, ob die Daten-LIFs auf den neuen Nodes korrekt sind. Wenn Sie die Konfiguration zurückschalten, versucht ONTAP, den Datenverkehr auf dem von den LIFs verwendeten Home Port wiederaufzunehmen. E/A-Fehler können auftreten, wenn die Verbindung des Home-Ports zum Switch-Port und VLAN falsch ist.

Schritte

1. Vergewissern Sie sich vor dem Switchback, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

- a. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

- b. Zeigen Sie die LIFs an und vergewissern Sie sich, dass jede Daten-LIF den richtigen Home Port verwendet:

```
network interface show
```

- c. Ändern Sie alle LIFs, die nicht den korrekten Home Port verwenden:

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

Wenn der Befehl einen Fehler zurückgibt, können Sie die Portkonfiguration überschreiben:

```
vserver config override -command "network interface modify -vserver <svm-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. Vergewissern Sie sich, dass alle Daten-LIFs nun am richtigen Home Port sind:

```
network interface show
```

- b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

```
network interface revert * -vserver <svm-name>
```

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

3. Vorgang fortsetzen:

```
system controller replace resume
```

Was kommt als Nächstes?

"Schließen Sie das Controller-Upgrade ab".

Schließen Sie das MetroCluster IP-Controller-Upgrade ab

Führen Sie das automatische Controller-Upgrade durch, indem Sie die Erreichbarkeit des Netzwerks überprüfen und die Überwachungskonfiguration wiederherstellen.

Überprüfung der Erreichbarkeit des Netzwerks

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 der Überprüfung nach dem Upgrade 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.

Aktualisieren Sie die Nodes auf Cluster_A

Sie müssen die Upgrade-Tasks wiederholen, um die Nodes auf „Cluster_A“ an Standort A zu aktualisieren

Schritte

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

Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt.

Fügen Sie interne Laufwerke erneut zum neuen Controller hinzu

Wenn Sie ein System mit ausschließlich externen Laufwerken auf ein System mit externen und internen Laufwerken (Festplatten und Controller im selben Gehäuse) aktualisiert haben, können Sie die aus den internen Steckplätzen des neuen Systems entfernten oder entfernten Festplatten hinzufügen oder neu einsetzen. Dies ist jederzeit möglich, nachdem das Upgrade an beiden Standorten abgeschlossen ist und der Cluster fehlerfrei ist.

Nachdem Sie die Laufwerke erneut hinzugefügt oder neu eingesetzt haben, können sie nach Bedarf in ONTAP verwendet werden.



Diese Aufgabe gilt nur für bestimmte Upgrade-Kombinationen. Weitere Informationen finden Sie unter ["Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers"](#).

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 ONTAP Mediator über eine MetroCluster-IP-Konfiguration"](#).

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 in ["Fügen Sie MetroCluster-Konfigurationen hinzu"](#).

Konfigurieren Sie die End-to-End-Verschlüsselung

Falls es von Ihrem System unterstützt wird, können Sie zwischen den MetroCluster IP-Standorten den Back-End-Verkehr, wie NVLOG- und Storage-Replizierungsdaten, verschlüsseln. Siehe ["Konfigurieren Sie die End-to-End-Verschlüsselung"](#) Finden Sie weitere Informationen.

Controller-Upgrade in MetroCluster IP durch Switchover und Switchback (ONTAP 9.8 und höher)

Workflow für MetroCluster IP-Controller-Upgrades mithilfe von 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.

Informationen zu diesem Workflow

Sie können diesen Workflow verwenden, um MetroCluster IP-Controller mithilfe von Switchover und Switchback auf Systemen mit ONTAP 9.8 oder höher zu aktualisieren.

1

"Upgrade wird vorbereitet"

Prüfen Sie die unterstützten Upgrade-Kombinationen und -Anforderungen und führen Sie die erforderlichen Aufgaben aus, um das System auf das Controller-Upgrade vorzubereiten.

2

"Upgrade Ihrer Controller"

Wechseln Sie die MetroCluster Konfiguration, um die Konfiguration der alten Controller zu entfernen, Rack und installieren Sie die neuen Controller, weisen Sie die Root-Aggregat-Festplatten neu zu und booten Sie die neuen Controller, bevor Sie einen Switchback durchführen.

3

"Schließen Sie das Upgrade ab"

Führen Sie das Controller-Upgrade durch, indem Sie die Upgrade-Aufgaben am zweiten Standort wiederholen und die Überwachungskonfiguration wiederherstellen.

Upgrade wird vorbereitet**Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens**

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



Sie müssen dieses Verfahren bei jedem Upgrade Ihrer Controller wie beschrieben durchführen. Wenn neue Plattformen veröffentlicht werden, müssen möglicherweise neue oder geänderte Schritte befolgt werden. Wenn Sie beispielsweise auf Plattformen aktualisieren, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie ["Legen Sie das erforderliche Bootarg fest"](#) und führen Sie weitere Schritte für ein erfolgreiches Upgrade aus.

Plattformen, die durch dieses Verfahren unterstützt werden

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

Siehe ["Wahl einer Upgrade- oder Aktualisierungsmethode"](#) Für zusätzliche Verfahren.

Anforderungen

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

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

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

Informationen zu unterstützten Switches und Firmware-Versionen finden Sie im ["Hardware Universe"](#) oder im ["IMT"](#).

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

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

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

Folgende Beispielnamen werden in diesem Verfahren verwendet:

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

Was kommt als Nächstes?

["Aktivieren Sie die Konsolenprotokollierung"](#).

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

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

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

Was kommt als Nächstes?

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

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

Wenn Sie auf ein System aktualisieren, das in ONTAP 9.15.1 oder höher eingeführt wurde, müssen Sie normalerweise ein Bootarg auf den alten Controllern festlegen, bevor Sie mit dem Upgrade beginnen können.



Wenn Ihre Upgrade-Kombination betroffen ist, ist für ein erfolgreiches Upgrade das Festlegen eines Bootarg auf allen alten Controllern erforderlich. Lesen Sie die Informationen in diesem Abschnitt sorgfältig durch, um zu prüfen, ob für Ihre Upgrade-Kombination die Festlegung eines Bootargs erforderlich ist und wie Sie das richtige Bootarg für Ihre Kombination festlegen.

Schritt 1: Bestimmen Sie, ob Sie auf den alten Controllern ein Bootarg festlegen müssen

Bevor Sie mit dem Upgrade beginnen, bestimmen Sie anhand der folgenden Informationen, ob Sie auf den alten Controllern ein bootarg festlegen müssen:

- Sie **müssen** auf den alten Controllern ein Bootarg für unterstützte Upgrades auf die folgenden Systeme festlegen, sofern nicht anders angegeben:
 - AFF A70, AFF A90, AFF A1K
 - FAS70, FAS90
 - AFF C80
 - AFF A50, AFF A20, AFF A30
 - AFF C30, AFF C60
 - FAS50
- Sie müssen auf den alten Controllern **kein** Bootarg festlegen, wenn Ihr Upgrade eine der folgenden Kombinationen ist:
 - Von einem AFF A70 -System zu einem AFF A90 -System
 - Von einem FAS70-System zu einem FAS90-System



Wenn Sie für Ihr Upgrade kein Bootarg festlegen müssen, können Sie diese Aufgabe überspringen und direkt zu ["Bereiten Sie das System für das Upgrade vor"](#) .

Schritt 2: Bestimmen Sie das Bootarg, das Sie auf den alten Controllern einstellen müssen

Bei den meisten betroffenen Upgrades müssen Sie Folgendes einstellen:

`hw.cxgbe.toe_keepalive_disable` Bootarg auf den alten Controllern. Für bestimmte Upgrade-Pfade müssen Sie jedoch die `bootarg.siw.interop_enabled` bootarg stattdessen.

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

Für dieses Upgrade...	Bootarg festlegen...
Von AFF A250 nach AFF A30	<code>bootarg.siw.interop_enabled</code>
Von AFF C250 nach AFF C30	<code>bootarg.siw.interop_enabled</code>
Von AFF A150 nach AFF A20	<code>bootarg.siw.interop_enabled</code>
Von AFF A220 nach AFF A20	<code>bootarg.siw.interop_enabled</code>
Alle anderen Upgrades für AFF A70, AFF A90, AFF A1K, FAS70-, FAS90-, AFF C80-, AFF A50-, AFF A30-, AFF C30-, AFF C60- oder FAS50-Systeme	<code>hw.cxgbe.toe_keepalive_disable</code>
Hinweis: Sie müssen kein Bootarg festlegen, wenn Ihr Upgrade von einem AFF A70 auf ein AFF A90-System oder von einem FAS70- auf ein FAS90-System erfolgt.	

Schritt 3: Stellen Sie das erforderliche Bootarg auf den alten Controllern ein

Nachdem Sie das für Ihre Upgrade-Kombination erforderliche bootarg ermittelt haben, befolgen Sie die Schritte, um das bootarg auf den alten Controllern festzulegen.



Sie müssen das Bootarg auf allen alten Knoten an beiden Standorten festlegen, bevor Sie mit dem Upgrade beginnen.

Schritte

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

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

2. Stellen Sie den erforderlichen Bootarg für Ihre Upgrade-Kombination ein. Sie haben bereits den Bootarg festgelegt, den Sie mithilfe der Tabelle in festlegen müssen [Bestimmen Sie, welchen Bootarg Sie einstellen müssen](#).

hw.cxgbe.toe_keepalive_disable

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

```
setenv hw.cxgbe.toe_keepalive_disable 1  
  
saveenv  
  
printenv hw.cxgbe.toe_keepalive_disable
```

bootarg.siw.interop_enabled

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

```
setenv bootarg.siw.interop_enabled 1  
  
saveenv  
  
printenv bootarg.siw.interop_enabled
```

3. Booten des Node:

```
boot_ontap
```

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

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

5. Wiederholen Sie die Schritte für alle Nodes in der DR-Gruppe oder DR-Gruppen, die Sie aktualisieren.

Was kommt als Nächstes?

["Bereiten Sie das System für das Upgrade vor".](#)

Bereiten Sie das MetroCluster IP-System für das Upgrade vor

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

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

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

Über diese Aufgabe

Führen Sie diese Aufgabe unter folgenden Umständen aus:

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

Bevor Sie beginnen

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

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

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

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

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



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

Schritte

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

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



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

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

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

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

- ["Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"](#)

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

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

Über diese Aufgabe

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

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

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

Schritte

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

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

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

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

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

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

Schritte

1. Netzboot der neuen Controller:

- Auf das zugreifen "[NetApp Support Website](#)" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
- Laden Sie die entsprechende ONTAP Software im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.

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

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

```
_ontap-version_image.tgz
```

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

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

Wenn IP-Adresse...	Dann...
DHCP	Konfigurieren der automatischen Verbindung: <code>ifconfig e0M -auto</code>
Festgelegt	Konfigurieren Sie die manuelle Verbindung: <code>ifconfig e0M -addr=<i>ip_addr</i> - mask=<i>netmask</i> -gw=<i>gateway</i></code>

- e. Führen Sie den Netzboot aus.

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

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

Ignorieren Sie die folgende Meldung:

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

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

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

- b. Geben Sie ggf. den Benutzernamen und das Kennwort ein, oder drücken Sie die Eingabetaste, um fortzufahren.
- c. Eingeben `n` Überspringen Sie die Backup-Wiederherstellung, wenn Sie eine ähnliche Aufforderung wie die folgende sehen:

```
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} y
```



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

```
halt
```

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

```
set-defaults
```

3. Umgebung speichern:

```
saveenv
```

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

```
boot_ontap menu
```

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

```
wipeconfig
```

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

Überprüfen Sie vor Standort-Upgrade den MetroCluster-Zustand

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



Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

Schritte

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

- a. Prüfen Sie, ob die Knoten multipathed sind:

```
node run -node <node_name> sysconfig -a
```

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

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

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

- c. Überprüfen Sie auf Statusmeldungen:

```
system health alert show
```

Geben Sie diesen Befehl für jedes Cluster ein.

- d. Überprüfen Sie die Lizenzen auf den Clustern:

```
system license show
```

Geben Sie diesen Befehl für jedes Cluster ein.

- e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Geben Sie diesen Befehl für jedes Cluster ein.

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

```
cluster date show
```

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

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

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

```
metrocluster show
```

- b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:

```
metrocluster node show
```

c. Geben Sie den folgenden Befehl ein:

```
metrocluster check run
```

d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

3. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.

a. Laden Sie Config Advisor herunter und führen Sie sie aus.

["NetApp Downloads: Config Advisor"](#)

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

Sammeln Sie vor dem Upgrade Informationen

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

Schritte

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

Sammeln Sie die Ausgabe der folgenden Befehle für jeden Node:

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

- ° vol show -fields type
- ° vol show -fields type , space-guarantee
- ° vserver fcp initiator show
- ° storage disk show
- ° metrocluster configuration-settings interface show

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

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

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

Im folgenden Beispiel wird die Befehlsausgabe mit den UUIDs angezeigt:

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

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

Cluster oder Node	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Knoten_B_1	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Knoten_B_2	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039

Node_A_1	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

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

Sammeln Sie die Ausgabe der folgenden Befehle:

- ° `fcg adapter show -instance`
- ° `fcg interface show -instance`
- ° `iscsi interface show`
- ° `ucadmin show`

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

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

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

Weitere Informationen finden Sie unter "[Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement](#)".

- a. Wenn Onboard Key Manager konfiguriert ist:

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

Sie benötigen die Passphrase später im Upgrade-Verfahren.

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

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

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

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

Die folgende Ausgabe zeigt die neu zugewiesenen Laufwerke.

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

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

Entfernen Sie die Mediator- oder Tiebreaker-Überwachung

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

Schritte

1. Sammeln Sie die Ausgabe für den folgenden Befehl:

```
storage iscsi-initiator show
```

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

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

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

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

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

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

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

Der `maintenance-window-in-hours` Parameter gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

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

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

Was kommt als Nächstes?

["Wechseln Sie über die MetroCluster-Konfiguration".](#)

Upgrade Ihrer Controller

Wechseln Sie über die MetroCluster IP-Konfiguration

Sie schalten die Konfiguration auf Site_A um, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe:

- „Cluster_A“ ist aktiv und stellt Daten für beide Standorte bereit.
- Cluster_B ist inaktiv und bereit für den Upgrade-Prozess.

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
```

Die automatische Reparatur von Aggregaten nach der ausgehandelten Umschaltung ist während eines Controller-Upgrades deaktiviert.

Was kommt als Nächstes?

["Entfernen Sie die Schnittstellenkonfigurationen, und deinstallieren Sie die alten Controller"](#).

Entfernen Sie die Schnittstellenkonfigurationen, und deinstallieren Sie die alten MetroCluster IP-Controller

Überprüfen Sie die korrekte LIF-Platzierung. Entfernen Sie dann die VLANs und Schnittstellengruppen auf den alten Controllern und deinstallieren Sie die Controller physisch.

Über diese Aufgabe

- Diese Schritte führen Sie auf den alten Controllern aus (Node_B_1-old, Node_B_2-old).
- Sie benötigen die Informationen, die Sie für diesen Vorgang gesammelt ["Weisen Sie den neuen Nodes Ports von den alten Nodes zu"](#) haben.

Schritte

1. Booten der alten Nodes und melden Sie sich bei den Nodes an:

```
boot_ontap
```

2. Wenn das System, auf das Sie aktualisieren, **Shared Cluster/HA-Ports** verwendet, überprüfen Sie, ob die MetroCluster-IP-Schnittstellen unterstützte IP-Adressen verwenden.

Verwenden Sie die folgenden Informationen, um zu bestimmen, ob das neue System gemeinsam genutzte Cluster/HA-Ports verwendet:

Shared-Cluster-/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte Cluster-/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90

Shared-MetroCluster/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte MetroCluster/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

- a. Überprüfen Sie die IP-Adressen der MetroCluster-Schnittstellen auf den alten Controllern:

```
metrocluster configuration-settings interface show
```

- b. Wenn die MetroCluster-Schnittstellen 169.254.17.x- oder 169.254.18.x-IP-Adressen verwenden, finden Sie unter ["Der Knowledge Base-Artikel „Ändern der Eigenschaften einer MetroCluster IP-Schnittstelle“"](#)

Informationen zum Ändern der Schnittstellen-IP-Adressen, bevor Sie mit dem Upgrade fortfahren.



Ein Upgrade auf ein System mit **Shared Cluster/HA-Ports** wird nicht unterstützt, wenn die MetroCluster-Schnittstellen mit 169.254.17.x- oder 169.254.18.x-IP-Adressen konfiguriert sind.

3. Ändern Sie die Intercluster LIFs auf den alten Controllern, um einen anderen Home Port zu verwenden als die Ports, die für HA Interconnect oder MetroCluster IP DR Interconnect auf den neuen Controllern verwendet werden.



Dieser Schritt ist für ein erfolgreiches Upgrade erforderlich.

Die Intercluster LIFs auf den alten Controllern müssen einen anderen Home Port verwenden als die Ports, die für HA Interconnect oder MetroCluster IP DR Interconnect auf den neuen Controllern verwendet werden. Wenn Sie beispielsweise auf AFF A90 Controller aktualisieren, sind die HA Interconnect-Ports e1a und e7a und die MetroCluster IP DR Interconnect-Ports e2b und e3b. Sie müssen die Intercluster LIFs auf den alten Controllern verschieben, wenn sie auf den Ports e1a, e7a, e2b oder e3b gehostet werden.

Informationen zur Portverteilung und -Zuweisung auf den neuen Knoten finden Sie im "[Hardware Universe](#)".

- a. Sehen Sie sich auf den alten Controllern die Intercluster LIFs an:

```
network interface show -role intercluster
```

Je nachdem, ob die Intercluster LIFs auf den alten Controllern die gleichen Ports verwenden, wie die Ports für HA Interconnect oder den MetroCluster IP DR Interconnect auf den neuen Controllern.

Wenn die Intercluster LIFs...	Gehe zu...
Verwenden Sie denselben Home-Port	Unterschrift b
Verwenden Sie einen anderen Home-Port	Schritt 4

- b. Ändern Sie die Intercluster-LIFs so, dass sie einen anderen Home Port verwenden:

```
network interface modify -vserver <vserver> -lif <intercluster_lif> -home  
-port <port-not-used-for-ha-interconnect-or-mcc-ip-dr-interconnect-on-new-  
nodes>
```

- c. Überprüfen Sie, ob sich alle Intercluster LIFs an ihren neuen Home Ports befinden:

```
network interface show -role intercluster -is-home false
```

Die Befehlsausgabe sollte leer sein und bedeutet, dass sich alle Intercluster LIFs auf ihren jeweiligen Home Ports befinden.

- d. Zurücksetzen aller LIFs, die sich nicht auf ihrem Home Port befinden:

```
network interface revert -lif <intercluster_lif>
```

Wiederholen Sie den Befehl für jede Intercluster LIF, die sich nicht im Home Port befindet.

4. Zuweisen des Home-Ports aller Daten-LIFs auf dem alten Controller zu einem gemeinsamen Port, der

sowohl auf den alten als auch auf den neuen Controller-Modulen identisch ist.



