Upgrade mithilfe von ARL

Upgrade controllers

NetApp
July 05, 2024

Inhalt

Upgrade mithilfe von ARL

Wählen Sie das ARL-Upgrade aus

In diesem Inhalt wird beschrieben, wie Sie mithilfe von Aggregate Relocation (ARL) ein unterbrechungsfreies Upgrade der Controller-Hardware durchführen.

Weitere Methoden zum Upgrade der Controller-Hardware finden Sie unter "Upgrade durch Verschieben von Volumes oder Storage".

Sie können die Controller-Hardware auf einem Node-Paar mit ONTAP unterbrechungsfrei aktualisieren, indem Sie Aggregate anderer Anbieter von den ursprünglichen Nodes auf die neuen Nodes im selben Cluster migrieren. Auf die Daten, die auf den Nodes gehostet werden, die während des Upgrades zugegriffen werden kann.

ARL bietet sich aus der HA-Konfiguration die Möglichkeit, die Eigentümerschaft von nicht-Root-Aggregaten von einem Node auf einen anderen zu verschieben, wenn sie Storage innerhalb desselben Clusters gemeinsam nutzen.

Es gibt zwei ARL-Methoden für ein Upgrade Ihrer Controller-Hardware unter Verwendung von Systembefehlen oder ein manuelles Upgrade. Bevor Sie beginnen, müssen Sie überprüfen, ob Sie den richtigen Inhalt für die Controller-Hardware-Aktualisierung ausgewählt haben.

Wenn Sie ein Upgrade mithilfe von Systembefehlen durchführen, finden Sie in der folgenden Tabelle:

Wenn Sie diese ONTAP-Version laufen…	**Verwenden Sie…, um ein Upgrade mit Systembefehlen durchzuführen**
9.15.1 oder höher	"Verwenden Sie Befehle zum Ersetzen des System-Controllers, um die mit ONTAP 9.15.1 eingeführte Controller-Hardware zu aktualisieren"
9.10.1 oder höher	"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“" Mit diesem Verfahren können Sie einen AFF-Controller, der als All-SAN-Array (ASA) konfiguriert ist, für bestimmte Modelle und ONTAP-Softwareversionen auf einen ASA-Controller aktualisieren. "Weitere Informationen .".
9.8 oder höher	"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"
9.5 bis 9.7	"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"

Wenn Sie ein manuelles Upgrade durchführen, lesen Sie bitte die folgende Tabelle:

Wenn Sie diese ONTAP-Version laufen…	**Um ein manuelles Upgrade durchzuführen, verwenden Sie…**
9.8 oder höher	"Führen Sie ein manuelles Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durch"
9.0 bis 9.7	"Manuelles Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version"

Verwenden Sie Befehle zum Ersetzen des System-Controllers, um die mit ONTAP 9.15.1 eingeführte Controller-Hardware zu aktualisieren

Überblick

Dieses Verfahren beschreibt das Upgrade der Controller-Hardware mithilfe von Aggregate Relocation (ARL) für die folgenden Systemkonfigurationen:

Methode	ONTAP-Version	Unterstützte Systeme
Wird Verwendet `system controller replace` Befehle	9.15.1 oder höher	"Link zur unterstützten Systemmatrix"

> Sie können dieses Verfahren nicht zum Upgrade einer MetroCluster FC- oder IP-Konfiguration verwenden. Informationen zum Upgrade einer MetroCluster-Konfiguration finden Sie unter, um eine "Quellen" Verknüpfung zur *MetroCluster-Upgrade- und Erweiterungsdokumentation* zu erhalten.

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Außerdem migrieren Sie Daten-logische Schnittstellen (LIFs) und weisen Sie die Netzwerk-Ports auf dem neuen Controller den Schnittstellengruppen zu, während Sie fortfahren.

In diesen Informationen verwendete Terminologie

In dieser Information werden die ursprünglichen Knoten „node1“ und „node2“ genannt und die neuen Knoten „node3“ und „node4“ genannt. Während des beschriebenen Verfahrens wird node1 durch node3 ersetzt und node2 durch node4 ersetzt.

Die Begriffe "node1", "node2", "node3" und "node4" werden nur verwendet, um zwischen den ursprünglichen und den neuen Knoten zu unterscheiden. Wenn Sie das Verfahren befolgen, müssen Sie die richtigen Namen Ihrer ursprünglichen und neuen Knoten ersetzen. In der Realität ändern sich jedoch die Namen der Nodes nicht: node3 hat den Namen node1 und node4 hat nach dem Upgrade der Controller-Hardware den Namen node2.

Wichtige Informationen:

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie müssen auch lesen und verstehen, die "Richtlinien für das Controller-Upgrade mit ARL" Und das "Überblick über das ARL Upgrade" Abschnitte vor Beginn der Aktualisierung.
- Bei dieser Vorgehensweise wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht verwendet wurde. Die erforderlichen Schritte zum Vorbereiten gebrauchter Controller mit dem `wipeconfig` Befehl sind in diesem Verfahren nicht enthalten. Sie müssen sich an den technischen Support wenden, wenn die Ersatz-Controller-Hardware zuvor verwendet wurde.
- Mit diesem Verfahren können Sie die Controller-Hardware in Clustern mit mehr als zwei Nodes aktualisieren. Sie müssen jedoch für jedes Hochverfügbarkeitspaar (HA) im Cluster separat vorgehen.
- Wenn Sie ein Upgrade auf ein in ONTAP 9.15.1 eingeführtes AFF A70, AFF A90 oder AFF A1K System durchführen, konvertiert ONTAP die Storage-Effizienz aller vorhandenen Thin Provisioning Volumes, auch

wenn diese die Storage-Effizienz nicht nutzen, und wendet die neuen Funktionen zur Storage-Effizienz an, die die Hardware-Offload-Funktion nutzen. Dies ist ein automatischer Hintergrundprozess, ohne sichtbare Auswirkungen auf die Leistung des Systems. "Weitere Informationen ."

Automatisierung des Controller-Upgrades

Während eines Controller-Upgrades wird der Controller durch einen anderen Controller ersetzt, auf dem eine neuere oder leistungsstärkere Plattform läuft. Dieser Inhalt enthält die Schritte für das teilweise automatisierte Verfahren, bei dem automatische Netzwerkport-Überprüfungen der Erreichbarkeit durchgeführt werden, um das Upgrade des Controllers noch weiter zu vereinfachen.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

Dieses Verfahren beschreibt, wie Sie die Storage Controller in einem HA-Paar mit neuen Controllern aktualisieren, während die vorhandenen Daten und Festplatten erhalten bleiben. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Sie können dieses Verfahren unter folgenden Umständen verwenden:

- Sie verwenden ONTAP 9.15.1 oder höher.
- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe der Volume-Verschiebung migrieren.
- Sie sind in der Verwaltung von ONTAP erfahren und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.

Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

Sie können dieses Verfahren unter folgenden Umständen nicht verwenden:

- Sie führen ein Upgrade eines AFF A800 auf einen AFF A70 oder AFF A90 durch. Informationen zum Durchführen dieses AFF A800 Upgrades finden Sie unter "Quellen" Link zu den Befehlen „System Controller ersetzen“ verwenden, um Controller-Modelle im gleichen Chassis zu aktualisieren_.
- Sie aktualisieren ein V-Series System oder ein FlexArray Virtualisierungs-Storage-System mit einem externen Array als Back-End Storage. Wenden Sie sich an den technischen Support, wenn Sie Optionen zum Upgrade eines V-Series oder FlexArray Systems benötigen.
- Sie aktualisieren eine MetroCluster FC- oder IP-Konfiguration. Informationen zum Upgrade einer MetroCluster-Konfiguration finden Sie unter, um eine "Quellen" Verknüpfung zur *MetroCluster-Upgrade- und Erweiterungsdokumentation* zu erhalten.

die folgende Tabelle zeigt die unterstützte Modellmatrix für das Controller-Upgrade.

Vorhandene Controller	Ersatz-Controller
AFF A300	AFF A70, AFF A90 und AFF A1K
AFF A400	AFF A70, AFF A90 und AFF A1K
AFF A700	AFF A70, AFF A90 und AFF A1K

Vorhandene Controller	Ersatz-Controller
AFF A900	AFF A90 und AFF A1K

Die AFF A70 und AFF A90 sind integrierte Systeme mit Onboard-Festplatten. Die beiden Controller und Festplatten befinden sich in einem einzelnen Chassis. Sie können ein vorhandenes System nicht aktualisieren, wenn die neuen Controller über interne Laufwerke verfügen.

Wenn die Kombination aus dem Controller-Upgrade-Modell nicht in der oben stehenden Tabelle aufgeführt ist, wenden Sie sich an den technischen Support.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu ONTAP 9 zugreifen können.

Die erforderlichen Tools und Dokumentationen

Sie müssen über spezielle Tools verfügen, um die neue Hardware zu installieren, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren.

Für die Durchführung des Upgrades benötigen Sie die folgenden Tools:

- Erdungsband
- #2 Kreuzschlitzschraubendreher

Wechseln Sie zum "Quellen" Abschnitt für den Zugriff auf die Liste der für dieses Upgrade erforderlichen Referenzdokumente und Referenzsites

Richtlinien für das Controller-Upgrade mit ARL

Ob Sie mit ARL ein Controller-Paar mit ONTAP 9.15.1 oder höher aktualisieren können, hängt von der Plattform und der Konfiguration des ursprünglichen Controllers und der Ersatz-Controller ab.

Unterstützte Upgrades für ARL

Bevor Sie ein Node-Paar mit diesem ARL-Verfahren aktualisieren, überprüfen Sie die folgenden Anforderungen, um sicherzustellen, dass Ihre Konfiguration unterstützt wird:

- Vergewissern Sie sich, dass ARL auf den Original- und Ersatz-Controllern ausgeführt werden kann.
- Prüfen Sie die Größe aller definierten Aggregate und die Anzahl der vom Originalsystem unterstützten Festplatten. Vergleichen Sie dann die Aggregatgröße und die Anzahl der unterstützten Festplatten mit der Aggregatgröße und der Anzahl der vom neuen System unterstützten Festplatten. Unter "Quellen" finden Sie einen Link zum *Hardware Universe*, wo diese Informationen verfügbar sind. Die Aggregatgröße und die Anzahl der vom neuen System unterstützten Festplatten müssen gleich oder größer sein als die Aggregatgröße und Anzahl der vom ursprünglichen System unterstützten Festplatten.
- In den Cluster-Mischungsregeln validieren, ob neue Nodes nach Austausch des ursprünglichen Controllers

mit den vorhandenen Nodes Teil des Clusters werden können. Weitere Informationen zu den Mischregeln für Cluster finden Sie unter "Quellen" , um mit dem *Hardware Universe* zu verlinken.

- Migrieren Sie die Cluster-LIFs und wechseln Sie zu zwei Cluster-Ports pro Node, wenn Sie über ein System wie z. B. AFF 700 mit der folgenden Konfiguration verfügen:
- Mehr als zwei Cluster-Ports pro Node
- Eine Cluster-Interconnect-Karte in Steckplatz 4 im Breakout-Modus zur Erstellung der Ports e4a, e4b, e4c und e4d sowie der Ports e4e, e4f, e4g und e4h

> Ein Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node kann nach dem Upgrade zu fehlenden Cluster-LIFs auf dem neuen Controller führen.

Weitere Informationen finden Sie im Knowledge Base-Artikel "So löschen Sie unerwünschte oder unnötige Cluster-LIFs".

Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise und SnapLock Compliance Volumes konfiguriert sind.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren.

Upgrades werden für ARL nicht unterstützt

Sie können keine Ersatz-Controller aufrüsten, die die mit den ursprünglichen Controllern verbundenen Festplatten-Shelfs nicht unterstützen.

Siehe "Quellen" Um Informationen zur Hardware Universe Festplattenunterstützung zu erhalten.

Wenn Sie Controller der Einstiegsklasse mit internen Laufwerken aktualisieren möchten, finden Sie unter "Quellen" Link zu *Upgrade by moving Volumes or Storage* und gehen Sie zum Verfahren *Upgrade eines Node-Paares, auf dem Clustered Data ONTAP ausgeführt wird, indem Sie Volumes verschieben*.

Fehlerbehebung

Wenn beim Aktualisieren der Controller Probleme auftreten, finden Sie weitere Informationen und mögliche Lösungen unter "Fehlerbehebung" .

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Überblick über das ARL Upgrade

Bevor Sie die Nodes mit ARL aktualisieren, sollten Sie unbedingt verstehen, wie das Verfahren funktioniert. In diesem Inhalt wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und dann für die ursprünglichen und die neuen Nodes eine Reihe von Schritten ausführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Beschreibung
"Stufe 1: Upgrade vorbereiten"	In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Sie müssen bestimmte Informationen aufzeichnen, wenn Sie Storage-Verschlüsselung mithilfe des OKM managen und Sie die SnapMirror Beziehungen stilllegen möchten. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate. • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate.
"Stufe 2: Knoten1 verschieben und ausmustern"	Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie erfassen Node1-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node1. Sie können sich auch später beim Verfahren auf den Netzboot node3 und node4 vorbereiten. Gesamteigentum am Ende von Phase 2: • Node2 ist der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.

Stufe	Beschreibung
"Phase 3: Installieren und booten Sie node3"	In Phase 3 installieren und booten Sie node3, überprüfen, ob die Cluster- und Node-Management-Ports von node1 auf node3 online geschaltet sind, und überprüfen Sie die Installation von node3. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind. Gesamteigentum am Ende von Stufe 3: • Node3 ist der Hausbesitzer und der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 4: Knoten2 verschieben und ausmustern"	Während Phase 4 werden Aggregate und NAS-Daten-LIFs von Knoten 2 auf Knoten 3 verschoben. Sie erfassen auch node2-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node2. Gesamteigentum am Ende von Stufe 4: • Node3 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehörten. • Node2 ist der Hausbesitzer von node2 Aggregaten. • Node3 ist der aktuelle Besitzer von node2 Aggregaten.
"Phase 5: installieren und booten sie node4"	In Phase 5 installieren und booten Sie node4, überprüfen, ob die Cluster- und Node-Management-Ports von node2 auf node4 online geschaltet sind, und überprüfen Sie die Installation von node4. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind. Gesamteigentum am Ende von Stufe 5: • Node3 ist der Hausbesitzer und aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Node4 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Phase 6: Schließen Sie das Upgrade ab"	In Phase 6 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden. Und wenn die neuen Nodes verschlüsselt sind, konfigurieren und einrichten Sie Storage Encryption oder NVE. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Außerdem zeichnen Sie bestimmte Informationen auf, wenn Sie Storage-Verschlüsselung mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten.

Schritte

1. "Bereiten Sie die Knoten für ein Upgrade vor"
2. "Management der Storage-Verschlüsselung mit dem Onboard Key Manager"

Bereiten Sie die Knoten für ein Upgrade vor

Der Prozess des Controller-Austauschs beginnt mit einer Reihe von Vorabprüfungen. Sie sammeln auch Informationen über die ursprünglichen Nodes, die Sie später verwenden können. Falls erforderlich, ermitteln Sie den Typ der verwendeten Self-Encrypting Drives.