Wenn die alten und neuen Controller keinen gemeinsamen Port haben, müssen Sie die Daten-LIFs nicht ändern. Überspringen Sie diesen Schritt und gehen Sie direkt zu [Schritt 5](#).

a. Anzeigen der LIFs:

```
network interface show
```

Alle Daten-LIFs wie SAN und NAS sind Administrator betriebsbereit und betriebsbereit, 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 für Plattformmodelle finden Sie im "[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
```

5. Ändern Sie Broadcast-Domänen, um das zu löschende VLAN und die physischen Ports zu entfernen:

```
broadcast-domain remove-ports -broadcast-domain <broadcast-domain-name> -ports <node-name:port-id>
```

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

6. 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 elc-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 ala -port e0d
```

a. VLAN- und Schnittstellengruppen-Ports aus der Broadcast-Domäne entfernen:

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

b. Ändern Sie die Schnittstellen-Gruppenanschlüsse, um andere physische Ports als Mitglied zu verwenden, falls erforderlich:

```
ifgrp add-port -node <node_name> -ifgrp <interface-group-name> -port <port-  
id>
```

7. Halten Sie die Nodes an der `LOADER` Eingabeaufforderung an:

```
halt -inhibit-takeover true
```

8. Stellen Sie an Standort_B eine Verbindung mit der seriellen Konsole der alten Controller (Node_B_1-old und Node_B_2-old) her, und überprüfen Sie, ob die Eingabeaufforderung angezeigt wird `LOADER`.

9. Ermitteln Sie die Bootarg-Werte:

```
printenv
```

10. Trennen Sie die Speicher- und Netzwerkverbindungen auf Node_B_1-old und Node_B_2-old. Beschriften Sie die Kabel, sodass Sie sie mit den neuen Nodes verbinden können.

11. Trennen Sie die Stromkabel von Node_B_1-old und Node_B_2-old.

12. Entfernen Sie die Controller Node_B_1-old und Node_B_2-old aus dem Rack.

Was kommt als Nächstes?

"Richten Sie die neuen Controller ein".

Richten Sie die neuen MetroCluster IP-Controller ein

Rack und Verkabelung der neuen MetroCluster IP-Controller

Schritte

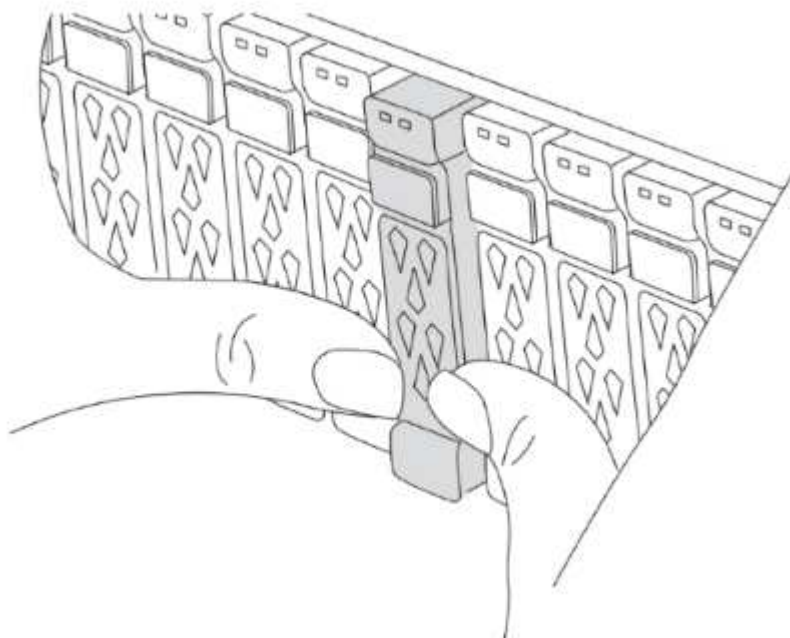
1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

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

2. Richtig gemahlen.

3. Wenn Ihr Upgrade den Austausch der Controller-Module erfordert, beispielsweise das Upgrade von einem AFF A800 auf ein AFF A90-System oder von einem AFF C800 auf ein AFF C80-System, müssen Sie das Controller-Modul aus dem Gehäuse entfernen, wenn Sie das Controller-Modul austauschen. Für alle anderen Upgrades fahren sie mit [Schritt 4](#) fort.

Drücken Sie auf der Vorderseite des Gehäuses die Daumen, um jedes Laufwerk fest einzuschieben, bis Sie einen positiven Stopp spüren. Dadurch wird bestätigt, dass die Laufwerke fest an der Mittelplatine des Gehäuses sitzen.



4. Installieren Sie die Controller-Module.

Welche Installationsschritte Sie durchführen, hängt davon ab, ob Ihr Upgrade den Austausch der Controller-Module erfordert oder ob IOM-Module zur Konvertierung der alten Controller in ein externes Shelf erforderlich sind.

Wenn Sie ein Upgrade durchführen...	Folgen Sie den Schritten für ...
• Ein AFF A150 auf ein AFF A20-System • Ein AFF A220 auf ein AFF A20-System	Konvertierung von Controller zu externem Shelf
• Ein AFF A800 auf ein AFF A90 System • Ein AFF C800 auf ein AFF C80-System • Ein AFF A250 zu einem AFF A30 System • Ein AFF C250 zu einem AFF C30 System • Ein AFF A70 zu einem AFF A90 System	Austausch des Controller-Moduls
Beliebige andere Kombinationen für Controller-Upgrades	Alle anderen Upgrades

Konvertierung von Controller zu externem Shelf

Bei ursprünglichen MetroCluster IP-Controllern handelt es sich um AFF A150- oder AFF A220-Modelle, können Sie das AFF A150 oder AFF A220 HA-Paar in ein DS224C Laufwerk-Shelf konvertieren und dann zu den neuen Nodes hinzufügen.

Wenn Sie beispielsweise ein Upgrade von einem AFF A150 oder AFF A220 System zu einem AFF A20 System durchführen, können Sie das AFF A150 oder AFF A220 HA-Paar in ein DS224C Shelf konvertieren, indem Sie die AFF A150 oder AFF A220 Controller-Module durch IOM12-Module austauschen.

Schritte

- a. Ersetzen Sie die Controller-Module im Node, den Sie mit IOM12 Shelf-Modulen konvertieren.

"Hardware Universe"

- b. Legen Sie die Festplatten-Shelf-ID fest.

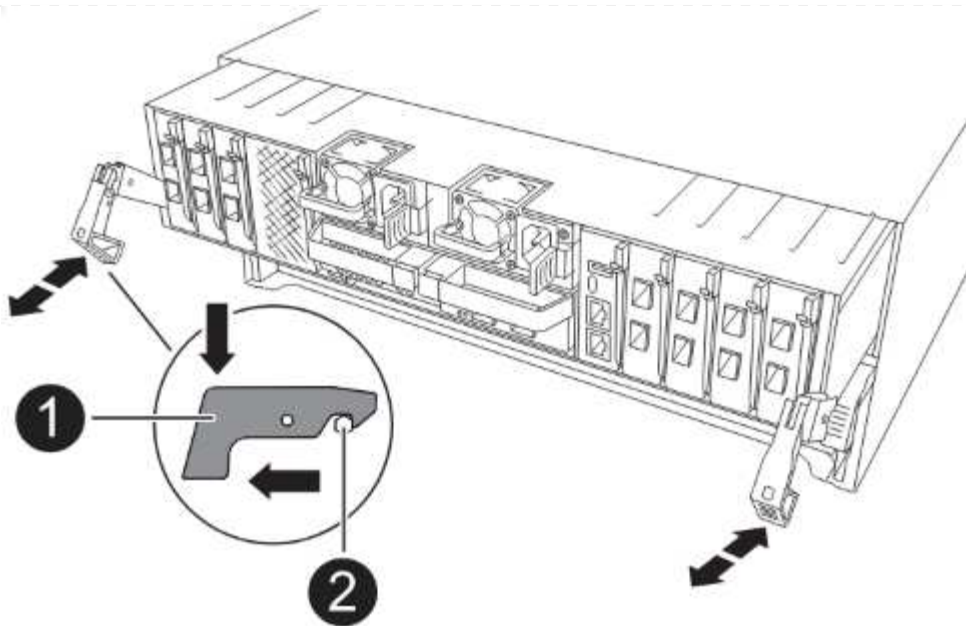
Jedes Festplatten-Shelf, einschließlich des Chassis, erfordert eine eindeutige ID.

- c. Setzen Sie andere Festplatten-Shelf-IDs bei Bedarf zurück.
- d. Schalten Sie die Shelves aus.
- e. Verkabeln Sie das umgewandelte Festplatten-Shelf mit einem SAS-Port auf dem neuen System und bei Verwendung von Out-of-Band-ACP-Verkabelung zum ACP-Port auf dem neuen Node.
- f. Schalten Sie das umgewandelte Laufwerk-Shelf und alle anderen an die neuen Nodes angeschlossenen Laufwerk-Shelves ein.
- g. Schalten Sie die neuen Nodes ein und unterbrechen Sie dann den Boot-Prozess auf jedem Node, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Austausch des Controller-Moduls

Die separate Installation der neuen Controller ist bei Upgrades integrierter Systeme mit Festplatten und Controllern im selben Chassis, beispielsweise von einem AFF A800 System auf ein AFF A90 System, nicht möglich. Sie müssen die neuen Controller-Module und I/O-Karten nach dem Ausschalten der alten Controller austauschen, wie in der Abbildung unten gezeigt.

Das folgende Beispielbild dient nur zur Darstellung. Die Controller-Module und E/A-Karten können zwischen den Systemen variieren.



Alle anderen Upgrades

Installieren Sie die Controller-Module im Rack oder Schrank.

5. Verkabeln Sie die Stromversorgungs-, seriellen Konsolen- und Managementverbindungen der Controller wie in beschrieben "[MetroCluster IP-Switches verkabeln](#)".

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

["Dokumentation zu ONTAP Hardwaresystemen"](#)

6. Starten Sie die neuen Nodes und starten Sie sie in den Wartungsmodus.

Was kommt als Nächstes?

["Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status fest"](#).

Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status des MetroCluster IP-Controllers und -Gehäuses fest

Konfigurieren Sie die HBA-Karten im Controller-Modul, und überprüfen und legen Sie den HA-Status des Controllers und des Gehäuses fest.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration von HBA-Karten im Controller-Modul müssen Sie sie für Ihren Standort korrekt 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 Porteeinstellungen nach Bedarf.

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

2. Beenden des Wartungsmodus:

```
halt
```

Warten Sie nach dem Ausführen des Befehls, bis der Node an der Eingabeaufforderung angehalten `LOADER` wird.

3. Booten Sie den Node wieder im Wartungsmodus, um die Konfigurationsänderungen anzuwenden:

```
boot_ontap maint
```

4. Überprüfen Sie die Änderungen:

Wenn Sie über diese Art von HBA verfügen...	Befehl
CNA	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

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 Systemstatus des Controllers oder Chassis nicht korrekt ist, legen Sie den HA-Status fest:

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

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

3. Überprüfen und ändern Sie die Ethernet-Ports, die mit NS224-Shelfs oder Speicher-Switches verbunden sind.

- a. Überprüfen Sie die Ethernet-Ports, die mit NS224-Shelfs oder Speicher-Switches verbunden sind:

```
storage port show
```

- b. Setzen Sie alle mit Ethernet-Shelfs oder Storage-Switches verbundenen Ethernet-Ports, einschließlich gemeinsam genutzter Switches für Storage und Cluster, auf den `storage` Modus:

```
storage port modify -p <port> -m storage
```

Beispiel:

```
*> storage port modify -p e5b -m storage
Changing NVMe-oF port e5b to storage mode
```



Dies muss für alle betroffenen Ports festgelegt werden, damit ein Upgrade erfolgreich durchgeführt werden kann.

Festplatten aus den an die Ethernet-Ports angeschlossenen Shelfs werden in der Ausgabe gemeldet `sysconfig -v`.

Informationen zu den Speicherports für das System, auf das Sie aktualisieren, finden Sie im ["Hardware Universe"](#).

- a. Überprüfen Sie, ob `storage` der Modus festgelegt ist, und vergewissern Sie sich, dass die Ports den Status „Online“ aufweisen:

```
storage port show
```

4. Stoppen Sie den Knoten: `halt`

Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

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

Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers

Wenn Sie ein Upgrade von einem System mit ausschließlich externen Laufwerken auf ein System mit externen und internen Laufwerken (Festplatten und Controller im selben Gehäuse) durchführen, müssen Sie alle internen Laufwerke aus dem neuen System entfernen oder ausbauen, bis Sie das Upgrade abgeschlossen haben.



Diese Aufgabe ist für ein erfolgreiches Controller-Upgrade auf betroffenen Systemen zwingend erforderlich.

1. Wenn Ihre Upgrade-Kombination mit **Hinweis 3** gekennzeichnet ist, müssen Sie die internen Laufwerke aus dem neuen System entfernen oder aus dem Sitz lösen

Nach Abschluss dieser Aufgabe sollten keine internen Laufwerke mehr zugänglich sein. Sie fügen die Laufwerke später im Verfahren zum neuen Controller hinzu.

Was kommt als Nächstes?

["Aktualisieren Sie die Switch-RCFs und legen Sie die MetroCluster IP-Bootarg-Werte fest"](#).

Aktualisieren Sie die Switch-RCFs und legen Sie die MetroCluster IP-Bootarg-Werte fest

Aktualisieren Sie die Switch-Referenzkonfigurationsdateien (RCFs) für die neuen Plattformen und legen Sie die MetroCluster IP-Bootarg-Werte auf den Controller-Modulen fest.

Aktualisieren Sie die Switch-RCFs, 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-Switches auf die Anwendung der neuen RCFs vor.

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

- ["Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"](#)

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

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

- ["Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"](#)

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

Sie müssen bestimmte MetroCluster IP-Bootarg-Werte auf den neuen Controller-Modulen konfigurieren. Die bootarg-Werte müssen mit denen übereinstimmen, die auf den alten Controller-Modulen konfiguriert sind.

Über diese Aufgabe

- Sie verwenden die UUIDs und System-IDs, die zuvor im Upgrade-Verfahren angegeben ["Sammeln Sie vor dem Upgrade Informationen"](#) wurden.
- Je nach Plattformmodell können Sie die VLAN-ID mit dem Parameter angeben `-vlan-id`. Die folgenden Plattformen unterstützen den Parameter nicht `-vlan-id`:
 - FAS8200 UND AFF A300
 - AFF A320
 - FAS9000 und AFF A700
 - AFF C800, ASA C800, AFF A800 und ASA A800

Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.

- Die von Ihnen festgelegten MetroCluster Bootarg-Werte hängen davon ab, ob Ihr neues System gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet.

Shared-Cluster-/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte Cluster-/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90

Shared-MetroCluster/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte MetroCluster/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

Schritte

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

Die Schritte, die Sie befolgen, hängen von den Ports ab, die vom neuen Plattformmodell verwendet werden.

Systeme, die Shared Cluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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



Wenn die Schnittstellen eine Standard-VLAN-ID verwenden, ist der `vlan-id` Parameter nicht erforderlich.

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

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

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

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

Im folgenden Beispiel werden die Werte für Node_B_1-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen festgelegt:

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

Im folgenden Beispiel werden die Werte für Node_B_2-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen festgelegt:

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

Systeme, die gemeinsam genutzte MetroCluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs 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 eine Standard-VLAN-ID verwenden, ist der `vlan-id` Parameter nicht erforderlich.

Im folgenden Beispiel werden die Werte für Node_B_1-New 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-New 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
```

Im folgenden Beispiel werden die Werte für Node_B_1-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen 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
```

Im folgenden Beispiel werden die Werte für Node_B_2-New mithilfe von Standard-VLANs für alle MetroCluster IP DR-Verbindungen 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
```

2. Legen Sie an DER LOADER-Eingabeaufforderung der neuen Nodes die UUIDs 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
```

3. Bestimmen Sie, ob die ursprünglichen Systeme für die erweiterte Laufwerkpartitionierung (Advanced Drive Partitioning, ADP) konfiguriert wurden, indem Sie den folgenden Befehl vom Standort aus ausführen:

disk show

In der Spalte „Containertyp“ wird in der Ausgabe „freigegeben“ angezeigt `disk show`, wenn ADP konfiguriert ist. Wenn „Containertyp“ einen anderen Wert hat, ist ADP auf dem System nicht konfiguriert. Die folgende Beispielausgabe zeigt ein mit ADP konfiguriertes System:

```
::> disk show
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
Info: This cluster has partitioned disks. To get a complete list of spare disk capacity use "storage aggregate show-spare-disks".						
1.11.0 node_A_1	894.0GB	11	0	SSD	shared	testaggr
1.11.1 node_A_1	894.0GB	11	1	SSD	shared	testaggr
1.11.2 node_A_1	894.0GB	11	2	SSD	shared	testaggr

4. Wenn die ursprünglichen Systeme mit partitionierten Laufwerken für ADP konfiguriert wurden, aktivieren Sie diese an der `LOADER` Eingabeaufforderung für jeden Ersatz-Node:

```
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
```

Was kommt als Nächstes?

"[Weisen Sie die Root-Aggregat-Festplatten neu zu](#)".

Weisen Sie die Festplatten des Root-Aggregats dem neuen MetroCluster IP-Controller-Modul neu zu

Weisen Sie die Festplatten des Stammaggregats dem neuen Controller-Modul mithilfe der zuvor zusammengefassten System-IDs neu zu.

Über diese Aufgabe

Die alten System-IDs wurden in identifiziert "[Sammeln Sie vor dem Upgrade Informationen](#)".

Sie führen die Schritte im Wartungsmodus aus.



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
```



Bevor Sie mit der Neuzuweisung der Festplatte fortfahren, überprüfen Sie, ob die zum Root-Aggregat des Node gehörenden Pool0- und Pool1-Festplatten in der Ausgabe angezeigt werden `disk show`. Im folgenden Beispiel werden in der Ausgabe die Laufwerke pool0 und pool1 aufgelistet, die sich im Besitz von Node_B_1-old befinden.

Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Die alte System-ID (537403322) besitzt jedoch immer noch die Root-Aggregat-Festplatten. Dieses Beispiel zeigt keine Laufwerke an, die anderen Nodes in der MetroCluster-Konfiguration gehören.

```

*> 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)  Pool10 S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3   node_B_1-old(537403322)  Pool10 S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27  node_B_1-old(537403322)  Pool10 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.	<code>disk reassign -s <old-sysid> -d <new-sysid> -r <dr-partner-sysid></code>
Nein	<code>disk reassign -s <old-sysid> -d <new-sysid></code>

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 wurden:

```
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	

Was kommt als Nächstes?

"Booten der neuen Controller und Wiederherstellen der LIF-Konfiguration".

Starten Sie die neuen MetroCluster IP-Controller und stellen Sie die LIF-Konfiguration wieder her

Starten Sie die neuen Controller und überprüfen Sie, ob LIFs auf entsprechenden Nodes und Ports gehostet werden.

Starten Sie die 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.



Bei Option 6 wird der Knoten zweimal neu gebootet, bevor der Vorgang abgeschlossen ist.

Reagieren Sie mit „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 an der `LOADER` Eingabeaufforderung die Bootarg-Werte, und aktualisieren Sie die Werte bei Bedarf.

Verwenden Sie die Schritte in ["Legen Sie die MetroCluster-IP-Bootarg-Variablen fest"](#).

8. Überprüfen Sie, 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 ausgetauschten Nodes gebootet werden.

Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben 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	<pre>security key-manager onboard sync</pre> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	<pre>`security key-manager external restore -vserver <SVM> -node <node> -key-server <host_name</pre>

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

a. Broadcast-Domänen anzeigen:

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

b. Wenn für die Datenports auf den neu aktualisierten Controllern eine neue Broadcast-Domäne erstellt wird, löschen Sie die Broadcast-Domäne:



Löschen Sie nur die neue Broadcast-Domäne. Löschen Sie keine der Broadcast-Domänen, die vor dem Start des Upgrades vorhanden waren.

```
broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

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

["Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"](#)

d. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

Die Mitgliedschaft in VLAN und Schnittstellengruppen kann sich vom alten Knoten unterscheiden.

["Erstellen Sie eine VLAN"](#)

["Kombinieren Sie physische Ports, um Schnittstellengruppen zu erstellen"](#)

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 ["Weisen Sie den neuen Nodes Ports von den alten Nodes zu"](#), den Sie in erstellt haben.



Sie müssen vor dem Wechsel zurück überprüfen, ob die Daten-LIFs auf den neuen Nodes korrekt sind. Wenn Sie die Konfiguration zurückschalten, versucht ONTAP, den Datenverkehr auf dem von den LIFs verwendeten Home Port wiederaufzunehmen. E/A-Fehler können auftreten, wenn die Verbindung des Home-Ports zum Switch-Port und VLAN falsch ist.

Schritte

1. Vergewissern Sie sich vor dem Switchback, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

- a. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

- b. Zeigen Sie die LIFs an und vergewissern Sie sich, dass jede Daten-LIF den richtigen Home Port verwendet:

```
network interface show
```

- c. Ändern Sie alle LIFs, die nicht den korrekten Home Port verwenden:

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

Wenn der Befehl einen Fehler zurückgibt, können Sie die Portkonfiguration überschreiben:

```
vserver config override -command "network interface modify -vserver <svm-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. Vergewissern Sie sich, dass alle Daten-LIFs nun am richtigen Home Port sind:

```
network interface show
```

- b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

```
network interface revert * -vserver <svm-name>
```

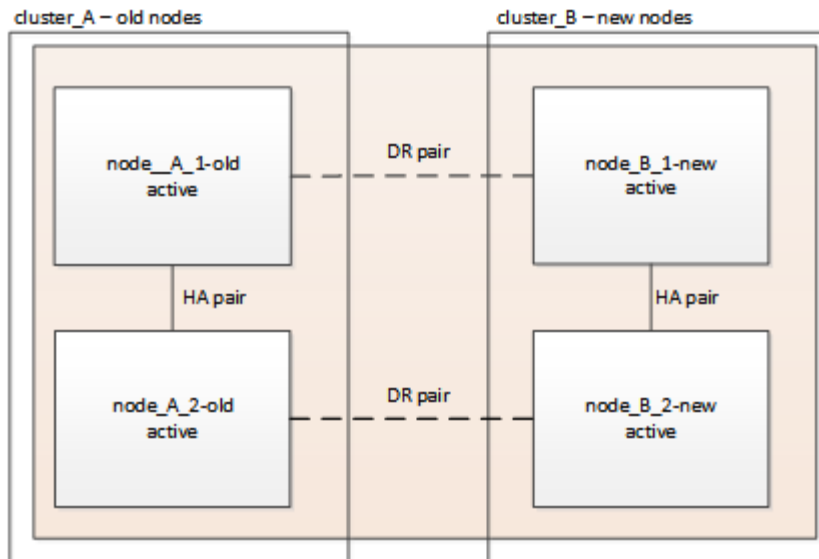
Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Was kommt als Nächstes?

["Umschalten der MetroCluster-Konfiguration"](#).

Schalten Sie die MetroCluster IP-Konfiguration zurück

Führen Sie den Switchback-Vorgang durch, um die MetroCluster-Konfiguration wieder in den normalen Betrieb zu bringen. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das `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 Umschaltvorgang 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.

Was kommt als Nächstes?

"Schließen Sie das Upgrade ab".

Schließen Sie das MetroCluster IP-Controller-Upgrade ab

Führen Sie nach dem Upgrade der Controller-Module die erforderlichen Aufgaben aus, um das Controller-Upgrade abzuschließen.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

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

Über diese Aufgabe

Sie können diese Aufgabe auf jedem beliebigen Knoten in der MetroCluster-Konfiguration ausführen.

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 Nodes auf Cluster_A

Sie müssen die Upgrade-Tasks wiederholen, um die Nodes auf „Cluster_A“ an Standort A zu aktualisieren

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit ["Bereiten Sie sich auf das Upgrade vor"](#).

Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

Fügen Sie die internen Laufwerke erneut zum neuen Controller hinzu

Wenn Sie ein System mit ausschließlich externen Laufwerken auf ein System mit externen und internen Laufwerken (Festplatten und Controller im selben Gehäuse) aktualisiert haben, können Sie die aus den internen Steckplätzen des neuen Systems entfernten oder entfernten Festplatten hinzufügen oder neu einsetzen. Dies ist jederzeit möglich, nachdem das Upgrade an beiden Standorten abgeschlossen ist und der Cluster fehlerfrei ist.

Nachdem Sie die Laufwerke erneut hinzugefügt oder neu eingesetzt haben, können sie nach Bedarf in ONTAP verwendet werden.



Diese Aufgabe gilt nur für bestimmte Upgrade-Kombinationen. Weitere Informationen finden Sie unter ["Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers"](#).

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	"Fügen Sie MetroCluster-Konfigurationen hinzu" .
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-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.

Konfigurieren Sie die End-to-End-Verschlüsselung

Falls es von Ihrem System unterstützt wird, können Sie zwischen den MetroCluster IP-Standorten den Back-End-Verkehr, wie NVLOG- und Storage-Replizierungsdaten, verschlüsseln. Siehe ["Konfigurieren Sie die End-to-End-Verschlüsselung"](#) Finden Sie weitere Informationen.

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

Aktivieren Sie die Konsolenprotokollierung

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

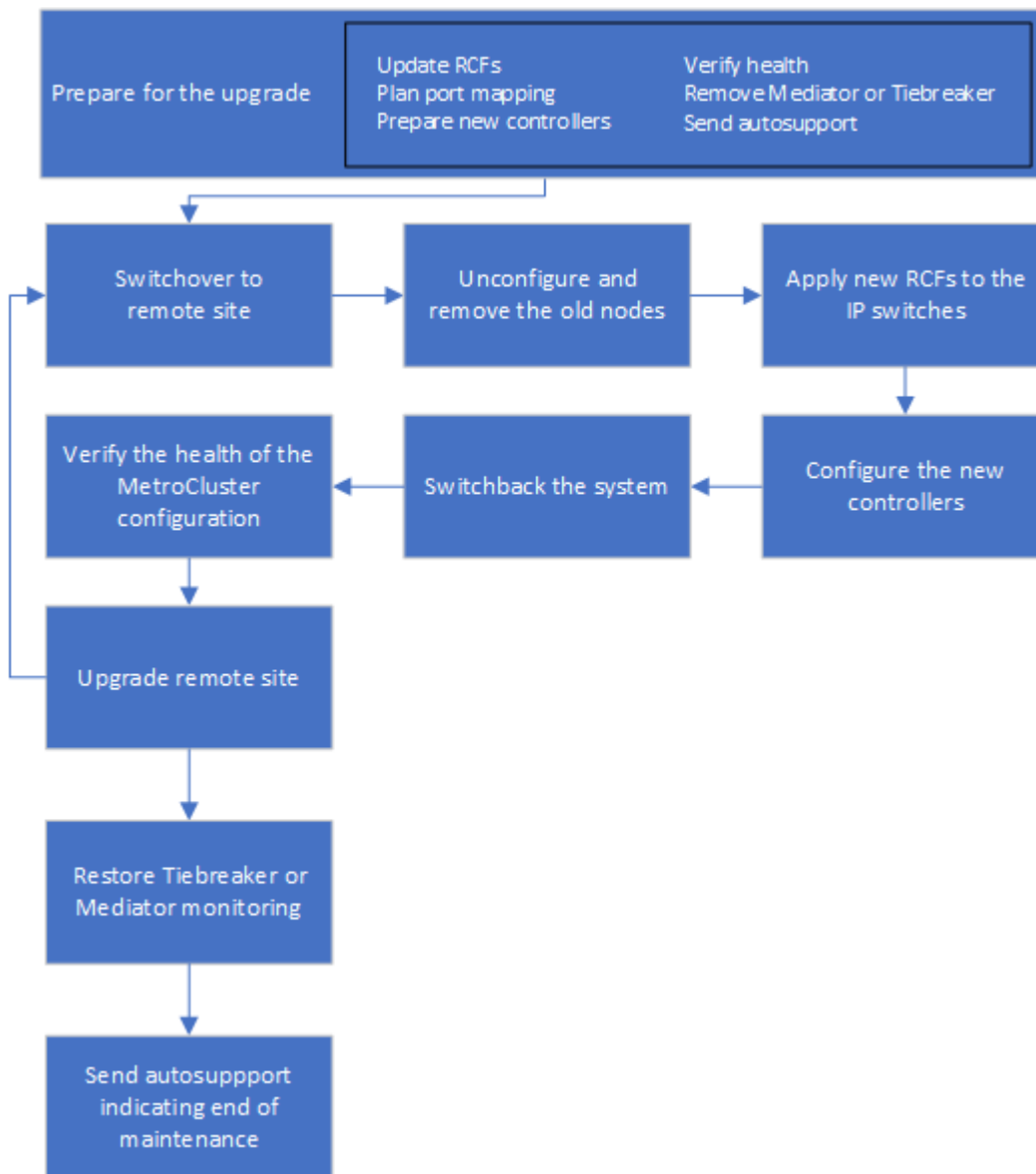
- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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.

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

- ["Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den NVIDIA IP-Switch auf die Werkseinstellungen zurück"](#)

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

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

- ["Laden Sie die Broadcom RCF-Dateien herunter, und installieren Sie sie"](#)
- ["Laden Sie die Cisco IP RCF-Dateien herunter, und installieren Sie sie"](#)
- ["Laden Sie die NVIDIA IP RCF-Dateien herunter, und installieren Sie sie"](#)

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

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



Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

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 zugewiesenen 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" im <i>MetroCluster Tiebreaker Installations- und Konfigurationsinhalt</i>
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: <pre>metrocluster configuration-settings mediator remove</pre>
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.

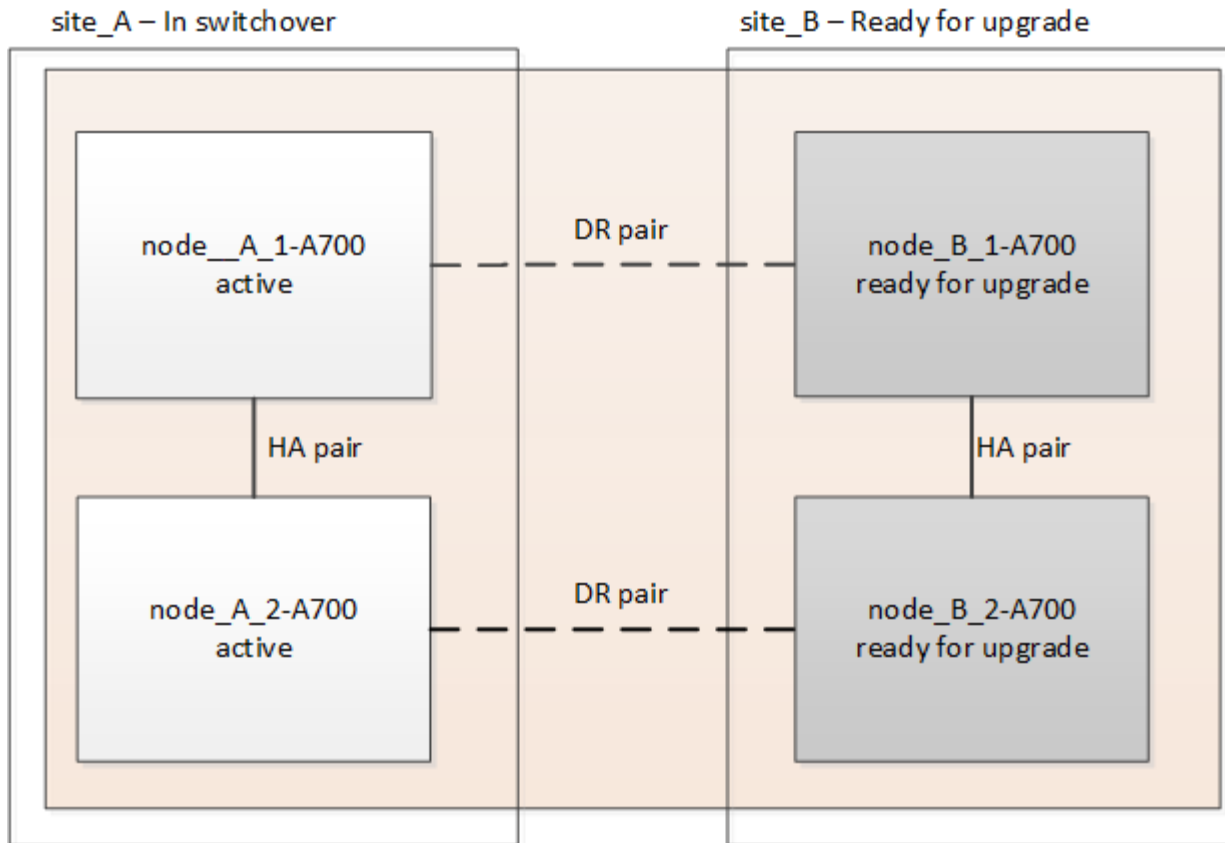
Wechseln Sie über die MetroCluster-Konfiguration

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

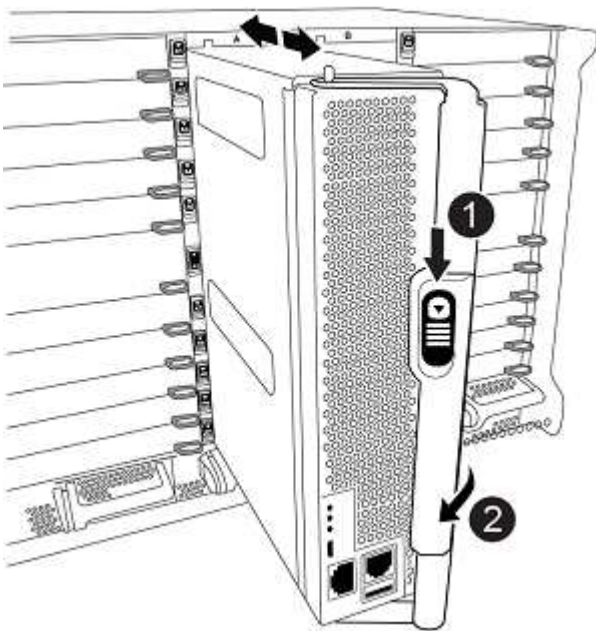
1. Ermitteln Sie die Bootarg-Werte von beiden Knoten an Site_B: `printenv`
2. Schalten Sie das Chassis an Site_B. aus

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.



	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.

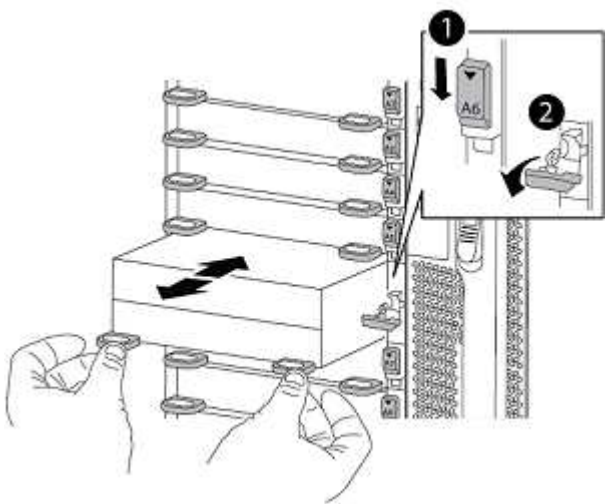
Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

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

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

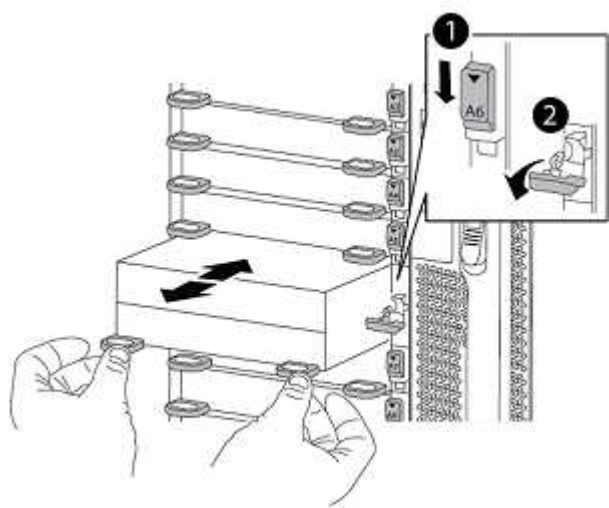
Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

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.

	Freigabetaste für den CAM-Griff
	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 im Abschnitt beschrieben. [Weisen Sie den neuen Nodes Ports von den alten Nodes zu](#)

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: <code>ifconfig e0M -auto</code>
Nicht Ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: <code>ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain></code> <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 <code>help ifconfig</code> 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. Eingeben `n` Um die Wiederherstellung der Sicherung zu überspringen, wenn die folgende Aufforderung angezeigt wird:

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

- b. Eingeben `y` Starten Sie das System neu, wenn die folgende Aufforderung angezeigt wird:

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

Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

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 Porteeinstellungen nach Bedarf.

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

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	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

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-Switches auf die Anwendung der neuen RCFs vor.

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

- ["Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"](#)
- ["Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"](#)

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

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

- ["Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"](#)
- ["Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"](#)

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 zuvor im Upgrade-Verfahren identifiziert wurden [Sammeln Sie vor dem Upgrade Informationen](#).

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, UUIDs 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)  Pool11  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool11  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21  node_B_1-A700(537403322)  Pool11  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2   node_B_1-A700(537403322)  Pool10  SOM1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3   node_B_1-A700(537403322)  Pool10  SOM0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27  node_B_1-A700(537403322)  Pool10  SOM1PSDW
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.	<code>disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid</code>
Nein	<code>disk reassign -s old-sysid -d new-sysid</code>

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 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	<code>security key-manager onboard sync</code> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement" .
Externes Verschlüsselungskeymanagement	<code>`security key-manager external restore -vserver SVM -node <i>node</i> -key-server <i>_host_name</i></code>

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 in erstellten Port-Mapping-Plan an [Weisen Sie den neuen Nodes Ports von den alten Nodes zu](#)

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
```

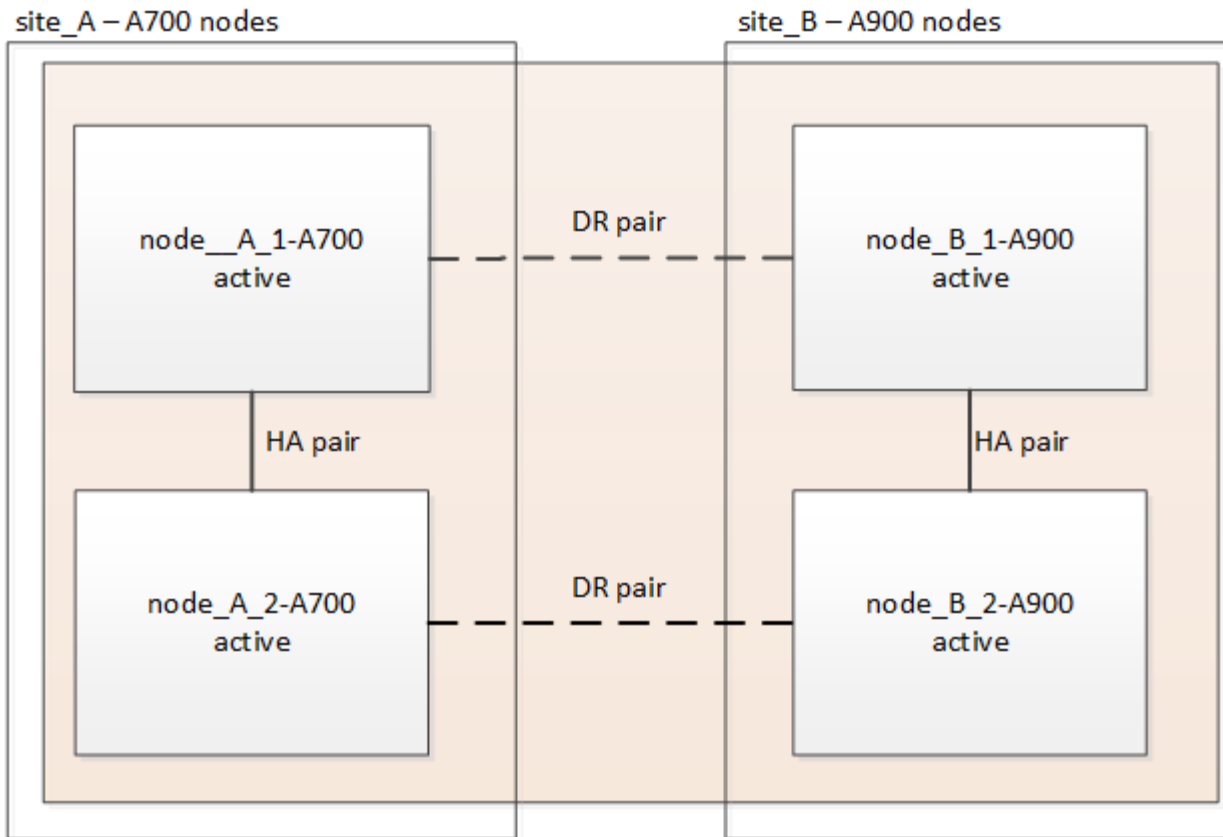
2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

```
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

- Stellen Sie das aus `metrocluster node show` Führen Sie den Befehl von Site_B aus, und überprüfen Sie die Ausgabe.
 - Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
 - Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
- 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).
 - Heilen Sie die Datenaggregate:

```
metrocluster heal aggregates
```
 - Heilen Sie die Root-Aggregate:

```
metrocluster heal root
```
 - Zurückwechseln des Clusters:

```
metrocluster switchback
```
- 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 Umschaltvorgang 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

- Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
 - Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
`metrocluster show`
 - Führen Sie eine MetroCluster-Prüfung durch:
`metrocluster check run`
 - Ergebnisse der MetroCluster-Prüfung anzeigen:
`metrocluster check show`
- 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 Site_A zu aktualisieren, beginnend 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 <i>MetroCluster Tiebreaker Installation und Konfiguration</i> .
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" im Abschnitt <i>MetroCluster IP-Installation und -Konfiguration</i> .
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 Sie Controller in einer MetroCluster FC Konfiguration mithilfe von 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 Shelves 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

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren

und folgende Aktionen durchzuführen:

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

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



Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

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.

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

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 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. Erstellen Sie nach dem Upgrade die Clusterports neu. "Bereiten Sie Cluster-Ports auf einem vorhandenen Controller-Modul vor"
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 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. 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 Passphrasen.

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.

"MetroCluster-Konfigurationen entfernen"

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.

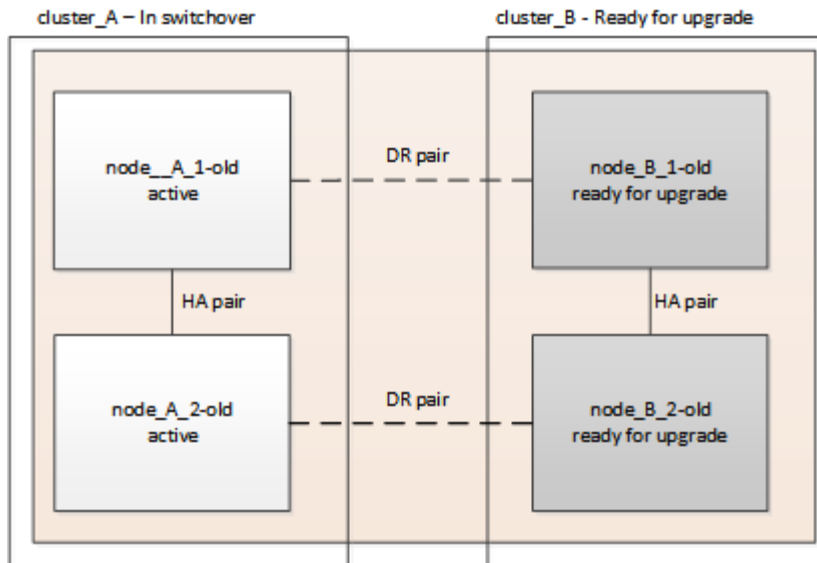
Wechseln Sie über die MetroCluster-Konfiguration

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 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 elc-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 ala -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 Sie die 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 Sie die 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.

Richten Sie die neuen Controller ein

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-Shelves 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.

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

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 <code>ontap-Version_image.tgz</code> file in das Zielverzeichnis: <code>Tar -zxvf ontap-Version_image.tgz</code> 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: <code>Netzboot/Kernel</code> enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: <code>ontap-Version_image.tgz</code> Sie müssen nicht die <code>ontap-Version_image.tgz</code> -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. Eingeben n Überspringen Sie die Backup-Wiederherstellung, wenn Sie eine ähnliche Aufforderung wie die folgende sehen:

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



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

```
halt
```

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

```
set-defaults
```

3. Umgebung speichern:

```
saveenv
```

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

```
boot_ontap menu
```

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

```
wipeconfig
```

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

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 Porteeinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen...	Befehl
CNA FC	<code>ucadmin modify -m fc -t initiator <i>adapter-name</i></code>

CNA-Ethernet	<code>ucadmin modify -mode cna adapter-name</code>
FC-Ziel	<code>fcadmin config -t target adapter-name</code>
FC-Initiator	<code>fcadmin config -t initiator adapter-name</code>

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	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

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	<code>mcc-2n</code>
Vier oder acht Nodes	<code>mcc</code>

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	<pre>ha-config modify controller mcc-2n ha-config modify chassis mcc-2n</pre>
Vier oder acht Knoten	<pre>ha-config modify controller mcc ha-config modify chassis mcc</pre>

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 Sie vor dem Upgrade Informationen](#)".

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)	Pool11	PZHYN0MD	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:9.126L49	node_B_1-old(4068741254)	Pool11	PPG3J5HA	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L21	node_B_1-old(4068741254)	Pool11	PZHTDSZD	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L2	node_B_1-old(4068741254)	Pool10	S0M1J2CF	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:8.126L3	node_B_1-old(4068741254)	Pool10	S0M0CQM5	
	node_B_1-old(4068741254)		node_B_1-old(4068741254)	
rr18:9.126L27	node_B_1-old(4068741254)	Pool10	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	<code>recover_onboard_keymanager</code>
Externes Verschlüsselungskeymanagement	<code>recover_external_keymanager</code>

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	<code>recover_onboard_keymanager</code>
Externes Verschlüsselungskeymanagement	<code>recover_external_keymanager</code>

Möglicherweise müssen Sie die ausgegeben `recover_XXXXXXX_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 Sie eine VLAN"](#)

["Kombinieren Sie physische 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	<pre>security key-manager onboard sync</pre> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	<pre>`security key-manager external restore -vserver SVM -node node -key-server _host_name`</pre>

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.

Installieren Sie die neuen Lizenzen

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

Schritte

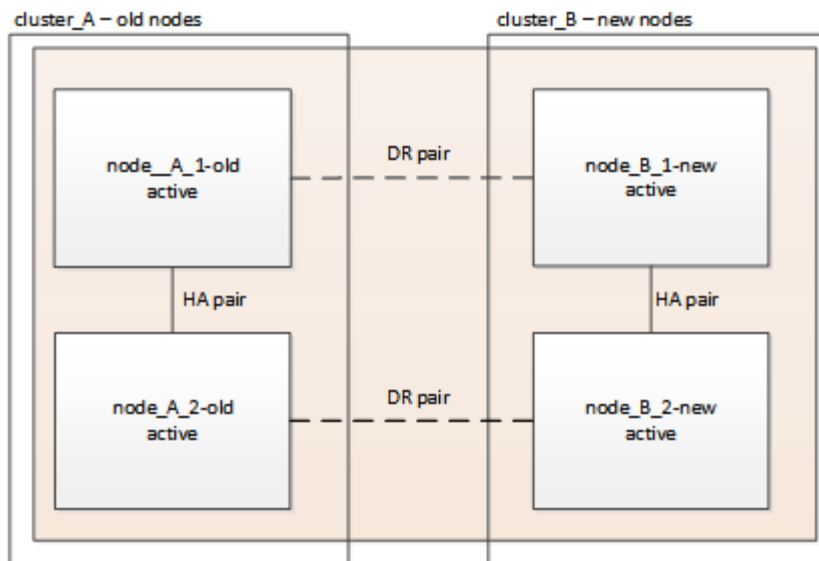
1. ["Installieren von Lizenzen für das neue Controller-Modul"](#)

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.



Schritte

1. Stellen Sie das `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 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 Sie die Nodes auf Cluster_A

Sie müssen die Upgrade-Aufgaben auf „Cluster_A“ wiederholen

Schritt

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit ["Bereiten Sie sich auf das Upgrade vor"](#).

Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

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 in ["Fügen Sie MetroCluster-Konfigurationen hinzu"](#) in *Installation und Konfiguration des MetroCluster-Tiebreakers*.

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 Shelves 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

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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.



Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

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 Zustandswarmmeldungen 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.

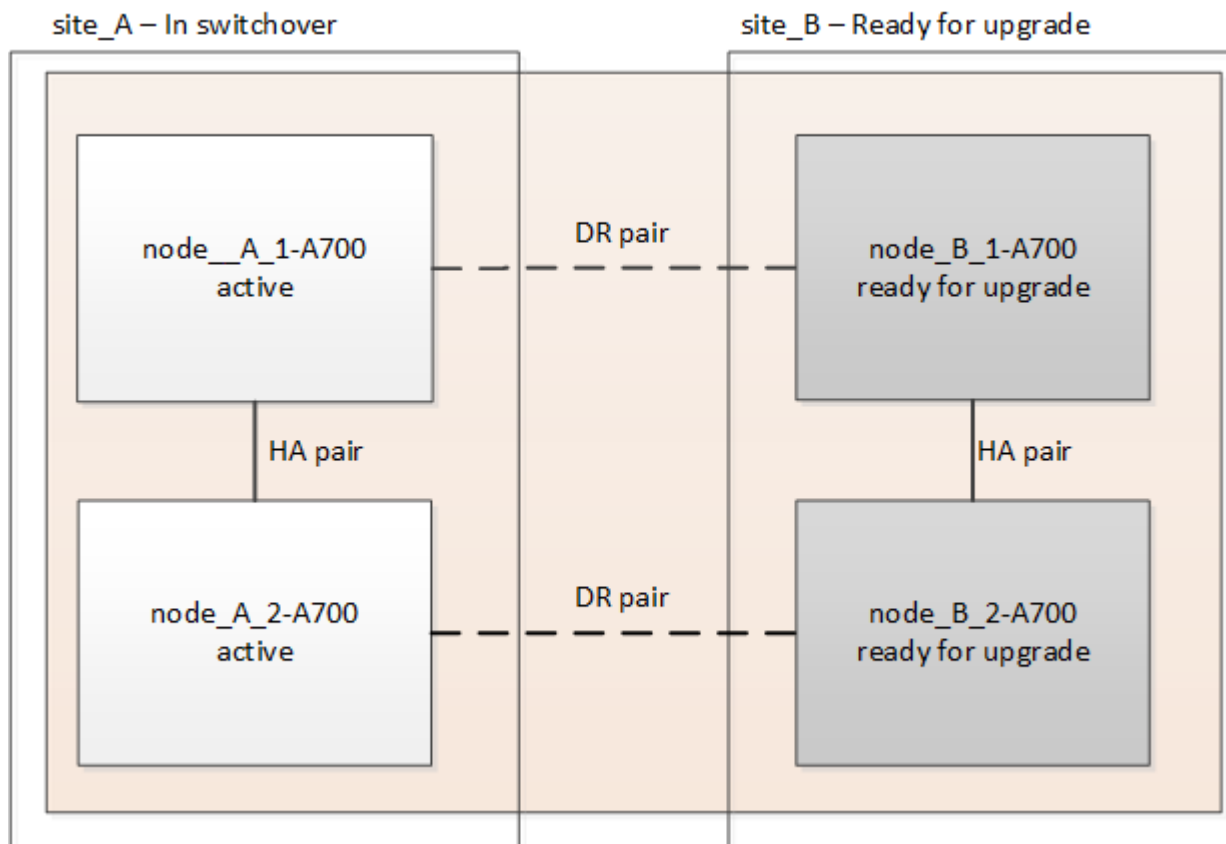
Wechseln Sie über die MetroCluster-Konfiguration

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

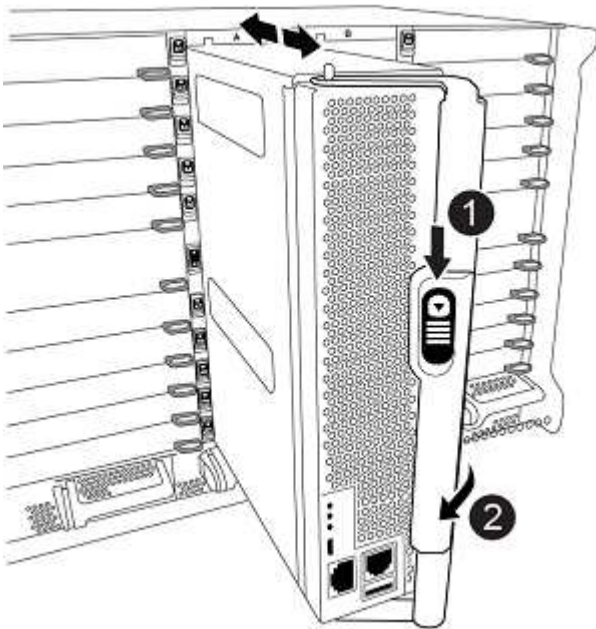
Entfernen Sie das Controller-Modul und den NVS von beiden Nodes an Site_B

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.

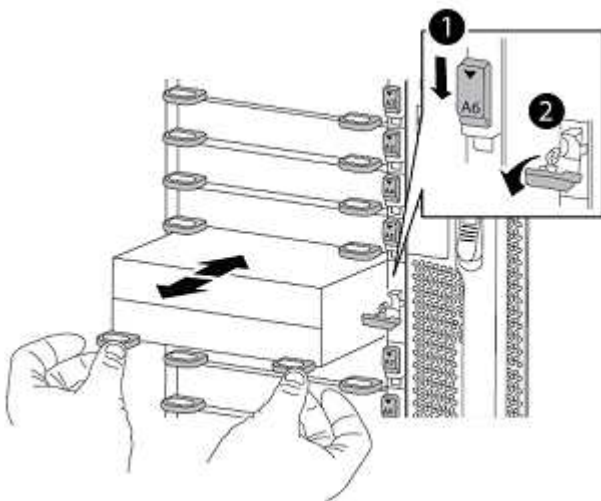
Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

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

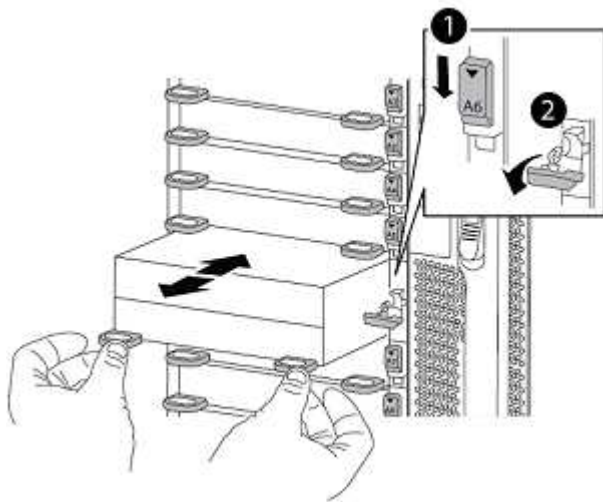
Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

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.

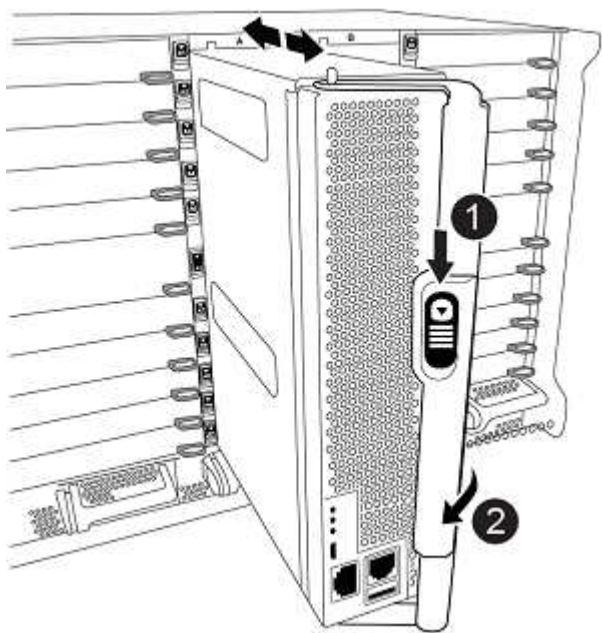
Schritte

- 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.