Schritte

1. Starten Sie den Controller-Ersatzprozess, indem Sie den folgenden Befehl in die ONTAP-Befehlszeile eingeben:

   ```
   system controller replace start -nodes <node_names>
   ```

   Sie können den Befehl „Ersetzen des System-Controllers“ nur auf der erweiterten Berechtigungsebene ausführen: `set -privilege advanced`

   Es wird eine Ausgabe wie im folgenden Beispiel angezeigt. In der Ausgabe wird die auf dem Cluster ausgeführte ONTAP-Version angezeigt:

```
Warning: 1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller
replacement supports only ARL based procedure.
Do you want to continue? {y|n}: y
```

2. Drücken Sie `y`, Sie sehen die folgende Ausgabe:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

Das System führt die folgenden Vorabprüfungen durch. Notieren Sie die Ausgabe jeder Vorabprüfung zur Verwendung im weiteren Verlauf des Verfahrens:

Pre-Check	Beschreibung
Cluster-Integritätsprüfung	Überprüft alle Nodes im Cluster, um sicherzustellen, dass sie sich in einem ordnungsgemäßen Zustand befinden.
Statusprüfung Der Aggregatverschiebung	Überprüft, ob eine Aggregatverschiebung bereits erfolgt. Wenn eine weitere Aggregatverschiebung erfolgt, schlägt die Prüfung fehl.
Modellname Prüfen	Überprüft, ob die Controller-Modelle bei diesem Verfahren unterstützt werden. Wenn die Modelle nicht unterstützt werden, schlägt die Aufgabe fehl.
Cluster-Quorum-Prüfung	Überprüft, ob die zu ersetzenden Nodes sich in Quorum befinden. Wenn sich die Knoten nicht im Quorum befinden, schlägt die Aufgabe fehl.

Pre-Check	Beschreibung
Überprüfung Der Bildversion	Überprüft, ob die zu ersetzenden Nodes dieselbe Version von ONTAP ausführen. Wenn sich die ONTAP-Image-Versionen unterscheiden, schlägt die Aufgabe fehl. Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version von ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation als Netzboot einsetzen. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.
HA-Statusüberprüfung	Überprüft, ob beide Nodes, die ersetzt werden, in einer HA-Paar-Konfiguration mit Hochverfügbarkeit vorhanden sind. Wenn das Speicher-Failover für die Controller nicht aktiviert ist, schlägt die Aufgabe fehl.
Aggregatstatus-Prüfung	Wenn die Nodes ersetzt werden, eigene Aggregate, für die sie nicht der Home-Inhaber sind, schlägt die Aufgabe fehl. Die Nodes sollten nicht im Besitz von nicht lokalen Aggregaten sein.
Überprüfung Des Festplattenstatus	Wenn zu ersetzende Knoten keine oder fehlerhafte Festplatten haben, schlägt die Aufgabe fehl. Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.
LIF-Statusüberprüfung von Daten	Überprüft, ob für einen der zu ersetzenden Nodes keine lokalen Daten-LIFs vorhanden sind. Die Nodes sollten keine Daten-LIFs enthalten, für die sie nicht der Home-Inhaber sind. Wenn einer der Nodes nicht-lokale Daten-LIFs enthält, schlägt die Aufgabe fehl.
LIF-Status des Clusters	Überprüft, ob die Cluster-LIFs für beide Nodes aktiv sind. Wenn die Cluster-LIFs ausgefallen sind, schlägt die Aufgabe fehl.
ASUP-Statusprüfung	Wenn ASUP Benachrichtigungen nicht konfiguriert sind, schlägt die Aufgabe fehl. Sie müssen AutoSupport aktivieren, bevor Sie mit dem Austausch des Controllers beginnen.
CPU-Auslastungs-Prüfung	Überprüft, ob die CPU-Auslastung bei allen zu ersetzenden Nodes mehr als 50 % beträgt. Wenn die CPU-Nutzung über einen erheblichen Zeitraum mehr als 50 % beträgt, schlägt die Aufgabe fehl.
Aggregatrekonstruktion	Überprüft, ob bei beliebigen Datenaggregaten eine Rekonstruktion durchgeführt wird. Wenn die Aggregatrekonstruktion ausgeführt wird, schlägt die Aufgabe fehl.
Knoten Affinität Job Überprüfung	Überprüft, ob Jobs mit Knotenorientierung ausgeführt werden. Wenn Knotenaffinitätsjobs ausgeführt werden, schlägt die Prüfung fehl.

3. Wenn der Controller-Ersatzvorgang gestartet und die Vorabprüfungen abgeschlossen sind, hält der Vorgang die Aktivierung ein, damit Sie die Ausgabeinformationen, die Sie später bei der Konfiguration von node3 benötigen könnten, sammeln können.

Bevor Sie mit dem Upgrade beginnen, migrieren Sie die Cluster-LIFs und erstellen Sie sie wieder zu zwei Cluster-Ports pro Node, wenn Sie über ein System, z. B. AFF 700, mit der folgenden Konfiguration verfügen:

- Mehr als zwei Cluster-Ports pro Node
- Eine Cluster-Interconnect-Karte in Steckplatz 4 im Breakout-Modus zur Erstellung der Ports e4a, e4b, e4c und e4d sowie der Ports e4e, e4f, e4g und e4h

Ein Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node kann nach dem Upgrade zu fehlenden Cluster-LIFs auf dem neuen Controller führen.

Weitere Informationen finden Sie im Knowledge Base-Artikel "So löschen Sie unerwünschte oder unnötige Cluster-LIFs".

4. Führen Sie den folgenden Befehlssatz aus, wie durch das Verfahren zum Austausch des Controllers auf der Systemkonsole gesteuert.

   Führen Sie von dem seriellen Port aus, der mit jedem Node verbunden ist, und speichern Sie die Ausgabe der folgenden Befehle einzeln:

   - `vserver services name-service dns show`
   - `network interface show -curr-node <local> -role <cluster,intercluster,node-mgmt,cluster-mgmt,data>`
   - `network port show -node <local> -type physical`
   - `service-processor show -node <local> -instance`
   - `network fcp adapter show -node <local>`
   - `network port ifgrp show -node <local>`
   - `system node show -instance -node <local>`
   - `run -node <local> sysconfig`
   - `storage aggregate show -r`
   - `storage aggregate show -node <local>`
   - `volume show -node <local>`
   - `system license show -owner <local>`
   - `storage encryption disk show`
   - `security key-manager onboard show-backup`
   - `security key-manager external show`
   - `security key-manager external show-status`
   - `network port reachability show -detail -node <local>`

   Wenn NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) mit dem Onboard Key Manager (OKM) verwendet wird, halten Sie die Passphrase bereit, um später im Verfahren die Neusynchronisierung des Schlüsselmanagers abzuschließen.

5. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:

   - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
   - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

   "Weitere Informationen zu unterstützten Self-Encrypting Drives".

Korrigieren Sie die Aggregateigentümer bei Ausfall einer ARL-Vorabprüfung

Wenn die aggregierte Statusprüfung fehlschlägt, müssen Sie Aggregate des Partner-Node an den Node „Home-Owner“ zurückgeben und den Vorabprüfvorgang erneut initiieren.

Schritte

1. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

   `storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *`

2. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Nachdem Sie fertig sind

Sie müssen den Controller-Ersatzprozess neu starten:

`system controller replace start -nodes node_names`

Lizenz

Ausführliche Informationen zur ONTAP-Lizenzierung finden Sie unter "Lizenzmanagement".