	Freigabetaste für den CAM-Griff
	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 heruntergeladen ["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: <code>ifconfig e0M -auto</code>

Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: <code>ifconfig e0M</code> <pre>-addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain></pre> <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 <code>ifconfig</code> 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. Eingeben `n` Um die Wiederherstellung der Sicherung zu überspringen, wenn die folgende Aufforderung angezeigt wird:

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

- b. Eingeben `y` Starten Sie das System neu, wenn die folgende Aufforderung angezeigt wird:

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

Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

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	<code>ucadmin modify -m fc -t initiator <i>adapter-name</i></code>
CNA-Ethernet	<code>ucadmin modify -mode cna <i>adapter-name</i></code>
FC-Ziel	<code>fcadmin config -t target <i>adapter-name</i></code>
FC-Initiator	<code>fcadmin config -t initiator <i>adapter-name</i></code>

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	<code>mcc-2n</code>
Vier oder acht Nodes	<code>mcc</code>

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	<pre>ha-config modify controller mcc-2n ha-config modify chassis mcc-2n</pre>
Vier oder acht Knoten	<pre>ha-config modify controller mcc ha-config modify chassis mcc</pre>

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  SOM1J2CF
node_B_1-A900(1574774970) node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)  Pool0  SOM0CQM5
node_B_1-A900(1574774970) node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)  Pool0  SOM1PSDW
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_XXXXXXX_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	<pre>security key-manager onboard sync</pre> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	<pre>`security key-manager external restore -vserver SVM -node node -key-server _host_name</pre>

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
```

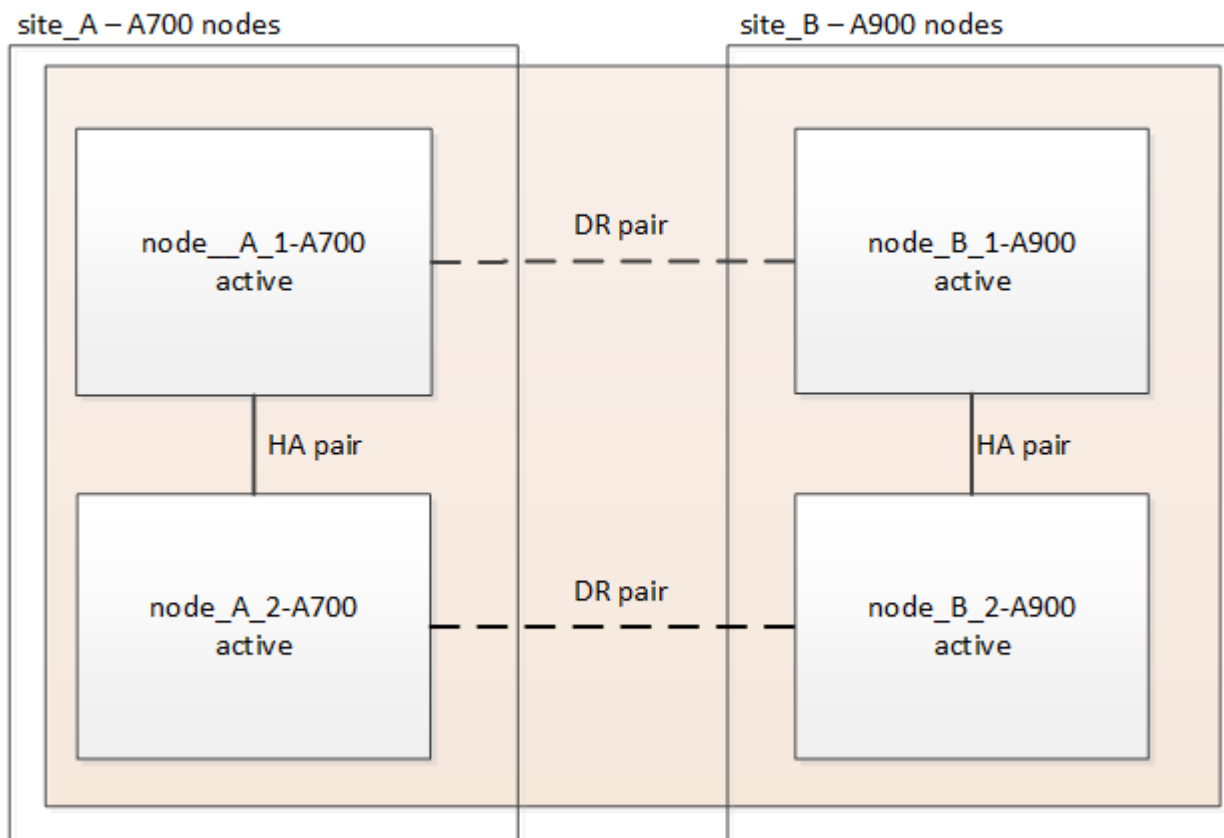
Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

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. Befolgen Sie die folgenden Schritte: ["Hinzufügen von MetroCluster Konfigurationen"](#) im Abschnitt *MetroCluster Tiebreaker Installation und Konfiguration*.

Aktualisieren Sie Controller in einer MetroCluster FC-Konfiguration mit vier Knoten mithilfe von Switchover und Switchback mit den Befehlen „System Controller Replace“ (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"](#).

Weitere Verfahren finden Sie unter ["Wählen Sie eine Upgrade- oder Aktualisierungsmethode aus"](#).

Über diese Aufgabe

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

Andere Komponenten in der Konfiguration, wie z. B. Storage Shelves 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

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

Bereiten Sie sich auf das Upgrade vor

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. Führen Sie den folgenden Befehl von Standort A aus, um die Controller an Standort B zu ersetzen:

```
system controller replace start
```



- Wenn Sie den Vorgang an einem Standort wiederholen, nachdem Sie die Controller am anderen Standort bereits ausgetauscht haben, tritt aufgrund einer Nichtübereinstimmung der Knoten an beiden Standorten ein Fehler auf. Dies ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind.

Wenn nur der Fehler „Mismatch“ zurückgegeben wird, können Sie die `-skip-metrocluster-check true` Option mit der `system controller replace start` Befehl, um die MetroCluster-Prüfungen zu überspringen.

Die Prüfungen werden im automatisierten Betrieb durchgeführt. 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 Quellcontroller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang nach dem Booten der neuen Knoten angehalten und meldet einen Fehler. Führen Sie die manuelle Wiederherstellung durch, um den Cluster wieder in einen fehlerfreien Zustand zu versetzen.

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 Sie vor dem Upgrade Informationen

Vor dem Upgrade, wenn das Root-Volume verschlüsselt ist, müssen Sie den Sicherheitsschlüssel 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 Sie die vorhandene 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"](#) aus der 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 Sie die alten Controller, und starten Sie die 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 werden die in gesammelten Informationen verwenden [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 elc-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 ala -port e0d
```

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

```
network port broadcast-domain remove-ports -ip-space ip-space -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.

Richten Sie die neuen Controller ein

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-Shelves 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.

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

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 <code>ontap-Version_image.tgz</code> file in das Zielverzeichnis: <code>Tar -zxvf ontap-Version_image.tgz</code> 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: <code>Netzboot/Kernel</code> enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: <code>ontap-Version_image.tgz</code> Sie müssen nicht die <code>ontap-Version_image.tgz</code> -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. Eingeben n Überspringen Sie die Backup-Wiederherstellung, wenn Sie eine ähnliche Aufforderung wie die folgende sehen:

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



Um die neu installierte Software nutzen zu können, müssen Sie den Knoten neu starten.

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

`halt`

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

`set-defaults`

3. Umgebung speichern:

`saveenv`

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

`boot_ontap menu`

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

`wipeconfig`

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

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	<code>ucadmin modify -m fc -t initiator adapter-name</code>
CNA-Ethernet	<code>ucadmin modify -mode cna adapter-name</code>
FC-Ziel	<code>fcadmin config -t target adapter-name</code>

FC-Initiator	<code>fcadmin config -t initiator adapter-name</code>
--------------	---

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	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

Neuzuweisung von Root-Aggregat-Festplatten

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 Sie vor dem Upgrade Informationen](#)".

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)	Pool11	PZHYN0MD	
	node_B_1-old(4068741254)			
rr18:9.126L49	node_B_1-old(4068741254)	Pool11	PPG3J5HA	
	node_B_1-old(4068741254)			
rr18:8.126L21	node_B_1-old(4068741254)	Pool11	PZHTDSZD	
	node_B_1-old(4068741254)			
rr18:8.126L2	node_B_1-old(4068741254)	Pool10	S0M1J2CF	
	node_B_1-old(4068741254)			
rr18:8.126L3	node_B_1-old(4068741254)	Pool10	S0M0CQM5	
	node_B_1-old(4068741254)			
rr18:9.126L27	node_B_1-old(4068741254)	Pool10	S0M1PSDW	
	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  SOM1J2CF
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  SOM0CQM5
node_B_1-new(1574774970) node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  SOM1PSDW
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 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 Sie eine VLAN"](#)

["Kombinieren Sie physische 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	<code>security key-manager onboard sync</code> Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement" .
Externes Verschlüsselungskeymanagement	<code>`security key-manager external restore -vserver SVM -node <i>node</i> -key-server <i>_host_name</i></code>

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
```

Schließen Sie das Upgrade ab

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.

Aktualisieren Sie die Nodes auf Cluster_A

Sie müssen die Upgrade-Tasks wiederholen, um die Nodes auf „Cluster_A“ an Standort A zu aktualisieren

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit [Bereiten Sie sich auf das Upgrade vor](#).

Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt.

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 ["Fügen Sie MetroCluster-Konfigurationen hinzu"](#).

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"](#).

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

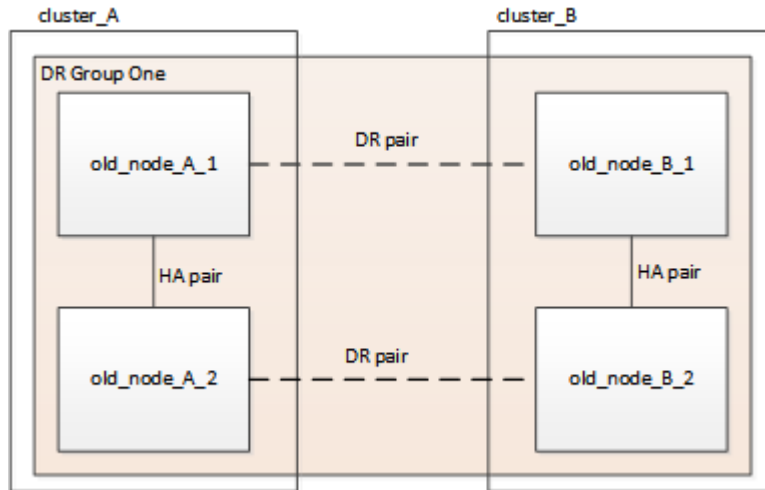
Führen Sie das Aktualisierungsverfahren durch

Führen Sie die folgenden Schritte aus, um die MetroCluster FC-Konfiguration zu aktualisieren.

Schritte

1. Erfassung von Informationen von den alten Knoten.

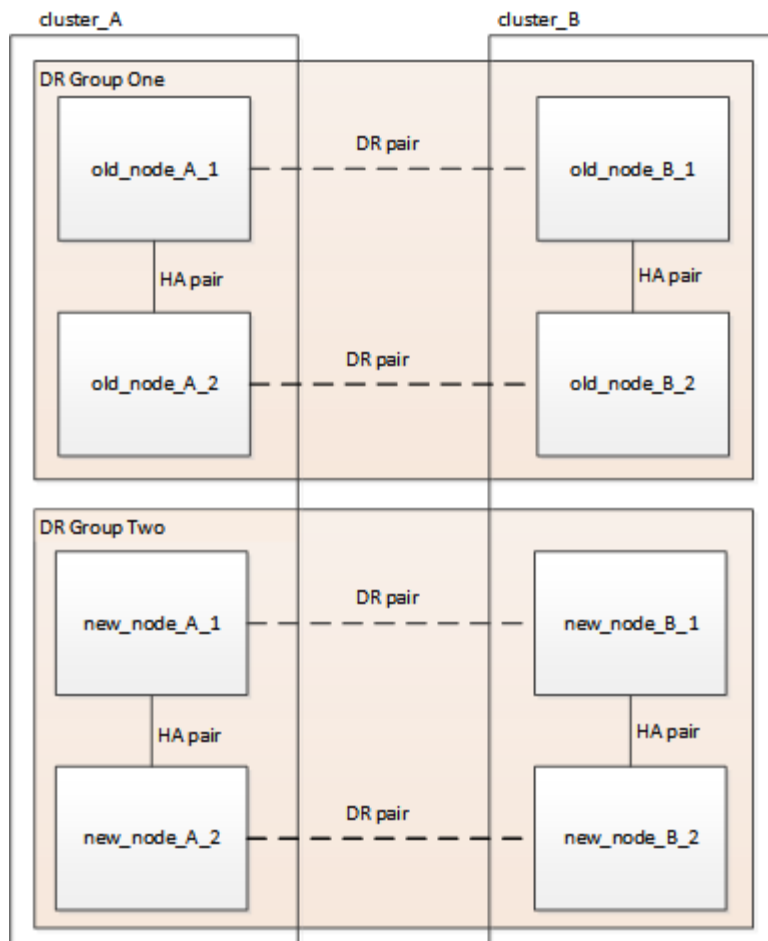
In dieser Phase wird die Konfiguration mit vier Nodes wie in der folgenden Abbildung dargestellt angezeigt:



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"](#).



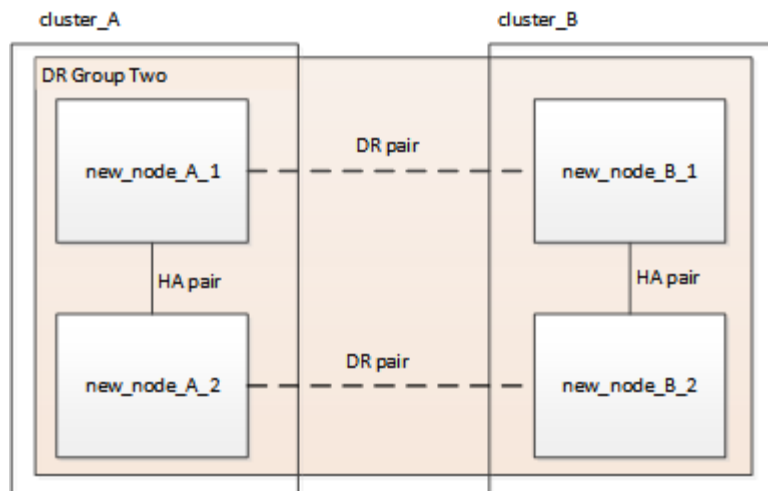
Sie könnten wählen, um das Aggregat zu spiegeln, wenn oder nachdem es erstellt wurde.

- 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.

Wichtige Informationen, wenn Sie ein älteres Plattformmodell hinzufügen

Die folgende Anleitung gilt für ein ungewöhnliches Szenario, in dem Sie einer vorhandenen MetroCluster -Konfiguration, die ein neueres Plattformmodell enthält (Plattformen, die in ONTAP 9.15.1 oder höher veröffentlicht wurden), ein älteres Plattformmodell (Plattformen, die vor ONTAP 9.15.1 veröffentlicht wurden) hinzufügen müssen.

Wenn Ihre vorhandene MetroCluster -Konfiguration eine Plattform enthält, die **gemeinsam genutzte Cluster-/HA-Ports** verwendet (Plattformen, die in ONTAP 9.15.1 oder höher veröffentlicht wurden), können Sie keine Plattform hinzufügen, die **gemeinsam genutzte MetroCluster/HA-Ports** verwendet (Plattformen, die vor ONTAP 9.15.1 veröffentlicht wurden), ohne alle Knoten in der Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher zu aktualisieren.



Das Hinzufügen eines älteren Plattformmodells, das **gemeinsam genutzte/ MetroCluster -HA -Ports** verwendet, zu einem MetroCluster , der ein neueres Plattformmodell enthält, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet, ist ein ungewöhnliches Szenario und die meisten Kombinationen sind nicht betroffen.

Prüfen Sie anhand der folgenden Tabelle, ob Ihre Kombination betroffen ist. Wenn Ihre vorhandene Plattform in der ersten Spalte aufgeführt ist und die Plattform, die Sie der Konfiguration hinzufügen möchten, in der zweiten Spalte aufgeführt ist, müssen alle Knoten in der Konfiguration ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen, um die neue DR-Gruppe hinzuzufügen.

Wenn Ihr vorhandener MetroCluster Folgendes enthält:		Und die Plattform, die Sie hinzufügen, ist ...		Dann...
Ein AFF-System, das gemeinsam genutzte Cluster-/HA-Ports verwendet:	Ein FAS-System, das gemeinsam genutzte Cluster-/HA-Ports verwendet:	Ein AFF-System, das gemeinsam genutzte MetroCluster/HA-Ports verwendet:	Ein FAS-System, das gemeinsam genutzte MetroCluster/HA-Ports verwendet:	Bevor Sie die neue Plattform zu Ihrer vorhandenen MetroCluster-Konfiguration hinzufügen, aktualisieren Sie alle Knoten in der vorhandenen und neuen Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher.
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90	• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500	

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.

Refresh DR groups one at a time.

- * References to "old nodes" mean the nodes that you intend to replace.
- * For eight-node configurations, the source and target eight-node MetroCluster platform combination must be supported.



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.

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

Führen Sie das Aktualisierungsverfahren durch

Führen Sie die folgenden Schritte aus, um die MetroCluster IP-Konfiguration zu aktualisieren.

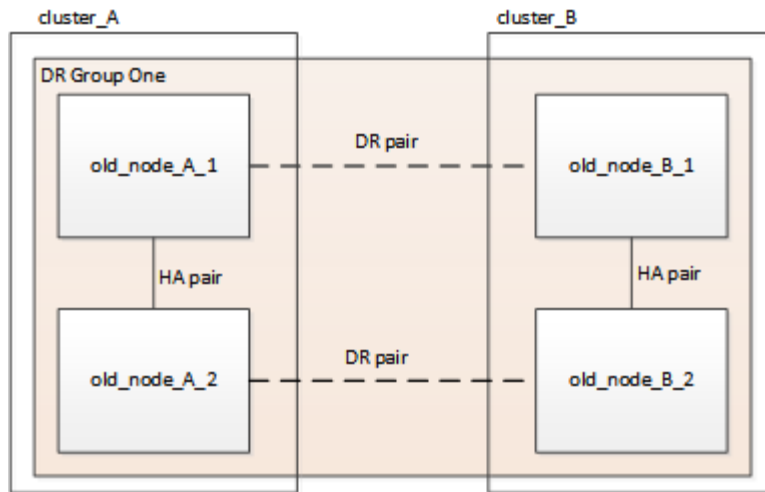
Schritte

1. Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

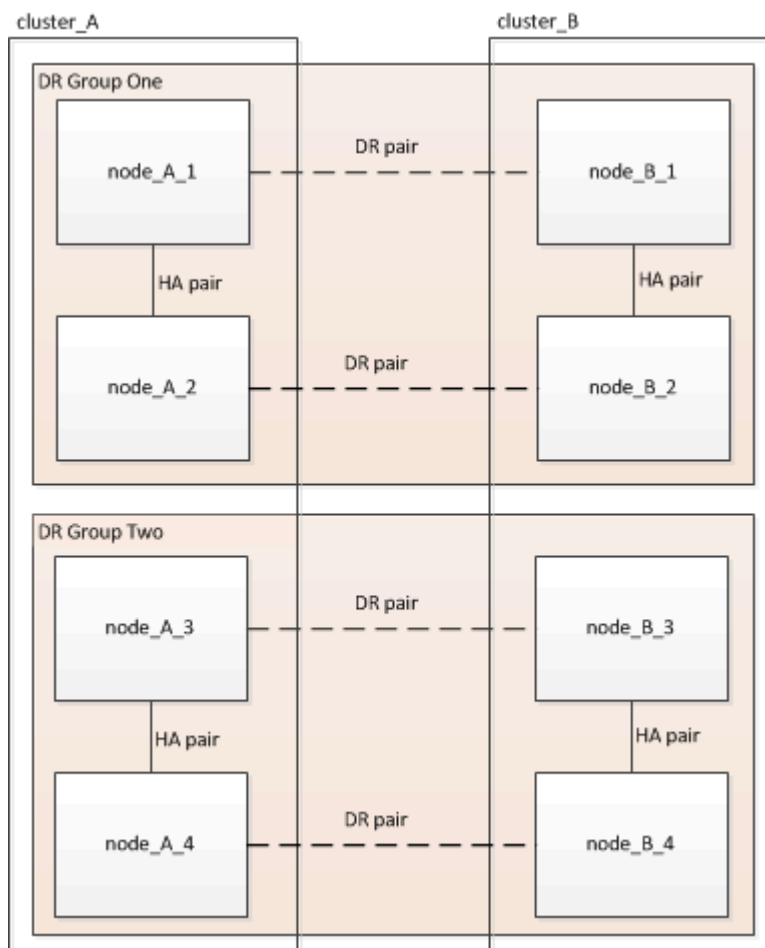
Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden, sondern UUIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel ["LIFs 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 10-stündiges Wartungsfenster an. Planen Sie je nach Plan zusätzliche

Zeit ein.

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. Wenn die End-to-End-Verschlüsselung aktiviert ist, führen Sie die Schritte bis aus ["End-to-End-Verschlüsselung deaktivieren"](#).
5. 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 <code>monitor remove</code> Befehl zum Entfernen der MetroCluster-Konfiguration. Im folgenden Beispiel wird „Cluster_A“ aus der Software entfernt: <pre>NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.</pre> b. Stellen Sie sicher, dass die MetroCluster Konfiguration mithilfe der Tiebreaker CLI ordnungsgemäß entfernt wurde <code>monitor show -status</code> Befehl. <pre>NetApp MetroCluster Tiebreaker :> monitor show -status</pre>
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: <pre>metrocluster configuration-settings mediator remove</pre>
Applikationen von Drittanbietern	Siehe Produktdokumentation.

6. 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:

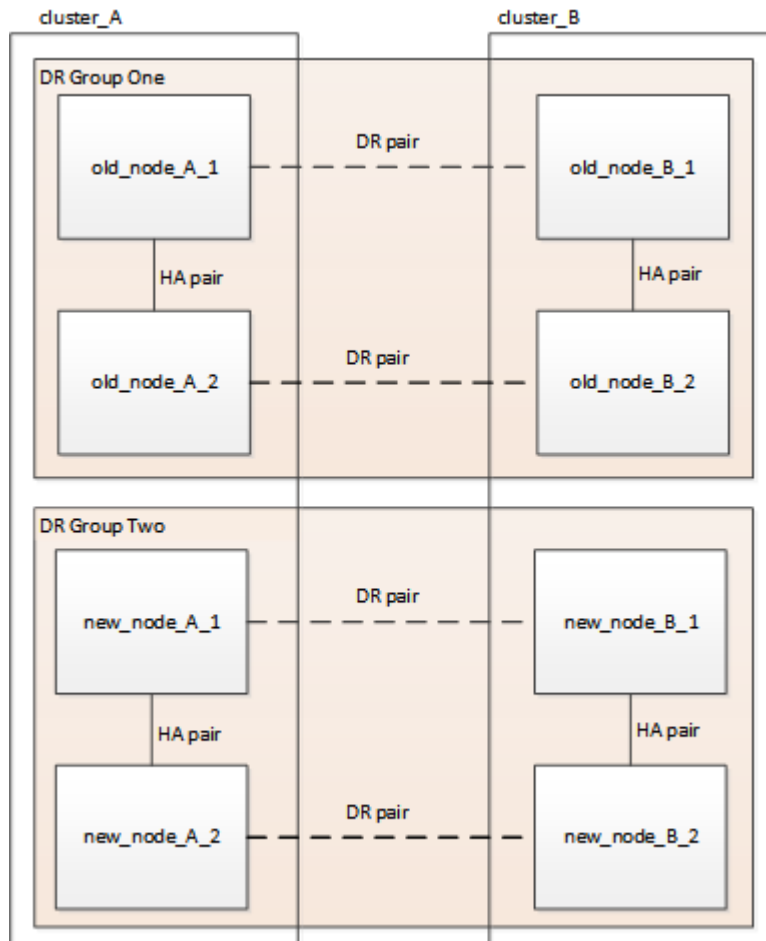


Abbildung 1. Temporäre Konfiguration mit acht Nodes

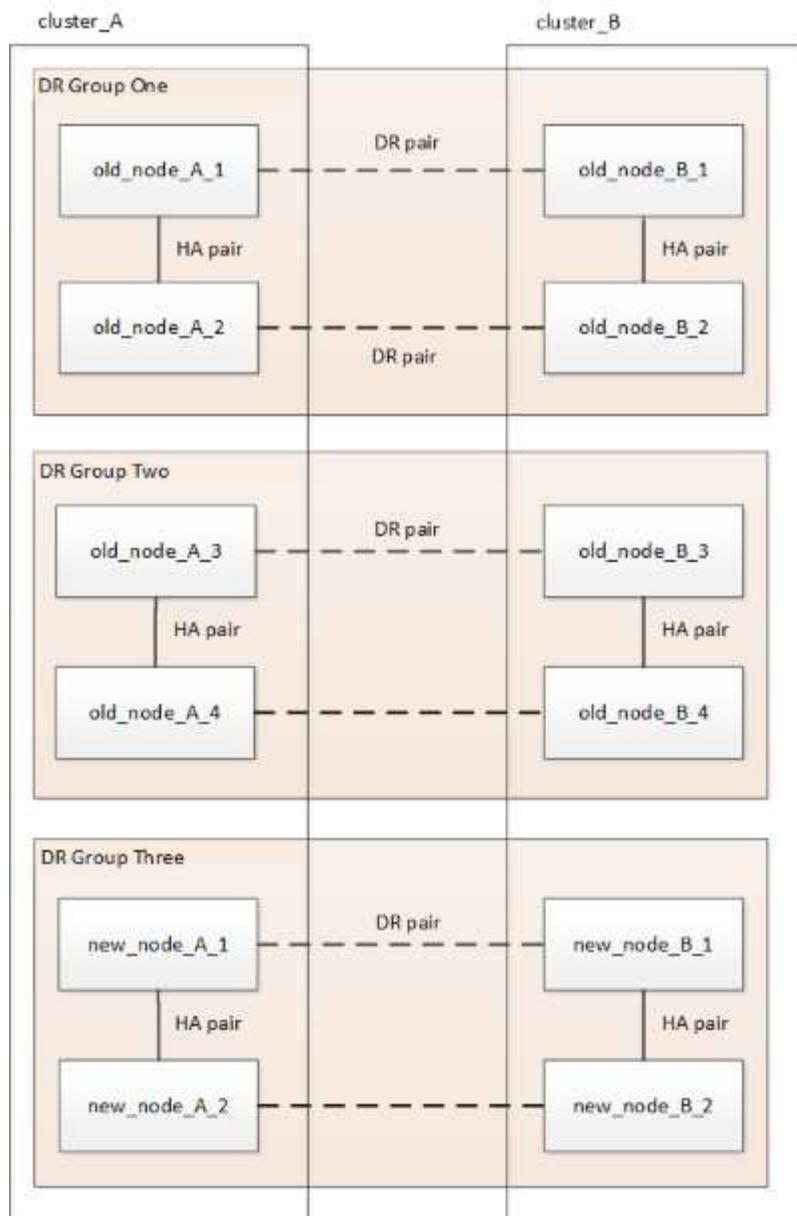


Abbildung 2. Temporäre Konfiguration mit zwölf Nodes

7. 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
```

Node	Partner	Takeover 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

8. Verschieben Sie die CRS-Volumes.

Führen Sie die Schritte unter aus "[Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen](#)".

9. 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](#)".

10. 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-addr 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-addr 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::>
```

11. Befolgen Sie die Schritte unter "[Entfernen einer Disaster Recovery-Gruppe](#)" Um die alte DR-Gruppe zu entfernen.
12. Wenn Sie beide DR-Gruppen in einer Konfiguration mit acht Knoten aktualisieren müssen, wiederholen Sie den gesamten Vorgang für jede DR-Gruppe.

Nachdem Sie die alte DR-Gruppe entfernt haben, wird die Konfiguration wie in den folgenden Bildern dargestellt angezeigt:

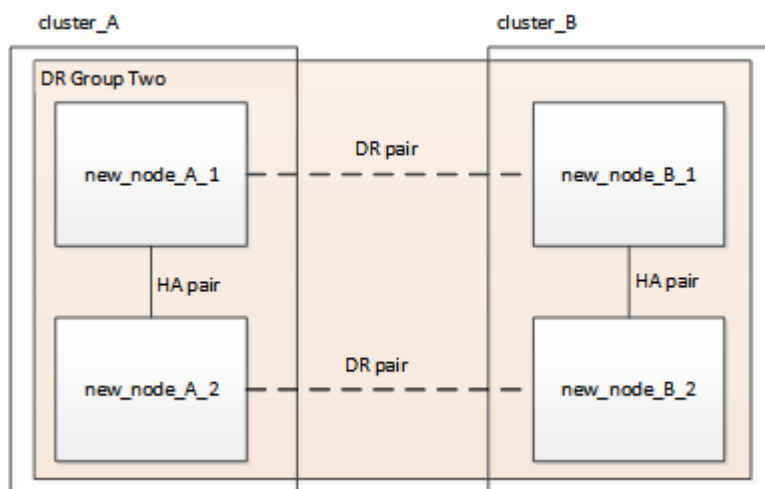


Abbildung 3. Konfiguration mit vier Nodes

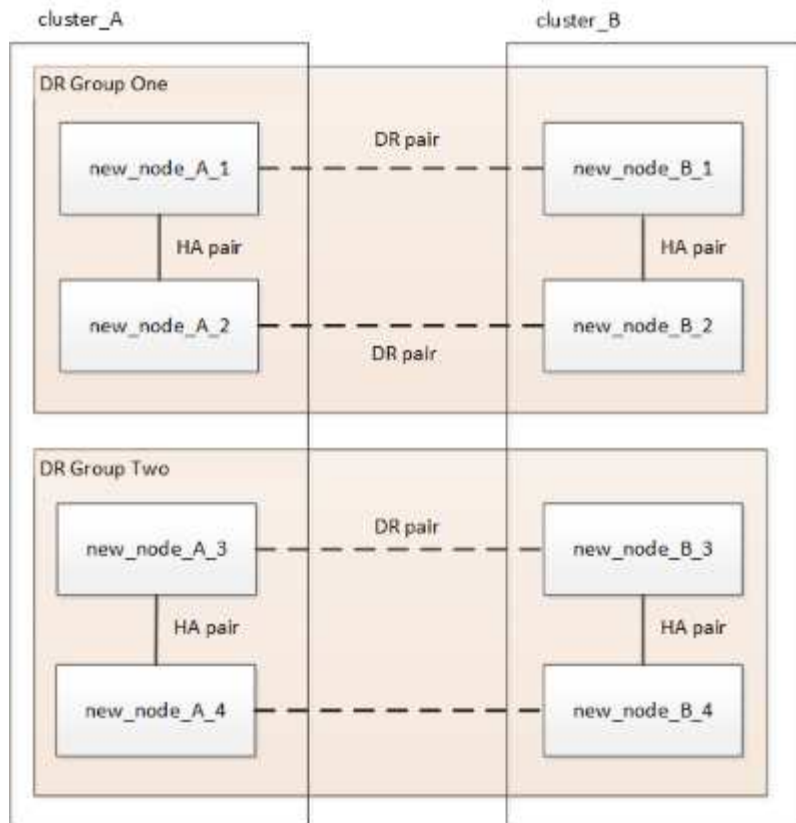


Abbildung 4. Konfiguration mit acht Nodes

13. 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
```

14. Wenn Sie die End-to-End-Verschlüsselung vor dem Hinzufügen der neuen Nodes deaktiviert haben, können Sie sie erneut aktivieren, indem Sie die Schritte unter ausführen ["End-to-End-Verschlüsselung"](#).

15. 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 <i>MetroCluster Tiebreaker Installation und Konfiguration</i> .
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" in der <i>MetroCluster IP-Installation und -Konfiguration</i> .
Applikationen von Drittanbietern	Siehe Produktdokumentation.

16. 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 befinden.
- 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.

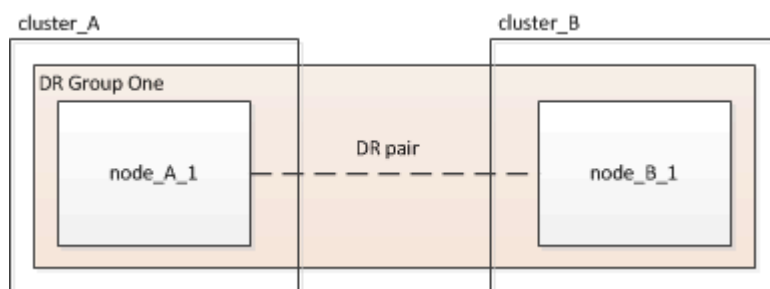
- Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

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 UUIDs (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"](#).

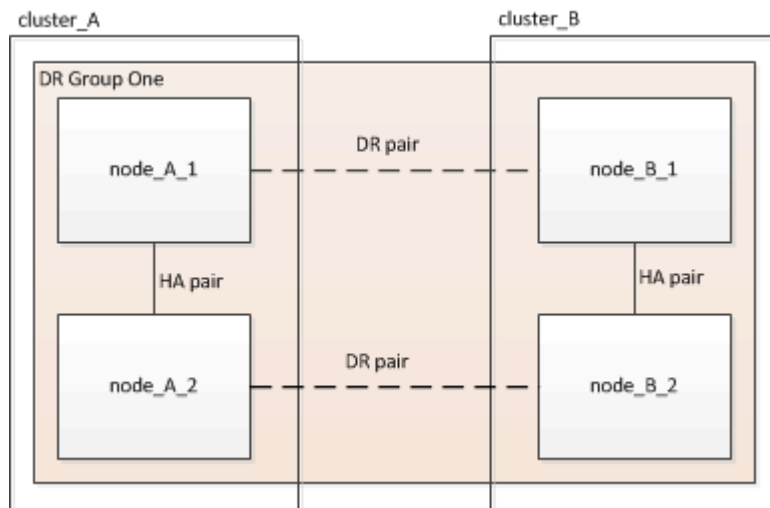
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

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:



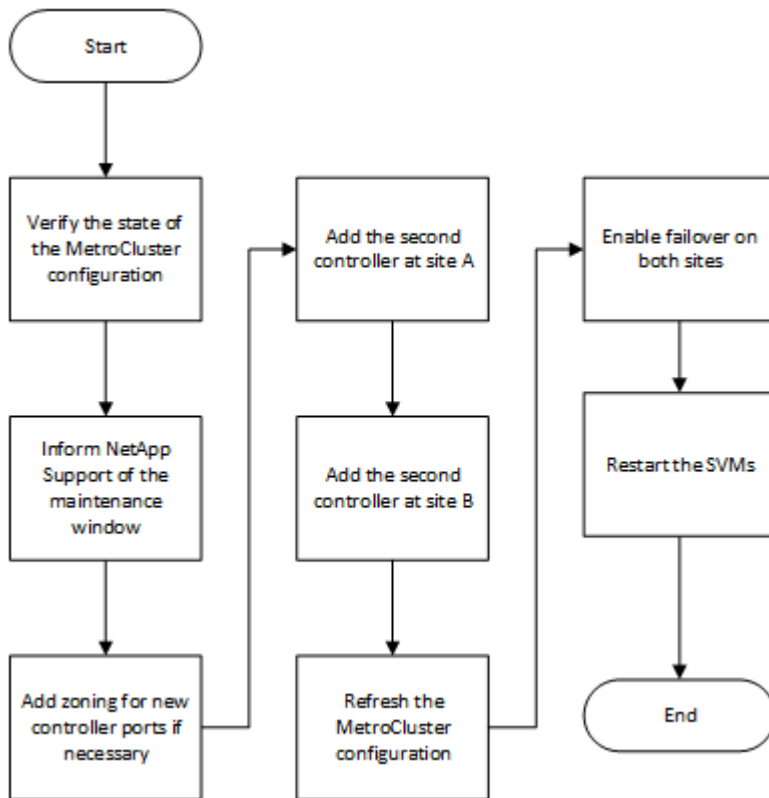
- Beide Standorte müssen gleichermaßen erweitert werden.

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:



Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie diese Aufgabe ausführen.

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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 RAID Status	Size	Available	Used%	State	#Vols	Nodes
-----	-----	-----	-----	-----	-----	
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.

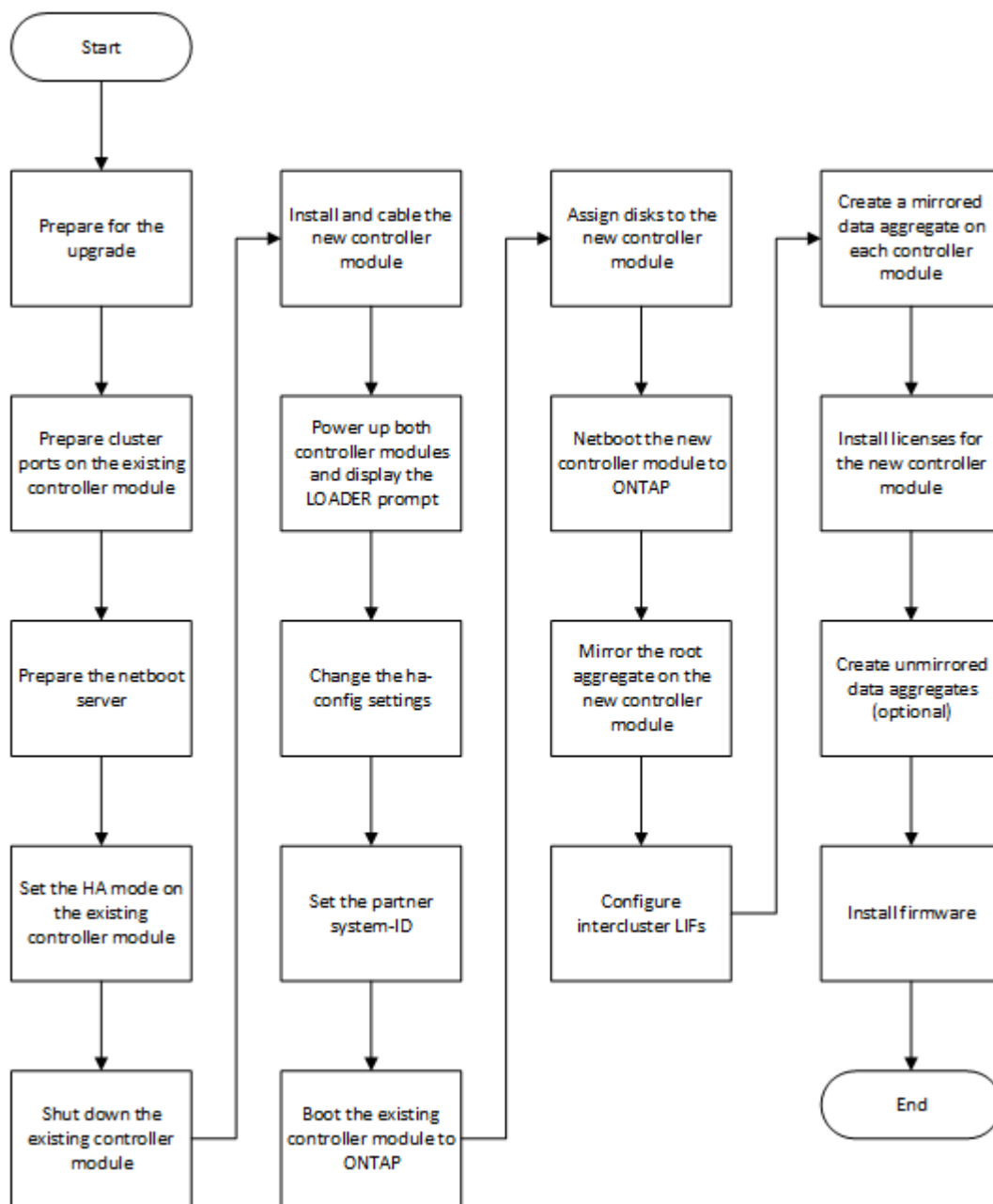


Diese Konfiguration wird nicht auf allen Systemen unterstützt.

- 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 den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

```
halt
```

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

```
set-defaults
```

3. Umgebung speichern:

```
saveenv
```

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

```
boot_ontap menu
```

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

```
wipeconfig
```

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

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 elc-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 ala -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 geschalteten 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 <code><ontap_version>_image.tgz</code> in das Zielverzeichnis: <pre>tar -zxvf <ontap_version>_image.tgz</pre>  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: <pre>netboot/kernel</pre>
Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: <pre><ontap_version>_image.tgz</pre>  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 Netzwerports, 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. Netzkabel 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 Unterschrift 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.
 - ["Portzuweisungen für FC-Switches"](#)
 - ["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	<pre>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></pre> <i>filer_addr</i> Ist die IP-Adresse des Storage-Systems. <i>netmask</i> Ist die Netzwerkmaske des Storage-Systems. <i>gateway</i> Ist das Gateway für das Storage-System. <i>dns_addr</i> Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. <i>dns_domain</i> Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netboot-Server-URL keinen vollqualifizierten Domännennamen. Sie benötigen nur den Host-Namen des Servers.  Andere Parameter können für Ihre Schnittstelle erforderlich sein. Verwenden Sie für Details den <code>help ifconfig</code> Befehl an der LOADER-Eingabeaufforderung.
-----------------	--

2. An der LOADER-Eingabeaufforderung „Netboot“ des neuen Node:

Für...	Geben Sie diesen Befehl aus...
SYSTEME DER FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 SERIE	<pre>netboot http://<i>web_server_ip/path_to_web- accessible_directory</i>/netboot/kernel</pre>
Alle anderen Systeme	<pre>netboot \http://<i>web_server_ip/path_to_web- accessible_directory</i>/<i><ontap_version></i>_image.tgz</pre>

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

Erfahren Sie, wie Sie Intercluster LIFs auf dedizierten und gemeinsam genutzten Ports konfigurieren.

Konfigurieren Sie Intercluster-LIFs auf dedizierten Ports

Es können Intercluster LIFs an dedizierten Ports konfiguriert werden, um die verfügbare Bandbreite für den Replizierungsdatenverkehr zu erhöhen.

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
```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster01-01:e0a, cluster01-01:e0b,
cluster01	Default	cluster01-02:e0a, cluster01-02:e0b
		cluster01-01:e0c, cluster01-02:e0c, cluster01-01:e0d,
		cluster01-02:e0d,
	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	<pre>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></pre>
9.5 und früher	<pre>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></pre>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic01“ 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 Sie Intercluster-LIFs an gemeinsam genutzten Datenports

Es können Intercluster LIFs an Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden, um die Anzahl der Ports zu reduzieren, die Sie für ein Intercluster-Netzwerk 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
```

Erstellen Sie auf jedem MetroCluster FC-Knoten ein gespiegeltes Datenaggregat

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 in Ihrem System mehrere Laufwerkstypen verwenden (heterogene Speicher), sollten Sie wissen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt wird.
- 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"

- Die Namen der Aggregate müssen auf allen MetroCluster-Standorten eindeutig sein. Das bedeutet, dass Sie nicht zwei verschiedene Aggregate mit demselben Namen auf Standort A und Standort B haben können.



Für optimale Speicherleistung und -verfügbarkeit wird empfohlen, mindestens 20 % freien Speicherplatz für gespiegelte Aggregate vorzuhalten. Obwohl für nicht gespiegelte Aggregate 10 % empfohlen werden, können die zusätzlichen 10 % vom Dateisystem genutzt werden, um inkrementelle Änderungen aufzufangen. Inkrementelle Änderungen erhöhen die Speicherauslastung für gespiegelte Aggregate aufgrund der Copy-on-Write-Snapshot-basierten Architektur von ONTAP. Die Nichtbeachtung dieser Best Practices kann sich negativ auf die Leistung 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 am Cluster über die Managementoberfläche angemeldet sind, können Sie auf jedem Knoten im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Knoten erstellt wurde, verwenden Sie den `-node` Parameter oder geben Sie Laufwerke an, die diesem Knoten 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

- Stellen Sie sicher, dass Sie wissen, welche Laufwerke 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 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.
- 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.

Vergewissern Sie sich, dass Sie nur Laufwerke auf dem nicht gespiegelten Shelf zum Aggregat hinzufügen.

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
- 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 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
```

+



Sie können auch mit dem `-disklist` Parameter im Befehl die Festplatten angeben, die Sie für das Aggregat verwenden möchten.