> Wenn Sie nicht lizenzierte Funktionen auf dem Controller verwenden, kann es sein, dass Sie Ihre Lizenzvereinbarung nicht einhalten.

Management der Storage-Verschlüsselung mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung der Schlüssel verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager onboard show-backup` Befehl.

Stilllegen der SnapMirror Beziehungen (optional)

Bevor Sie mit dem Verfahren fortfahren, müssen Sie bestätigen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   > Wenn der Status „Übertragen“ lautet, müssen Sie diese Transfers abbrechen: `snapmirror abort -destination-vserver` *`vserver_name`*

   Der Abbruch schlägt fehl, wenn sich die SnapMirror-Beziehung nicht im Zustand „Übertragen“ befindet.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Stufe 2: Knoten1 verschieben und ausmustern

Phase-2-Übersicht

Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie zeichnen auch die

erforderlichen node1-Informationen auf, nehmen Node1 außer Betrieb und bereiten den Netzboot node3 und node4 später im Verfahren vor.

Schritte

1. "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2"
2. "Verschiebung ausgefallener oder Vetos von Aggregaten"
3. "Node1 ausmustern"
4. "Vorbereitungen für den Netzboot"

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2

Bevor Sie node1 durch Node3 ersetzen können, müssen Sie die nicht-Root-Aggregate und NAS-Daten-LIFs von node1 auf node2 verschieben, bevor Sie die Ressourcen von node1 schließlich in node3 verschieben.

Bevor Sie beginnen

Der Vorgang sollte bereits angehalten werden, wenn Sie mit der Aufgabe beginnen. Sie müssen den Vorgang manuell fortsetzen.

Über diese Aufgabe

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. In dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in node3 migriert werden.

> Der Home-Inhaber für die Aggregate und LIFs wird nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Wiederaufnahme der Vorgänge für die Aggregatverschiebung und die LIF-Verschiebung von NAS-Daten:

   ```
   system controller replace resume
   ```

   Alle Aggregate ohne Root-Root-Root-Root-Daten und LIFs werden von node1 auf node2 migriert.

   Der Vorgang angehalten, damit Sie überprüfen können, ob alle node1-Aggregate und LIFs für nicht-SAN-Daten in node2 migriert wurden.

2. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   ```
   system controller replace show-details
   ```

3. Wenn der Vorgang noch angehalten wird, vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind, damit ihr Status bei node2 lautet:

   ```
   storage aggregate show -node node2 -state online -root false
   ```

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

```
cluster::> storage aggregate show -node node2 state online -root false

Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
---------  -------  ---------  -----  ------ -----  ------
--------------
aggr_1     744.9GB  744.8GB    0%     online     5  node2
raid_dp,normal
aggr_2     825.0GB  825.0GB    0%     online     1  node2
raid_dp,normal
2 entries were displayed.
```

Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

`storage aggregate online -aggregate` *`aggr_name`*

4. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 verwenden und seine Ausgabe überprüfen:

   `volume show -node` *`node2`* `-state offline`

   Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

   `volume online -vserver` *`vserver_name`* `-volume` *`volume_name`*

   Der *`vserver_name`* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

5. Wenn irgendeine LIFs inaktiv sind, setzen Sie den Administratorstatus der LIFs auf `up` Mit dem folgenden Befehl, so wie es für jedes LIF ist:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`nodename`* `-status-admin up`

Verschiebung ausgefallener oder Vetos von Aggregaten

Falls Aggregate nicht verschoben oder ein Vetos ausfällt, müssen sie die Aggregate manuell verschieben oder, falls erforderlich, die Vetos oder Zielprüfungen überschreiben.

Über diese Aufgabe

Der Umzugsvorgang wird aufgrund des Fehlers angehalten.

Schritte

1. Überprüfen Sie die EMS-Protokolle (Event Management System), um festzustellen, warum das Aggregat nicht verschoben oder gegen ein Vetos eingesetzt wurde.
2. Verschiebung ausgefallener oder Vetos von Aggregaten:

   `storage aggregate relocation start -node` *`node1`* `-destination` *`node2`* `-aggregate`

```
-list aggr_name -ndo-controller-upgrade true
```

3. Geben Sie bei der entsprechenden Aufforderung ein `y`.
4. Sie können die Verschiebung mit einer der folgenden Methoden erzwingen:

Option	Beschreibung
Veto-Prüfungen werden überschrieben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true`
Zielprüfungen überschreiben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true`

Node1 ausmustern

Um „node1“ außer Betrieb zu nehmen, setzen Sie den automatischen Vorgang fort, um das HA-Paar mit node2 zu deaktivieren und node1 ordnungsgemäß herunterzufahren. Später im Verfahren entfernen Sie Knoten 1 aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

```
system controller replace resume
```

2. Vergewissern Sie sich, dass node1 angehalten wurde:

```
system controller replace show-details
```

Nachdem Sie fertig sind

Sie können Node1 nach Abschluss des Upgrades außer Betrieb nehmen. Siehe "Ausmustern des alten Systems".

Vorbereitungen für den Netzboot

Nachdem Sie später noch Node3 und node4 physisch gerast haben, müssen Sie sie eventuell als Netzboot Netboot eingesetzt werden. Der Begriff „Netzboot“ bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf den Netzboot legen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver, auf den das System zugreifen kann.

Sie können auch die USB-Boot-Option verwenden, um einen Netzboot durchzuführen. Weitere Informationen finden Sie im Knowledge Base-Artikel "So verwenden Sie den Boot_Recovery-LOADER-Befehl zum Installieren von ONTAP für die Ersteinrichtung eines Systems".

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Siehe "Quellen" Um eine Verknüpfung zur NetApp Support-Website zu erhalten und die erforderlichen Systemdateien für Ihre Plattform und die richtige Version von ONTAP herunterzuladen.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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. Rufen Sie die NetApp Support Site auf, um die Dateien zum Netzboot des Systems herunterzuladen.
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. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

   Ihre Verzeichnisliste sollte die folgende Datei enthalten:
   `<ontap_version>_image.tgz`

   Sie müssen den Inhalt des nicht extrahieren `<ontap_version>_image.tgz` Datei:

   Sie verwenden die Informationen in den Verzeichnissen in "Phase 3".

Phase 3: Installieren und booten Sie node3

Phase-3-Übersicht

In Phase 3 installieren und booten Sie node3, überprüfen, ob die Cluster- und Node-Management-Ports von node1 auf node3 online geschaltet sind, und überprüfen Sie die Installation von node3. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Schritte

1. "Installieren und booten Sie node3"
2. "Überprüfen Sie die Installation von node3"
3. "Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3"
4. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3"

Installieren und booten Sie node3

Sie installieren node3 im Rack, übertragen die Verbindungen von node1 zu node3,

starten node3 und installieren ONTAP. Sie weisen dann alle Spare-Festplatten von node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate neu zu, die zu einem früheren Zeitpunkt nicht zu node2 verschoben wurden, wie in diesem Abschnitt beschrieben.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Außerdem müssen Sie überprüfen, ob die SAN LIFs erfolgreich online geschaltet wurden und den korrekten physischen FC-Ports in Knoten3 zugewiesen wurden.

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

   Die Platz- und Höhenanforderungen der neuen Nodes können sich von den vorhandenen Nodes unterscheiden. Planen Sie den Platzbedarf für Ihr Upgrade-Szenario.

2. Installieren Sie node3 im Rack und befolgen Sie die Anweisungen *Installation und Setup* für Ihr Node-Modell.
3. Kabelnode3, Verschieben der Verbindungen von node1 nach node3.

   Ab ONTAP 9.15.1 verfügen neue Controller-Modelle über nur einen „Schraubenschlüssel“ Port für den Baseboard Management Controller (BMC) und Management-Verbindungen. Planen Sie die Verkabelungsänderungen entsprechend.

   - Konsole (Remote-Management-Port)
   - Cluster- und HA-Ports
   - Datenports
   - Cluster- und Node-Management-Ports
   - Serial-Attached SCSI (SAS)- und Ethernet-Storage-Ports
   - SAN-Konfigurationen: ISCSI-Ethernet-, FC- und NVMe/FC-Switch-Ports

   Möglicherweise müssen Sie die Verbindungskabel zwischen den alten und den neuen Controllern ändern, um die Interoperabilität zwischen den verschiedenen Controller- und Kartenmodellen zu ermöglichen. Eine Verkabelungskarte der Ethernet-Storage-Shelfs für Ihre Systeme finden Sie im "Verfahren zur Systeminstallation" .

   Für ab ONTAP 9.15.1 eingeführte Controller verwenden Cluster und HA Interconnects die gleichen Ports. Bei Switch-verbundenen Konfigurationen müssen ähnliche Ports mit denselben Cluster-Switches verbunden werden. Wenn Sie beispielsweise von einem vorhandenen Controller auf einen AFF A1K aktualisieren, sollten Sie die e1a-Ports beider Nodes mit einem Switch und die e7a-Ports beider Nodes mit dem zweiten Switch verbinden.

4. Einschalten Sie den Netzstrom auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an

der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. Wenn die Warnmeldung in angezeigt wird Schritt 4, Nehmen Sie die folgenden Aktionen:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.

Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Ist der Domain-Name (DNS) (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Netzboot auf Node3 durchführen:

```
netboot http://<web_server_ip/path_to_web-
accessible_directory>/<ontap_version>_image.tgz
```

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` Im Abschnitt "Vorbereitungen für den Netzboot".

Unterbrechen Sie den Startvorgang nicht.

8. im Startmenü Option wählen `(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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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. Vervollständigen Sie die folgenden Teilschritte, um das Controller-Modul neu zu starten:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie den Wartungsmodus aus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12.] Überprüfen Sie, ob Controller und Chassis als ha konfiguriert sind:

    ```
    ha-config show
    ```

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn der Controller und das Chassis nicht als ha konfiguriert sind, korrigieren Sie die Konfiguration mit den folgenden Befehlen:

    ```
    ha-config modify controller ha

    ha-config modify chassis ha
    ```

14. Vergewissern Sie sich, dass alle Ethernet-Ports, die zur Verbindung mit den Ethernet-Shelfs verwendet werden, als Speicher konfiguriert sind:

    ```
    storage port show
    ```

    Die angezeigte Ausgabe hängt von der Systemkonfiguration ab. Das folgende Ausgabebeispiel gilt für einen Knoten mit einer einzelnen Speicherkarte in Steckplatz 11. Die Ausgabe für Ihr System kann unterschiedlich sein:

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Ändern Sie die Ports, die nicht auf Speicher festgelegt sind:

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

    Alle mit Storage Shelfs verbundenen Ethernet-Ports müssen als Storage konfiguriert werden, um den Zugriff auf Festplatten und Shelfs zu ermöglichen.

16. Beenden des Wartungsmodus:

    `halt`

    Unterbrechen Sie den Autoboot, indem Sie auf drücken `Ctrl-C` An der Eingabeaufforderung für die Boot-Umgebung.

17. Überprüfen Sie in node2 das Systemdatum, die Uhrzeit und die Zeitzone:

    `date`

18. Überprüfen Sie bei node3 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    `show date`

19. Stellen Sie bei Bedarf das Datum auf Knoten 3 ein:

    `set date <mm/dd/yyyy>`

20. Überprüfen Sie bei node3 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    `show time`

21. Stellen Sie bei Bedarf die Zeit auf node3 ein:

    `set time <hh:mm:ss>`

22. Legen Sie im Boot-Loader die Partner-System-ID auf node3 fest:

    `setenv partner-sysid <node2_sysid>`

    Für Knoten 3, `partner-sysid` Muss der von node2 sein.

    a. Einstellungen speichern:

       `saveenv`

23. Überprüfen Sie den `partner-sysid` Für Knoten 3:

```
printenv partner-sysid
```

24. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.

> Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	**Dann…**
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

25. Boot-Node im Startmenü:

```
boot_ontap menu
```

26. Gehen Sie auf node3 zum Boot-Menü und wählen Sie mit 22/7 die versteckte Option aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node1 ein, um die Festplatten von node1 node3 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
```

```
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes
.
<output truncated>
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
<output truncated>
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
```

```
<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:
```

Im obigen Beispiel der Konsolenausgabe werden Sie von ONTAP aufgefordert, den Namen des Partner-Node anzugeben, wenn das System ADP-Festplatten (Advanced Disk Partitioning) verwendet.

27. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, zeigt dies an, dass ein Problem mit der Neuzuweisung der Festplatte aufgetreten ist. Informationen zur Behebung des Problems finden Sie unter "Fehlerbehebung" .
28. Drücken Sie `Ctrl-C` während des Autoboots, um den Knoten an der Eingabeaufforderung anzuhalten `LOADER>` .
29. Wechseln Sie an der LOADER-Eingabeaufforderung in den Wartungsmodus:

    ```
    boot_ontap maint
    ```

30. Überprüfen Sie die Festplattenkonnektivität, den Controller-Modell-String, die HA-Konfiguration und andere Details zur Hardware-Konnektivität.
31. Beenden des Wartungsmodus:

    ```
    halt
    ```

32. Starten Sie an der LOADER-Eingabeaufforderung:

    ```
    boot_ontap menu
    ```

    Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

    Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her.

Dies gilt nur, wenn das Root-Volume NetApp-Volume-Verschlüsselung verwendet.

a. Zurück zum speziellen Startmenü:
`LOADER> boot_ontap menu`

```
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)? 10
```

b. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

c. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

e. Geben Sie bei Aufforderung die Backup-Daten ein.

Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

f. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 32 , bis das System ordnungsgemäß gebootet wird.

Überprüfen Sie die Installation von node3

Sie müssen überprüfen, ob die physischen Ports von node1 den physischen Ports auf node3 korrekt zugeordnet sind. Dadurch kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Abhängig vom Modell der Nodes kann das physische Port-Layout variieren. Wenn der neue Node gestartet wird, versucht ONTAP, zu ermitteln, welche Ports die Cluster LIFs hosten sollten, damit es automatisch zu Quorum kommt.

Wenn die physischen Ports auf node1 nicht direkt den physischen Ports auf node3 zugeordnet werden, wird der folgende Abschnitt angezeigt Stellen Sie die Netzwerkkonfiguration auf node3 wieder her Muss zur Reparatur der Netzwerkverbindung verwendet werden.

Nach der Installation und dem Booten von node3 müssen Sie überprüfen, ob die Installation korrekt ist. Sie müssen warten, bis Knoten 3 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen.

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node3 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node3 dem Quorum beigetreten ist:

   ```
   cluster show -node node3 -fields health
   ```

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node3 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Wechseln Sie in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

4. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand wie zuvor in node1 befand, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

   ```
   system controller replace show
   ```

   ```
   system controller replace show-details
   ```

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Austausch des Controllers wird anhand der folgenden Meldung unterbrochen:

```
Cluster::*> system controller replace show
Node             Status                       Error-Action
---------------- ------------------------
---------------------------------
Node1(now node3) Paused-for-intervention      Follow the instructions
given in
                                              Step Details
Node2                      None

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.

2 entries were displayed.
```

In diesem Verfahren wurde der Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node3_ umbenannt.

7. Wenn der Controller-Austausch im Status „Pause“ steht, fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, um die Netzwerkkonfiguration auf dem Node wiederherzustellen.

Stellen Sie die Netzwerkkonfiguration auf node3 wieder her

Nachdem Sie bestätigt haben, dass node3 sich im Quorum befindet und mit node2 kommunizieren kann, überprüfen Sie, ob node1 VLANs, Interface Groups und Broadcast-Domains auf node3 zu sehen sind. Überprüfen Sie außerdem, ob alle node3-Netzwerk-Ports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Verknüpfen mit *Network Management*.

Schritte

1. Listen Sie alle physischen Ports auf, die auf dem aktualisierten Knoten 1 (als Knoten 3 bezeichnet) sind:

```
network port show -node node3
```

Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. In dieser Ausgabe sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um zu entscheiden, welche Ports als Ports für Schnittstellengruppen, VLAN-Basis-Ports oder eigenständige physische Ports zum Hosten von LIFs verwendet werden müssen.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node3 auflisten:

```
network port reachability show
```

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
ClusterA::*> network port reachability show
Node      Port     Expected Reachability               Reachability
Status
--------- -------- ------------------------------------
---------------------
node1_node3
          e0M      Default:Mgmt                        ok
          e10a     Default:Default                     ok
          e10b     -                                   no-reachability
          e10c     Default:Default                     ok
          e10d     -                                   no-reachability
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
node2_node4
          e0M      Default:Mgmt                        ok
          e4a      Default:Default                     ok
          e4b      -                                   no-reachability
          e4c      Default:Default                     ok
          e4d      -                                   no-reachability
          e3a      Cluster:Cluster                     ok
          e3b      Cluster:Cluster                     ok
18 entries were displayed.
```

Im vorherigen Beispiel wird node1_node3 kurz nach dem Austausch des Controllers gestartet. Einige Ports verfügen nicht über die Fähigkeit, ihre zu erwartenden Broadcast-Domänen zu erreichen und müssen repariert werden.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node3 mit einem anderen Status als der Erreichbarkeit `ok`. Führen Sie den folgenden Befehl aus, zuerst auf beliebigen physischen Ports, dann auf

beliebigen VLAN-Ports, nacheinander:

`network port reachability repair -node <node_name> -port <port_name>`

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node1_node3 -port e4a
```

```
Warning: Repairing port "node1_node3: e4a" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Wie oben dargestellt, wird eine Warnmeldung für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Wiederachbarkeit der Broadcast-Domain unterscheiden können, wo sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

`network port reachability show`

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Wenn die Konfiguration der Schnittstellengruppe nicht mit dem physischen Portlayout des neuen Controllers übereinstimmt, ändern Sie diese mit den folgenden Schritten.

   a. Sie müssen zunächst physische Ports entfernen, die als Ports für Schnittstellengruppen von ihrer Broadcast-Domain-Mitgliedschaft verwendet werden sollen. Dazu verwenden Sie den folgenden Befehl:

      `network port broadcast-domain remove-ports -broadcast-domain <broadcast-domain_name> -ports <node_name:port_name>`

   b. Hinzufügen eines Mitgliedports zu einer Schnittstellengruppe:

      `network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port <port_name>`

   c. Die Schnittstellengruppe wird der Broadcast-Domäne automatisch ca. eine Minute nach dem Hinzufügen des ersten Mitgliedports hinzugefügt.

   d. Vergewissern Sie sich, dass die Schnittstellengruppe der entsprechenden Broadcast-Domäne hinzugefügt wurde:

      `network port reachability show -node <node_name> -port <ifgrp>`

      Wenn der Status der Erreichbarkeit der Schnittstellengruppe nicht lautet `ok`, Weisen Sie es der entsprechenden Broadcast-Domain zu:

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. Weisen Sie der Broadcast-Domäne geeignete physische Ports zu `Cluster` , indem Sie die folgenden Schritte ausführen:

   a. Ermitteln Sie, welche Ports eine Reachability zum haben `Cluster` Broadcast-Domäne:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Reparieren Sie jeden Port mit Erreichbarkeit zum `Cluster` Broadcast-Domäne, wenn ihr Status der Erreichbarkeit nicht lautet `ok`:

      ```
      network port reachability repair -node <node_name> -port <port_name>
      ```

7. Verschieben Sie die verbleibenden physischen Ports in ihre richtigen Broadcast-Domänen mithilfe eines der folgenden Befehle:

   ```
   network port reachability repair -node <node_name> -port <port_name>

   network port broadcast-domain remove-port

   network port broadcast-domain add-port
   ```

   Vergewissern Sie sich, dass keine unerreichbaren oder unerwarteten Ports vorhanden sind. Überprüfen Sie den Status der Erreichbarkeit aller physischen Ports mithilfe des folgenden Befehls und überprüfen Sie die Ausgabe, um sicherzustellen, dass der Status lautet `ok`:

   ```
   network port reachability show -detail
   ```

8. Stellen Sie alle VLANs wieder her, die möglicherweise verschoben wurden, indem Sie die folgenden Schritte ausführen:

   a. Versetzte VLANs auflisten:

      ```
      cluster controller-replacement network displaced-vlans show
      ```

      Die Ausgabe sollte wie folgt angezeigt werden:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                Original
      Node      Base Port   VLANs
      --------  ----------  ----------------------------------------
      Node1       a0a       822, 823
                  e4a       822, 823
      2 entries were displayed.
      ```

   b. Stellen Sie VLANs wieder her, die von ihren früheren Basis-Ports verdrängt wurden:

      ```
      cluster controller-replacement network displaced-vlans restore
      ```

Das folgende Beispiel zeigt die Wiederherstellung von VLANs, die aus der Schnittstellengruppe „a0a“ wieder in dieselbe Schnittstellengruppe verschoben wurden:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

Das folgende Beispiel zeigt die Wiederherstellung von verlagerten VLANs am Port „e9a“ an' e9d:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

Wenn eine VLAN-Wiederherstellung erfolgreich ist, werden die verschobenen VLANs auf dem angegebenen Zielport erstellt. Die VLAN-Wiederherstellung schlägt fehl, wenn der Zielport Mitglied einer Schnittstellengruppe ist oder der Zielport nicht verfügbar ist.

Warten Sie etwa eine Minute, bis neu wiederhergestellte VLANs in ihren entsprechenden Broadcast-Domänen platziert werden.

a. Erstellen Sie bei Bedarf neue VLAN-Ports für VLAN-Ports, die nicht im enthalten sind `cluster controller-replacement network displaced-vlans show` Ausgabe sollte aber auf anderen physischen Ports konfiguriert werden.

9. Löschen Sie alle leeren Broadcast-Domänen, nachdem alle Port-Reparaturen abgeschlossen wurden:

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

10. Überprüfung der Anschlussfähigkeit:

    `network port reachability show`

    Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn ein Port einen anderen Status als diese beiden meldet, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

11. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

    `network port show`

12. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

    `network port broadcast-domain show`

13. Stellen Sie die LIF-Start-Ports wieder her und geben Sie ggf. den Vserver(s) und die Home Ports von LIFs an, die über folgende Schritte wiederhergestellt werden müssen:

    a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

b. LIF-Home-Knoten und Home-Ports wiederherstellen:

```
cluster controller-replacement network displaced-interface restore-home-node
-node <node_name> -vserver <vserver_name> -lif-name <LIF_name>
```

14. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

```
network interface show -fields home-port, status-admin
```

Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3

Wenn Sie mithilfe von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Volumes auf dem System verschlüsseln, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht synchronisieren, können beim Verschieben der Node1-Aggregate mit ARL von node2 auf node3 Ausfälle auftreten, da node3 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie den folgenden Befehl von node3 aus:

```
security key-manager onboard sync
```

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node3 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK
```

Beispiel

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node3    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3

Nachdem Sie die Netzwerkkonfiguration auf node3 und bevor Sie Aggregate von node2 auf node3 verschoben haben, müssen Sie überprüfen, ob die NAS-Daten-LIFs, die zu node1 gehören und sich derzeit auf node2 befinden, von node2 in node3 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Die iSCSI LIFs finden automatisch die richtigen Home Ports mithilfe der Erreichbarkeit. Die FC- und NVMe/FC-SAN-LIFs werden nicht automatisch verschoben. Sie zeigen weiterhin den Home-Port an, an dem sie vor dem Upgrade waren.