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
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) 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:

- Rufen Sie den erweiterten Berechtigungsmodus auf, und drücken Sie **y** Wenn Sie dazu aufgefordert werden:

```
set -privilege advanced
```

- Starten Sie die SVMs neu:

```
vserver start -vserver SVM_name -force true
```

- 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

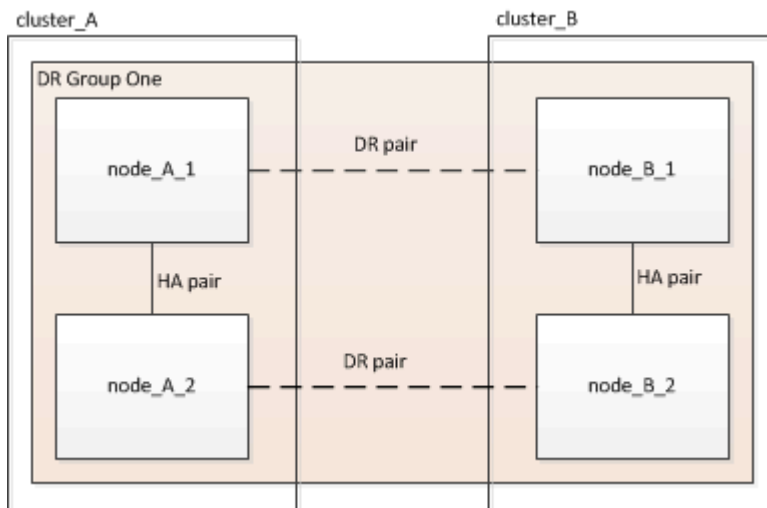
Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes

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.

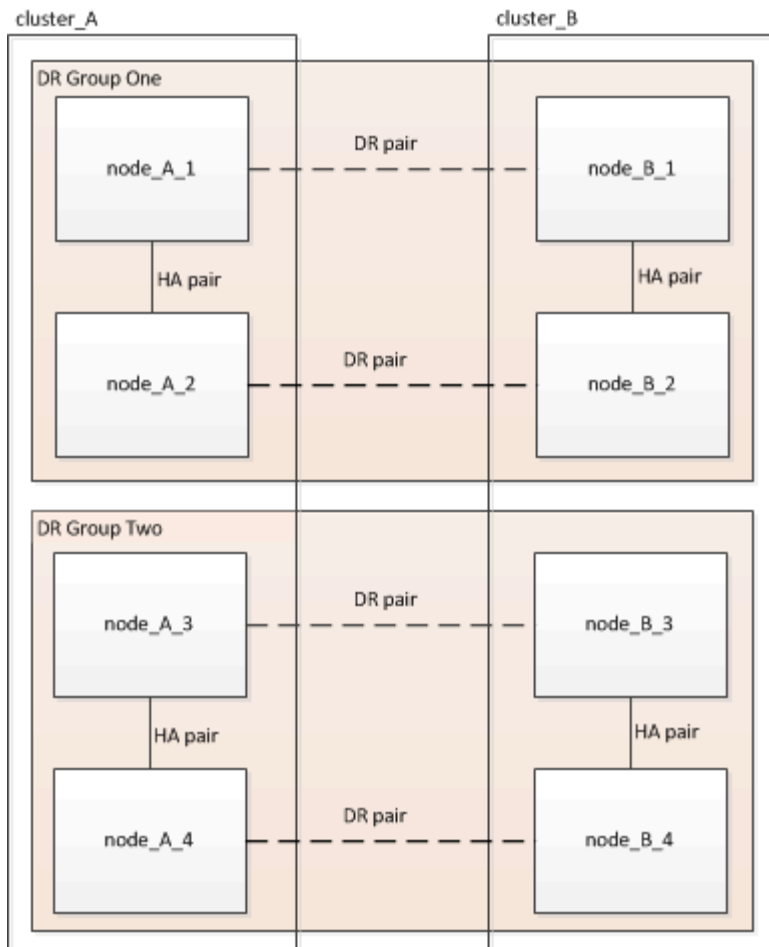
Über diese Aufgabe

- 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 befinden.
- 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 sind 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 gelten **nicht**, wenn Sie die Übergangs- oder Aktualisierungsverfahren verwenden.
- Alle Nodes in einer DR-Gruppe müssen vom gleichen Typ und von derselben Konfiguration sein.

Unterstützte AFF- und FAS MetroCluster-FC-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum erweitern eines AFF oder FAS Systems in einer MetroCluster FC-Konfiguration aufgeführt:

FAS and AFF		Eight-node DR group 2							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Eight-node DR group 1	FAS8200								
	AFF A300								
	FAS8300								
	AFF A400								
	FAS9000								
	AFF A700								
	FAS9500								
	AFF A900								

Unterstützte ASA MetroCluster FC-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum erweitern eines ASA Systems in einer MetroCluster FC-Konfiguration aufgeführt:

DR-Gruppe 1 mit acht Nodes	DR-Gruppe 2 mit acht Nodes	Unterstützt?
ASA A400	ASA A400	Ja.
	ASA A900	Nein
ASA A900	ASA A400	Nein
	ASA A900	Ja.

Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie diese Aufgabe ausführen.

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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:

- 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.

- 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 den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

```
halt
```

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

```
set-defaults
```

3. Umgebung speichern:

```
saveenv
```

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

```
boot_ontap menu
```

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

```
wipeconfig
```

Antworten `yes` An die Bestätigungsaufforderung.

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

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

Antworten `yes` An die Bestätigungsaufforderung.

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 Shelves 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-Shelves den Nodes des ersten Standorts (Standort A) zu:

Festplatten-Shelves an demselben Standort wie der Node werden Pool 0 zugewiesen, und Festplatten-Shelves, die sich am Standort des Partners befinden, werden Pool 1 zugewiesen.

Sie sollten jedem Pool die gleiche Anzahl von Shelves zuweisen.

- a. Weisen Sie beim ersten Knoten systematisch die lokalen Festplatten-Shelves dem Pool 0 und den Remote-Festplatten-Shelves 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-Shelves 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-Shelves den Nodes am zweiten Standort (Standort B) zu:

Festplatten-Shelves an demselben Standort wie der Node werden Pool 0 zugewiesen, und Festplatten-Shelves, die sich am Standort des Partners befinden, werden Pool 1 zugewiesen.

Sie sollten jedem Pool die gleiche Anzahl von Shelves zuweisen.

- a. Weisen Sie beim ersten Knoten am Remote-Standort systematisch seine lokalen Festplatten-Shelves dem Pool 0 und seinen Remote-Festplatten-Shelves 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-Shelves systematisch dem Pool 0 und den Remote-Festplatten-Shelves 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
```

(Mbps)					Speed	
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

Erfahren Sie, wie Sie Intercluster LIFs auf dedizierten und gemeinsam genutzten Ports konfigurieren.

Konfigurieren Sie Intercluster-LIFs auf dedizierten Ports

Es können Intercluster LIFs an dedizierten Ports konfiguriert werden, um die verfügbare Bandbreite für den Replizierungsdatenverkehr zu erhöhen.

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
```

Vserver	Group	Failover Targets
Cluster	Cluster	cluster01-01:e0a, cluster01-01:e0b,
cluster01	Default	cluster01-02:e0a, cluster01-02:e0b
	Default	cluster01-01:e0c, cluster01-01:e0d,
		cluster01-02:e0c, cluster01-02:e0d,
	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	<pre>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></pre>
9.5 und früher	<pre>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></pre>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic01“ 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 Sie Intercluster-LIFs an gemeinsam genutzten Datenports

Es können Intercluster LIFs an Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden, um die Anzahl der Ports zu reduzieren, die Sie für ein Intercluster-Netzwerk 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
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) 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

Erstellen Sie auf jedem MetroCluster FC-Knoten ein gespiegeltes Datenaggregat

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 in Ihrem System mehrere Laufwerkstypen verwenden (heterogene Speicher), sollten Sie wissen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt wird.
- 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"

- Die Namen der Aggregate müssen auf allen MetroCluster-Standorten eindeutig sein. Das bedeutet, dass Sie nicht zwei verschiedene Aggregate mit demselben Namen auf Standort A und Standort B haben können.



Für optimale Speicherleistung und -verfügbarkeit wird empfohlen, mindestens 20 % freien Speicherplatz für gespiegelte Aggregate vorzuhalten. Obwohl für nicht gespiegelte Aggregate 10 % empfohlen werden, können die zusätzlichen 10 % vom Dateisystem genutzt werden, um inkrementelle Änderungen aufzufangen. Inkrementelle Änderungen erhöhen die Speicherauslastung für gespiegelte Aggregate aufgrund der Copy-on-Write-Snapshot-basierten Architektur von ONTAP. Die Nichtbeachtung dieser Best Practices kann sich negativ auf die Leistung 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 am Cluster über die Managementoberfläche angemeldet sind, können Sie auf jedem Knoten im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Knoten erstellt wurde, verwenden Sie den `-node` Parameter oder geben Sie Laufwerke an, die diesem Knoten 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

Erfahren Sie, wie Sie die FC-zu-SAS-Bridges für die Zustandsüberwachung konfigurieren.

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 `system bridge` ersetzt. 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	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>
9.4 und früher	<code>storage bridge add -address <i>bridge-ip-address</i> -name <i>bridge-name</i></code>

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 Model	Symbolic Name	Is Monitored	Monitor Status	Vendor
	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 bewegendes 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
ok
ok
ok
controller_A_1_aggr2
ok
ok
ok
controller_A_2
controller_A_2_aggr0
ok
ok
ok
controller_A_2_aggr1
ok
ok
ok
controller_A_2_aggr2
ok
ok
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 Umschaltvorgänge, 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 Sie eine 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.

Wichtige Informationen, wenn Sie ein älteres Plattformmodell hinzufügen

Die folgende Anleitung gilt für ein ungewöhnliches Szenario, in dem Sie einer vorhandenen MetroCluster -Konfiguration, die ein neueres Plattformmodell enthält (Plattformen, die in ONTAP 9.15.1 oder höher veröffentlicht wurden), ein älteres Plattformmodell (Plattformen, die vor ONTAP 9.15.1 veröffentlicht wurden) hinzufügen müssen.

Wenn Ihre vorhandene MetroCluster -Konfiguration eine Plattform enthält, die **gemeinsam genutzte Cluster-/HA-Ports** verwendet (Plattformen, die in ONTAP 9.15.1 oder höher veröffentlicht wurden), können Sie keine Plattform hinzufügen, die **gemeinsam genutzte MetroCluster/HA-Ports** verwendet (Plattformen, die vor ONTAP 9.15.1 veröffentlicht wurden), ohne alle Knoten in der Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher zu aktualisieren.



Das Hinzufügen eines älteren Plattformmodells, das **gemeinsam genutzte/ MetroCluster -HA -Ports** verwendet, zu einem MetroCluster , der ein neueres Plattformmodell enthält, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet, ist ein ungewöhnliches Szenario und die meisten Kombinationen sind nicht betroffen.

Prüfen Sie anhand der folgenden Tabelle, ob Ihre Kombination betroffen ist. Wenn Ihre vorhandene Plattform in der ersten Spalte aufgeführt ist und die Plattform, die Sie der Konfiguration hinzufügen möchten, in der zweiten Spalte aufgeführt ist, müssen alle Knoten in der Konfiguration ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen, um die neue DR-Gruppe hinzuzufügen.

Wenn Ihr vorhandener MetroCluster Folgendes enthält:		Und die Plattform, die Sie hinzufügen, ist ...		Dann...
Ein AFF-System, das gemeinsam genutzte Cluster-/HA-Ports verwendet:	Ein FAS-System, das gemeinsam genutzte Cluster-/HA-Ports verwendet:	Ein AFF-System, das gemeinsam genutzte MetroCluster/HA-Ports verwendet:	Ein FAS-System, das gemeinsam genutzte MetroCluster/HA-Ports verwendet:	Bevor Sie die neue Plattform zu Ihrer vorhandenen MetroCluster-Konfiguration hinzufügen, aktualisieren Sie alle Knoten in der vorhandenen und neuen Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher.
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90	• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500	

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 UUIDs (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"](#).

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

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

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 MetroCluster 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 unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im ["Hardware Universe"](#).
- 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.

Unterstützte AFF- und FAS MetroCluster-IP-Erweiterungskombinationen

Die folgenden Tabellen zeigen die unterstützten Plattformkombinationen für die Erweiterung eines AFF- oder FAS-Systems in einer MetroCluster IP-Konfiguration. Die Tabellen sind in zwei Gruppen aufgeteilt:

- **Gruppe 1** zeigt Kombinationen für AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF C400, AFF A400, AFF A220, AFF A300, AFF A320 und FAS8700 Systeme.
- **Gruppe 2** zeigt Kombinationen für AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

Die folgenden Hinweise gelten für beide Gruppen:

- 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.

AFF- und FAS-Kombinationen, Gruppe 1

Prüfen Sie die Erweiterungskombinationen für AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A400, AFF A220, AFF C400, AFF A320 und FAS8700 Systeme.

AFF and FAS		Eight-node DR group 2									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Eight-node DR group 1	AFF A150	Note 2									
	AFF A20										
	FAS2750 AFF A220										
	FAS500f AFF C250 AFF A250										
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300							Note 1			
	AFF A320							Note 1			
	FAS8300 AFF C400 AFF A400							Note 1	Note 1		
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFF und FAS Kombinationsgruppe 2

Prüfen Sie die Erweiterungskombinationen für AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

AFF and FAS		Eight-node DR group 2									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Eight-node DR group 1	AFF A150										
	AFF A20										
	FAS2750										
	AFF A220										
	FAS500f										
	AFF C250										
	AFF A250										
	FAS50										
	AFF C30										
	AFF A30										
	FAS8200										
	AFF A300										
	AFF A320										
	FAS8300	Note 1									
	AFF C400										
	AFF A400										
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70				Note 1						
	FAS9000			Note 1	Note 1						
	AFF A700										
	AFF A70										
	AFF C800										
	AFF A800										
	FAS9500										
	AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

Unterstützte ASA MetroCluster IP-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für die Erweiterung eines ASA-Systems in einer MetroCluster IP-Konfiguration aufgeführt:

ASA		Eight-node DR group 2							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Eight-node DR group 1	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

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.

Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe

- Beim erweitern einer MetroCluster-IP-Konfiguration gelten die folgenden VLAN-Überlegungen:

Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

Falls unterstützt, können Sie auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben. Verwenden Sie dazu den `-vlan-id` Parameter im `metrocluster configuration-settings interface create` Befehl.

Die folgenden Plattformen unterstützen **Not** den `-vlan-id` Parameter:

- FAS8200 UND AFF A300
- AFF A320
- FAS9000 und AFF A700
- AFF C800, ASA C800, AFF A800 und ASA A800

Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.

Die Standard- und gültigen VLAN-Zuweisungen hängen davon ab, ob die Plattform den folgenden Parameter unterstützt `-vlan-id`:

Plattformen, die `-vlan-` unterstützen

Standard-VLAN:

- Wenn der `-vlan-id` Parameter nicht angegeben wird, werden die Schnittstellen mit VLAN 10 für die „A“-Ports und VLAN 20 für die „B“-Ports erstellt.
- Das angegebene VLAN muss mit dem im RCF ausgewählten VLAN übereinstimmen.

Gültige VLAN-Bereiche:

- Standard-VLAN 10 und 20
- VLANs 101 und höher (zwischen 101 und 4095)

Plattformen, die `-vlan-` nicht unterstützen

Standard-VLAN:

- Keine Angabe. Für die Schnittstelle muss kein VLAN auf der MetroCluster-Schnittstelle angegeben werden. Der Switch-Port definiert das verwendete VLAN.

Gültige VLAN-Bereiche:

- Alle VLANs werden beim Generieren der RCF nicht explizit ausgeschlossen. Die RCF warnt Sie, wenn das VLAN ungültig ist.

- Beide DR-Gruppen nutzen die gleichen VLANs, wenn Sie eine MetroCluster-Konfiguration mit vier Nodes auf acht Nodes erweitern.
- Wenn beide DR-Gruppen nicht mit demselben VLAN konfiguriert werden können, müssen Sie die DR-Gruppe, die den Parameter nicht unterstützt, aktualisieren `vlan-id`, um ein VLAN zu verwenden, das von der anderen DR-Gruppe unterstützt wird.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Vor der Erweiterung 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 das System multipathed ist:

```
node run -node <node-name> sysconfig -a
```

- b. Überprüfen Sie auf beiden Clustern auf Zustandswarmmeldungen:

```
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
```

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

```
Node: node_A_2-old
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health 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
```

Vserver	Logical 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: <pre>metrocluster configuration-settings mediator remove</pre>
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. Verkabeln Sie die neuen MetroCluster IP-Knoten wie in dargestellt mit den IP-Switches "[Verkabeln Sie die IP-Switches](#)".
3. Konfigurieren Sie die MetroCluster IP-Nodes wie folgt:
 - a. "[Sammeln Sie die erforderlichen Informationen](#)"
 - b. "[Systemstandardwerte auf einem Controller-Modul wiederherstellen](#)"
 - c. "[Überprüfen Sie den Status der HA-Konfiguration der 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         ok
clusters           ok
connections        ok
volumes            ok
7 entries were displayed.
```

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

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

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

```
system health alert show
```

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

Befolgen Sie die Schritte für Ihren Switch-Anbieter:

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

3. Laden Sie je nach Switch-Anbieter die IP RCF-Datei herunter, und installieren Sie sie.



Aktualisieren Sie die Schalter in folgender Reihenfolge: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

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



Wenn Sie über eine freigegebene L2- oder L3-Netzwerkconfiguration verfügen, müssen Sie möglicherweise die ISL-Ports an den Zwischen-/Kunden-Switches anpassen. Der Switch-Port-Modus wechselt möglicherweise vom „Access“- in den „Trunk“-Modus. 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 Sie die 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 für Ihre MetroCluster IP Node-Plattform spezifischen Home Port verwenden.
- Überprüfen Sie die Informationen in [Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe](#) , bevor Sie diese Aufgabe ausführen.

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
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:



- Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.
- Wenn unterstützt, können Sie ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) mit dem Parameter im Befehl angeben `-vlan-id` `metrocluster configuration-settings interface create`. Informationen zu unterstützten Plattformen finden Sie unter [Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe](#).
- Sie können die MetroCluster-IP-Schnittstellen von beiden Clustern konfigurieren.

```
metrocluster configuration-settings interface create -cluster-name
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port ela -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 elb -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 ela -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 elb -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 ela -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 elb -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 ela -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 elb -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: ela
                172.17.28.11      255.255.255.0    -
completed
                Home Port: elb
                172.17.29.11      255.255.255.0    -
completed
    cluster_B
        node_B_3-new
            Home Port: ela
            172.17.28.13      255.255.255.0    -
completed
            Home Port: elb
            172.17.29.13      255.255.255.0    -
completed
        node_B_3-new
            Home Port: ela
            172.17.28.12      255.255.255.0    -
completed
            Home Port: elb
            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
Group Cluster Node      Source          Destination
Config State    Network Address Network Address Partner Type
-----
-----
-----
-----
-----

```

```

1      cluster_A
      node_A_1-old
      Home Port: ela
      172.17.28.10      172.17.28.11      HA Partner
completed
      Home Port: ela
      172.17.28.10      172.17.28.12      DR Partner
completed
      Home Port: ela
      172.17.28.10      172.17.28.13      DR Auxiliary
completed
      Home Port: elb
      172.17.29.10      172.17.29.11      HA Partner
completed
      Home Port: elb
      172.17.29.10      172.17.29.12      DR Partner
completed
      Home Port: elb
      172.17.29.10      172.17.29.13      DR Auxiliary
completed
      node_A_2-old
      Home Port: ela
      172.17.28.11      172.17.28.10      HA Partner
completed
      Home Port: ela
      172.17.28.11      172.17.28.13      DR Partner
completed
      Home Port: ela
      172.17.28.11      172.17.28.12      DR Auxiliary
completed
      Home Port: elb
      172.17.29.11      172.17.29.10      HA Partner
completed
      Home Port: elb
      172.17.29.11      172.17.29.13      DR Partner
completed
      Home Port: elb
      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: ela
    172.17.28.13    172.17.28.12    HA Partner
completed
  Home Port: ela
    172.17.28.13    172.17.28.11    DR Partner
completed
  Home Port: ela
    172.17.28.13    172.17.28.10    DR Auxiliary
completed
  Home Port: elb
    172.17.29.13    172.17.29.12    HA Partner
completed
  Home Port: elb
    172.17.29.13    172.17.29.11    DR Partner
completed
  Home Port: elb
    172.17.29.13    172.17.29.10    DR Auxiliary
completed
node_B_1-old
  Home Port: ela
    172.17.28.12    172.17.28.13    HA Partner
completed
  Home Port: ela
    172.17.28.12    172.17.28.10    DR Partner
completed
  Home Port: ela
    172.17.28.12    172.17.28.11    DR Auxiliary
completed
  Home Port: elb
    172.17.29.12    172.17.29.13    HA Partner
completed
  Home Port: elb
    172.17.29.12    172.17.29.10    DR Partner
completed
  Home Port: elb
    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**

```

```

completed      Home Port: ela
                  172.17.26.10      172.17.26.11      HA Partner

completed      Home Port: ela
                  172.17.26.10      172.17.26.12      DR Partner

completed      Home Port: ela
                  172.17.26.10      172.17.26.13      DR Auxiliary

completed      Home Port: elb
                  172.17.27.10      172.17.27.11      HA Partner

completed      Home Port: elb
                  172.17.27.10      172.17.27.12      DR Partner

completed      Home Port: elb
                  172.17.27.10      172.17.27.13      DR Auxiliary

completed      node_A_2-new
                  Home Port: ela
                    172.17.26.11      172.17.26.10      HA Partner

completed      Home Port: ela
                  172.17.26.11      172.17.26.13      DR Partner

completed      Home Port: ela
                  172.17.26.11      172.17.26.12      DR Auxiliary

completed      Home Port: elb
                  172.17.27.11      172.17.27.10      HA Partner

completed      Home Port: elb
                  172.17.27.11      172.17.27.13      DR Partner

completed      Home Port: elb
                  172.17.27.11      172.17.27.12      DR Auxiliary

DR
Group Cluster Node      Source      Destination
Config State      Network Address Network Address Partner Type
-----
2      cluster_B
      node_B_2-new
      Home Port: ela

```

```

172.17.26.13      172.17.26.12      HA Partner
completed
Home Port: ela
172.17.26.13      172.17.26.11      DR Partner
completed
Home Port: ela
172.17.26.13      172.17.26.10      DR Auxiliary
completed
Home Port: elb
172.17.27.13      172.17.27.12      HA Partner
completed
Home Port: elb
172.17.27.13      172.17.27.11      DR Partner
completed
Home Port: elb
172.17.27.13      172.17.27.10      DR Auxiliary
completed
node_B_1-new
Home Port: ela
172.17.26.12      172.17.26.13      HA Partner
completed
Home Port: ela
172.17.26.12      172.17.26.10      DR Partner
completed
Home Port: ela
172.17.26.12      172.17.26.11      DR Auxiliary
completed
Home Port: elb
172.17.27.12      172.17.27.13      HA Partner
completed
Home Port: elb
172.17.27.12      172.17.27.10      DR Partner
completed
Home Port: elb
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
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
-----	-----	-----	---	-----	-----	-----
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)

Physical                                     Usable
Size      Position   Disk                               Type      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 neu hinzugefügten Knoten:

Wenn Ihre MetroCluster Konfiguration...	Dann tun Sie das...
Mehrere Datenaggregate	Führen Sie an der Eingabeaufforderung eines beliebigen Knotens Folgendes aus: <code>metrocluster configure <node-name></code>
Ein einziges gespiegeltes Datenaggregat an einem oder beiden Standorten	Konfigurieren Sie an einer beliebigen Node-Eingabeaufforderung die MetroCluster mit dem <code>-allow-with-one-aggregate true</code> Parameter: <code>metrocluster configure -allow-with-one-aggregate true <node-name></code>

c. Starten Sie jeden der neuen Nodes neu:

```
node reboot -node <node_name> -inhibit-takeover true
```



Die Nodes müssen nicht in einer bestimmten Reihenfolge neu gebootet werden. Sie sollten jedoch warten, bis ein Node vollständig gebootet wurde und alle Verbindungen hergestellt sind, bevor Sie den nächsten Node neu booten.

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 ist akzeptabel, dass ein Standort der MetroCluster ein einziges gespiegeltes Datenaggregat hat und der andere Standort mehr als ein gespiegeltes Datenaggregat hat.
- Die Namen der Aggregate müssen auf allen MetroCluster-Standorten eindeutig sein. Das bedeutet, dass Sie nicht zwei verschiedene Aggregate mit demselben Namen auf Standort A und Standort B haben können.

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 im erweiterten Berechtigungsmodus.

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.

Wenn Sie eine MetroCluster-Konfiguration mit vier Knoten auf eine permanente Konfiguration mit acht Knoten erweitern, sollten Sie eines der MDV-Volumes in die neue DR-Gruppe verschieben.

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 <svm-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.
```

6. Wenn Ihr System End-to-End-Verschlüsselung unterstützt, können Sie dies tun ["End-to-End-Verschlüsselung"](#) Auf der neuen DR-Gruppe.

Entfernen einer DR-Gruppe aus einer MetroCluster -Konfiguration

Ab ONTAP 9.8 können Sie eine Disaster Recovery (DR)-Gruppe aus einer MetroCluster Konfiguration mit acht Knoten entfernen, um eine MetroCluster Konfiguration mit vier Knoten zu erstellen.



Sie verwenden diese Schritte während der Übergangs- und Systemaktualisierungs-Workflows.

Aktivieren Sie die Konsolenprotokollierung

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

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

Siehe Knowledge Base-Artikel ["Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"](#).

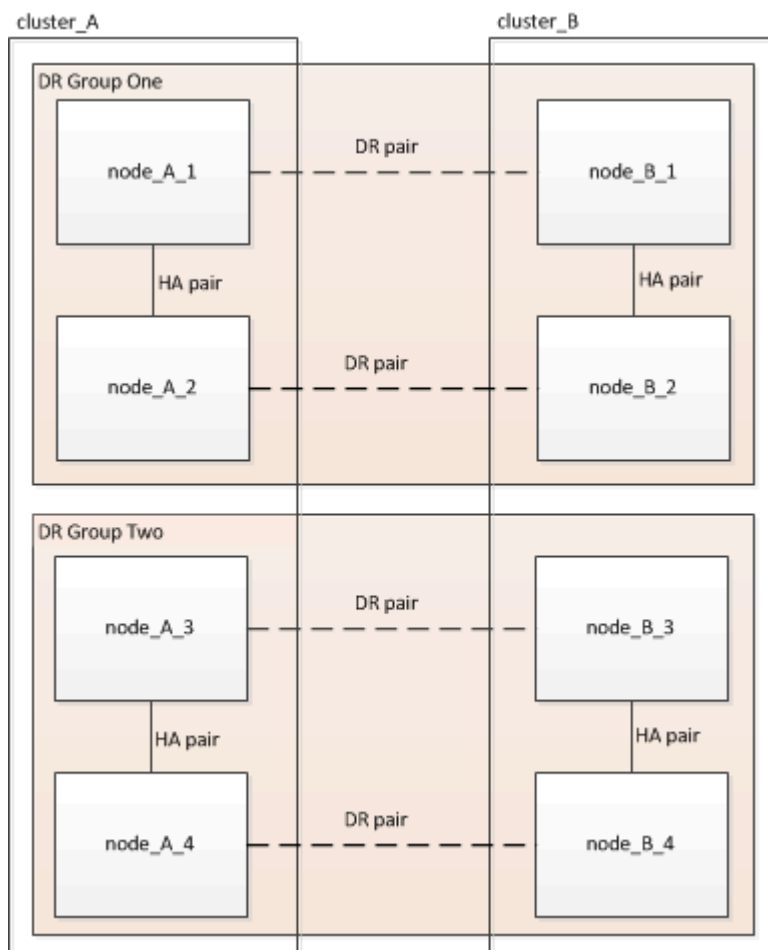
- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel ["So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen"](#).

Entfernen Sie die DR-Gruppenknoten aus jedem Cluster

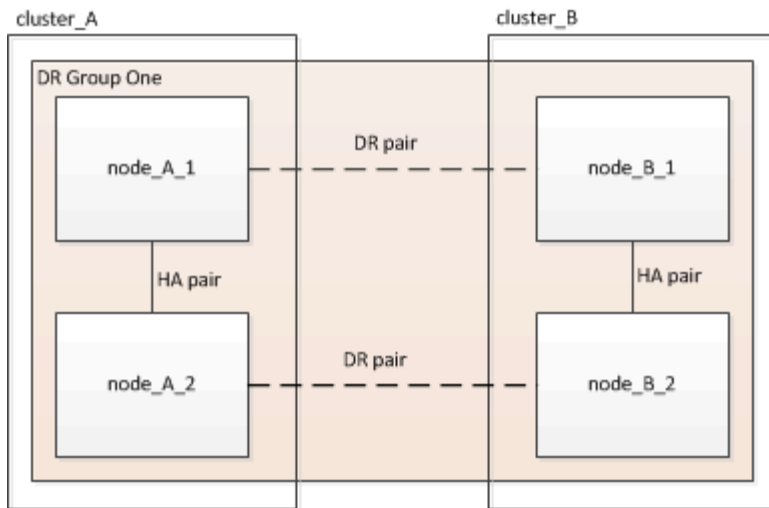
Dieses Verfahren wird ab ONTAP 9.8 unterstützt. Informationen zu Systemen mit ONTAP 9.7 oder früher finden Sie im Knowledge Base-Artikel: ["So entfernen Sie eine DR-Gruppe aus einer MetroCluster-Konfiguration"](#).

Über diese Aufgabe

Eine Konfiguration mit acht Nodes umfasst acht Nodes, die als zwei DR-Gruppen mit vier Nodes organisiert sind.



Wenn Sie eine DR-Gruppe entfernen, verbleiben vier Knoten in der Konfiguration.



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 das Entfernen der DR-Gruppe vor, falls Sie dies noch nicht getan haben.
 - a. Verschieben Sie alle Daten-Volumes in eine andere DR-Gruppe.
 - b. Wenn die zu entfernende DR-Gruppe über Load-Sharing-Spiegelvolumes verfügt, erstellen Sie alle Load-Sharing-Spiegelvolumes in einer anderen DR-Gruppe neu und löschen Sie sie aus 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 zu entfernenden DR-Gruppe:

```
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. Migrieren Sie alle NAS-Daten-LIFs, die Sie für NFS und CIFS (SMB) verwenden, auf Home-Knoten in einer anderen DR-Gruppe.

```
network interface show -home-node <old_node>
```

```
network interface migrate -vserver <svm_name> -lif <data_lif> -destination
-node <new_node> -destination-port <port>
```

g. Verschieben Sie die Daten-LIFs auf den neuen Home-Knoten in einer anderen DR-Gruppe. `network interface modify -vserver <svm-name> -lif <data-lif> -home-node <new_node> -home-port <port>`

h. 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>
```



- Knotenverwaltung und LIFs zwischen Clustern werden nicht migriert. Erstellen Sie nach Bedarf neue Knotenverwaltungs- und Cluster-übergreifende LIFs auf Knoten der DR-Gruppe.
- Sie können FCP-Schnittstellen, die für den Blockzugriff (SAN) verwendet werden, nicht zwischen den Knoten migrieren oder verschieben. Erstellen Sie nach Bedarf neue FCP-Schnittstellen.
- iSCSI SAN LIFs müssen ausgefallen sein, bevor der Home-Knoten und der Home-Port aktualisiert werden können.

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

Beispiel

```
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. Deaktivieren Sie das Speicherfailover auf den Knoten der alten DR-Gruppe:

```
storage failover modify -node <node-name> -enable false
```

5. Wenn Sie sich in einer MetroCluster -IP-Konfiguration befinden, führen Sie die folgenden Schritte aus, um die Remote-Plexes der Root-Aggregate zu löschen und den Festplattenbesitz auf den Knoten der alten DR-Gruppe zu entfernen.

Diese Schritte müssen für beide Knoten im HA-Paar an jedem Standort ausgeführt werden.

- a. Zeigen Sie die Remote-Plexes der Root-Aggregate auf den Knoten in der DR-Gruppe an, die gelöscht werden soll:

```
storage aggregate plex show -aggregate <root_aggr_name> -pool 1
```

- b. Löschen Sie die Remote-Plexes:

```
storage aggregate plex delete -aggregate <root_aggr_name> -plex  
<plex_from_previous_step>
```

- c. Identifizieren Sie die Remote-Datenträger, die den Knoten in der DR-Gruppe gehören.

Die zu verwendenden Befehle hängen davon ab, ob Sie partitionierte/gemeinsam genutzte Festplatten oder ganze Festplatten verwenden:



Verwenden Sie eine durch Kommas getrennte Liste in der `-owner <node_names>`, um die Knotennamen in der DR-Gruppe anzugeben, die gelöscht werden soll.

Partitionierte/gemeinsam genutzte Datenträger:

- i. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set advanced
```

- ii. Zeigen Sie die Remote-Festplatten an:

```
storage disk show -pool Pool1 -owner <node_names> -partition  
-ownership
```

Ganze Festplatten:

- i. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set advanced
```

- ii. Zeigen Sie die Remote-Festplatten an:

```
storage disk show -pool Pool1 -owner <node_names>
```

- d. Automatische Datenträgerzuweisung deaktivieren:

```
disk option modify -node <node_names_in_the_DR_group_to_be_deleted>  
-autoassign off
```

e. Entfernen Sie den Besitz der Pool1-Datenträger auf jedem zu löschenden DR-Gruppenknoten. Führen Sie diese Schritte auf jedem zu entfernenden Knoten aus.

i. Gehen Sie zur Node-Shell:

```
run -node <node_name>
```

ii. Identifizieren Sie die Pool1-Festplatten:

```
aggr status -s
```

Es werden alle Ersatzfestplatten angezeigt, einschließlich der Ersatzfestplatten Pool0 und Pool1, die dem Knoten gehören.

i. Entfernen Sie den Festplattenbesitz für jede Ersatzfestplatte von Pool1:

```
disk remove_ownership <disk_name>
```

Entfernen Sie bei partitionierten Datenträgern den Partitionsbesitz und dann den Containerdatenträgerbesitz.

6. Wenn Sie sich in einer MetroCluster -IP-Konfiguration befinden, entfernen Sie die MetroCluster Verbindungen auf den Knoten der alten DR-Gruppe.

Diese Befehle können von beiden Clustern ausgegeben werden und gelten für die gesamte DR-Gruppe, die beide Cluster umfasst.

a. Trennen Sie die Verbindungen:

```
metrocluster configuration-settings connection disconnect -dr-group-id  
<dr_group_id>
```

Beispiel

```
cluster_A::~*> metrocluster configuration-settings connection  
disconnect -dr-group-id 1
```

Warning: For the nodes in the DR group 1, this command will remove the existing connections that are used to mirror NV logs and access remote storage.

Do you want to continue? {y|n}: y

Warning: Before proceeding with disconnect, you must verify the following:

1. Unmirrored aggregates do not have disks in remote plexes.

2. Aggregates are not mirrored.

3. No disks are assigned in Pool1.

4. Storage failover is not enabled.

Follow the "MetroCluster Installation and Configuration guide" for detailed instructions to verify this.

Do you want to continue? {y|n}: y

b. Löschen Sie die MetroCluster-Schnittstellen auf den Knoten der alten DR-Gruppe:



Dieser Schritt muss auf jedem Knoten der DR-Gruppe wiederholt werden.

```
metrocluster configuration-settings interface delete
```

a. Löschen Sie die Konfiguration der alten DR-Gruppe.

```
metrocluster configuration-settings dr-group delete
```

7. Heben Sie die Verbindung zu den Knoten in der alten DR-Gruppe auf.

Führen Sie diesen Schritt auf jedem Cluster aus.

a. Legen Sie die erweiterte Berechtigungsebene fest:

```
set -privilege advanced
```

b. Knoten trennen:

```
cluster unjoin -node <node-name>
```

Wiederholen Sie diesen Schritt für den anderen lokalen Knoten in der alten DR-Gruppe.

c. Legen Sie die Administratorberechtigungsstufe fest:

```
set -privilege admin
```

8. Überprüfen Sie, ob Cluster-HA in der neuen DR-Gruppe aktiviert ist. Aktivieren Sie Cluster HA bei Bedarf

erneut:

```
cluster ha modify -configured true
```

Führen Sie diesen Schritt auf jedem Cluster aus.

9. Halten Sie den Vorgang an, schalten Sie ihn aus und entfernen Sie die alten Controller-Module und Storage-Shelves.

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 © 2026 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 IRGEND EINER 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.