   Prüfen Sie die SAN LIFs auf Knoten3:

   a. Ändern Sie alle iSCSI SAN LIFs, die über einen „down“-Status für die neuen Daten-Ports verfügen:

      ```
      network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down

      network interface modify -vserver <vserver> -lif <iscsi_san_lif> port
      <new_port> node <node>

      network interface modify -vserver <vserver> -lif <iscsi_san_lif>
      ```

   b. Ändern Sie alle FC- und NVMe/FC-SAN-LIFs, die den neuen Controller Zuhause haben, und melden Sie den Betriebsstatus der FCP-Ports am neuen Controller an:

      ```
      network interface modify -vserver <vserver> -lif <fc_san_lif> admin down

      network interface modify -vserver <vserver> -lif <fc_san_lif> port
      ```

```
<new_port> node <node>

network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

3. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen verschiebt das System die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf den neuen Controller, node3. Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

4. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   ```
   system controller replace show-details
   ```

   Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

5. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

   ```
   cluster controller-replacement network displaced-interface show
   ```

   Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in Knoten 3 wieder her:

   ```
   cluster controller-replacement network displaced-interface restore-home-node
   ```

6. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung
- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster
- Lautstärkerprüfung

Phase 4: Knoten2 verschieben und ausmustern

Phase-4-Übersicht

Während Phase 4 werden Aggregate und NAS-Daten-LIFs von Knoten 2 auf Knoten 3 verschoben. Sie zeichnen auch die erforderlichen node2-Informationen für die spätere Verwendung im Verfahren auf und ziehen dann node2 zurück.

Schritte

1. "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3"
2. "Node2 ausmustern"

Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3

Bevor Sie node2 durch node4 ersetzen, verschieben Sie die nicht-Root-Aggregate und NAS-Daten-LIFs, die im Besitz von node2 sind, auf node3.

Bevor Sie beginnen

Nach den Nachprüfungen aus der vorherigen Phase wird automatisch die Ressourcenfreigabe für node2 gestartet. Die Aggregate außerhalb des Root-Bereichs und LIFs für nicht-SAN-Daten werden von node2 auf node3 migriert.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich.

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. In dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in node3 migriert werden.

Der Home-Inhaber für die Aggregate und LIFs werden nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind und ihren Status auf node3:

   `storage aggregate show -node node3 -state online -root false`

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

```
cluster::> storage aggregate show -node node3 state online -root false

Aggregate      Size         Available   Used%   State   #Vols  Nodes
RAID     Status
----------     ---------    ---------   ------  -----   -----  ------
-------  ------
aggr_1         744.9GB      744.8GB      0%     online  5      node2
raid_dp  normal
aggr_2         825.0GB      825.0GB      0%     online  1      node2
raid_dp  normal
2 entries were displayed.
```

Wenn die Aggregate offline sind oder in node3 offline sind, bringen Sie sie mit dem folgenden Befehl auf node3 online, einmal für jedes Aggregat:

`storage aggregate online -aggregate` *`aggr_name`*

2. Überprüfen Sie, ob alle Volumes auf node3 online sind, indem Sie den folgenden Befehl auf node3 verwenden und die Ausgabe überprüfen:

   `volume show -node` *`node3`* `-state offline`

   Wenn ein Volume auf node3 offline ist, schalten Sie sie online. Verwenden Sie dazu den folgenden Befehl auf node3, einmal für jedes Volume:

   `volume online -vserver` *`vserver_name`* `-volume` *`volume_name`*

   Der *`vserver_name`* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

3. Überprüfen Sie, ob die LIFs zu den richtigen Ports verschoben wurden und über den Status von verfügen `up`. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node_name`* `-status-admin up`

4. Wenn die Ports, die derzeit Daten-LIFs hosten, nicht auf der neuen Hardware vorhanden sind, entfernen Sie diese aus der Broadcast-Domäne:

   `network port broadcast-domain remove-ports`

5. Überprüfen Sie, ob auf node2 keine Daten-LIFs bleiben, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

   `network interface show -curr-node` *`node2`* `-role data`

Node2 ausmustern

Um node2 außer Betrieb zu nehmen, schalten Sie node2 zunächst ordnungsgemäß aus und entfernen Sie es aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

   Der Knoten wird automatisch angehalten.

Nachdem Sie fertig sind

Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5: installieren und booten sie node4

Phase-5-Übersicht

In Phase 5 installieren und booten Sie node4, überprüfen, ob die Cluster- und Node-Management-Ports von node2 auf node4 online geschaltet sind, und überprüfen Sie die Installation von node4. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind.

Schritte

1. "installieren und booten sie node4"
2. "Überprüfen Sie die installation von node4"
3. "Wiederherstellen der Key-Manager-Konfiguration auf node4"
4. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4"

installieren und booten sie node4

Sie installieren node4 im Rack, übertragen die Verbindungen von Node2 zu node4, starten node4 und installieren ONTAP. Sie weisen dann jede der Spare-Festplatten von Node2, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate neu zu, die zuvor nicht zu Node3 verschoben wurden, wie in diesem Abschnitt beschrieben.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Vorgang wird größtenteils automatisch durchgeführt. Der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen.

Sie müssen node4 als Netzboot ausführen, wenn es nicht die gleiche Version von ONTAP 9 hat, die auf node2 installiert ist. Nachdem sie node4 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem

Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Schritte

1. stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt.

   Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

2. installieren sie node4 im Rack gemäß den Anweisungen in der Anleitung *Installation and Setup Instructions* für das Node-Modell.
3. Kabel node4, ziehen Sie die Verbindungen von node2 nach node4.

   Verkabeln Sie die folgenden Verbindungen mithilfe der Anleitung im *Installation and Setup Instructions* oder beim *FlexArray Installation Requirements and Reference* für die node4-Plattform, dem entsprechenden Platten-Shelf-Dokument und *High Availability Management*.

   Siehe "Quellen" Link zu den Installationsanforderungen für die FlexArray-Virtualisierung und „ Reference_“ und „ High Availability Management_“.

   - Konsole (Remote-Management-Port)
   - Cluster- und HA-Ports
   - Datenports
   - Cluster- und Node-Management-Ports
   - Serial-Attached SCSI (SAS)- und Ethernet-Storage-Ports
   - SAN-Konfigurationen: ISCSI-Ethernet-, FC- und NVMe/FC-Switch-Ports

   Möglicherweise müssen Sie die Verbindungskabel zwischen den alten und den neuen Controllern ändern, um die Interoperabilität zwischen den verschiedenen Controller- und Kartenmodellen zu ermöglichen. Eine Verkabelungskarte der Ethernet-Storage-Shelfs für Ihre Systeme finden Sie im "Verfahren zur Systeminstallation" .

   Für ab ONTAP 9.15.1 eingeführte Controller verwenden Cluster und HA Interconnects die gleichen Ports. Bei Switch-verbundenen Konfigurationen müssen ähnliche Ports mit denselben Cluster-Switches verbunden werden. Wenn Sie beispielsweise von einem vorhandenen Controller auf einen AFF A1K aktualisieren, sollten Sie die e1a-Ports beider Nodes mit einem Switch und die e7a-Ports beider Nodes mit dem zweiten Switch verbinden.

4. Schalten Sie node4 ein, und unterbrechen Sie den Bootvorgang, indem Sie auf drücken `Ctrl-C` An der Konsole, um auf die Eingabeaufforderung für die Boot-Umgebung zuzugreifen.

   Wenn Sie node4 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
         because the battery is discharged but could be due to other
temporary
         conditions.
         When the battery is ready, the boot process will complete
         and services will be engaged. To override this delay, press 'c'
followed
         by 'Enter'
```

5. Wenn die Warnmeldung in Schritt 4 angezeigt wird, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

   Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.

   Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der DNS-Domain-Name (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Ausführen eines Netzboots auf node4:

   ```
   netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
   ```

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 1 im Abschnitt "Vorbereitungen für den Netzboot".

   Unterbrechen Sie den Startvorgang nicht.

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.

   Ignorieren Sie die folgende Meldung:

   ```
   This procedure is not supported for Non-Disruptive Upgrade on an HA pair
   ```

   Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

   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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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

```
http://<web_server_ip/path_to_web-
accessible_directory>/<ontap_version>_image.tgz
```

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12. Vergewissern Sie sich, dass Controller und Chassis als HA konfiguriert sind:

    ```
    ha-config show
    ```

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    ⓘ Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn der Controller und das Chassis nicht als HA konfiguriert wurden, verwenden Sie zum Korrigieren der Konfiguration die folgenden Befehle:

    ```
    ha-config modify controller ha

    ha-config modify chassis ha
    ```

14. Vergewissern Sie sich, dass alle Ethernet-Ports, die zur Verbindung mit den Ethernet-Shelfs verwendet werden, als Speicher konfiguriert sind:

    ```
    storage port show
    ```

    Die angezeigte Ausgabe hängt von der Systemkonfiguration ab. Das folgende Ausgabebeispiel gilt für einen Knoten mit einer einzelnen Speicherkarte in Steckplatz 11. Die Ausgabe für Ihr System kann unterschiedlich sein:

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Ändern Sie die Ports, die nicht auf Speicher festgelegt sind:

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

    Alle mit Storage Shelfs verbundenen Ethernet-Ports müssen als Storage konfiguriert werden, um den Zugriff auf Festplatten und Shelfs zu ermöglichen.

16. Beenden des Wartungsmodus:

    `halt`

    Unterbrechen Sie die Autoboot-Ausführung, indem Sie an der Eingabeaufforderung der Boot-Umgebung Strg-C drücken.

17. auf node3 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

    `date`

18. Überprüfen Sie am node4 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    `show date`

19. Legen Sie bei Bedarf das Datum auf node4 fest:

    `set date <mm/dd/yyyy>`

20. Überprüfen Sie auf node4 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    `show time`

21. Stellen Sie bei Bedarf die Uhrzeit auf node4 ein:

    `set time <hh:mm:ss>`

22. Legen Sie im Boot-Loader die Partner-System-ID auf node4 fest:

    `setenv partner-sysid <node3_sysid>`

    Für node4, `partner-sysid` Muss das der Node3 sein.

    Einstellungen speichern:

    `saveenv`

23. [[Auto_install4_step21] Verify the `partner-sysid` für node4:

    `printenv partner-sysid`

24. Wenn Sie NSE-Laufwerke (NetApp Storage Encryption) installiert haben, führen Sie die folgenden Schritte aus.

    Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

    a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`.

Wenn die folgenden Laufwerke verwendet werden…	**Dann…**
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

    b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

    Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

25. Boot-Node im Startmenü:

    `boot_ontap menu`.

26. auf node4, gehen Sie zum Boot-Menü und mit 22/7, wählen Sie die versteckte Option `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node2 ein, um die Festplatten von node2 node4 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7
(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
```

```
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to
restore the system configuration, or option (4) to initialize all
disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure
you want to continue?: yes
.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:
<nodename of the node being replaced>
Changing sysid of node node2 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
```

```
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote
    key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

Im obigen Beispiel der Konsolenausgabe werden Sie von ONTAP aufgefordert, den Namen des Partner-Node anzugeben, wenn das System ADP-Festplatten (Advanced Disk Partitioning) verwendet.

27. Starten Sie an der LOADER-Eingabeaufforderung:

```
boot_ontap menu
```

Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her:

Wenn das Root-Volume verschlüsselt ist, stellen Sie die Onboard-Schlüssel-Management-Geheimnisse wieder her, damit das System das Root-Volume finden kann.

a. Zurück zum speziellen Startmenü:
`LOADER> boot_ontap menu`

```
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)? 10
```

b. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

c. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

e. Geben Sie bei Aufforderung die Backup-Daten ein.

> Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

f. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

> In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 27 , bis das System ordnungsgemäß gebootet wird.

Überprüfen Sie die installation von node4

Sie müssen überprüfen, ob die physischen Ports von node2 den physischen Ports auf node4 korrekt zugeordnet sind. Dadurch kann node4 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Abhängig vom Modell der Nodes kann das physische Port-Layout variieren. Wenn der neue Node gestartet wird, versucht ONTAP, zu ermitteln, welche Ports die Cluster LIFs hosten sollten, damit es automatisch zu Quorum kommt.

Wenn die physischen Ports auf node2 nicht direkt den physischen Ports auf node4 zugeordnet werden, wird der folgende Abschnitt angezeigt Stellen Sie die Netzwerkkonfiguration auf node4 wieder her Muss zur Reparatur der Netzwerkverbindung verwendet werden.

Nachdem sie node4 installiert und gestartet haben, müssen Sie überprüfen, ob es ordnungsgemäß installiert wurde. sie müssen warten, bis node4 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen kann.

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node4 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node4 dem Quorum beigetreten ist:

   ```
   cluster show -node node4 -fields health
   ```

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node4 Teil desselben Clusters wie node3 ist und dass es sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Wechseln in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

4. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand befindet, bevor node2 angehalten wurde, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

   ```
   system controller replace show
   ```

   ```
   system controller replace show-details
   ```

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Austausch des Controllers wird anhand der folgenden Meldung unterbrochen:

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
-----------------------------------
Node2(now node4) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be
manually adjusted to match the new physical network configuration of the
hardware.
This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed
commands and instructions, refer to the "Re-creating VLANs, ifgrps, and
broadcast
domains" section of the upgrade controller hardware guide for the ONTAP
version
running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show"
to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement
network displaced-vlans restore" to restore the VLAN on the desired
port.
2 entries were displayed.
```

In diesem Verfahren wurde Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node4_ umbenannt.

7. Wenn der Controller-Austausch im Status „Pause“ steht, fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, um die Netzwerkkonfiguration auf dem Node wiederherzustellen.

Stellen Sie die Netzwerkkonfiguration auf node4 wieder her

Nachdem Sie bestätigt haben, dass node4 sich im Quorum befindet und mit node3 kommunizieren kann, überprüfen Sie, ob node2 VLANs, Interface Groups und Broadcast-Domains auf node4 zu sehen sind. Überprüfen Sie außerdem, ob alle node4-Netzwerkports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Verknüpfen mit *Network Management*.

Schritte

1. Listen Sie alle physischen Ports auf Upgrade-Knoten 2 (node4 genannt) auf:

   ```
   network port show -node node4
   ```

   Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. Von dieser Ausgabe aus sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um die Entscheidung zu erleichtern, welche Ports als Ports für Schnittstellengruppen, als VLAN-Basis-Ports oder als eigenständige physische Ports zum Hosten von LIFs verwendet werden sollten.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node4 auflisten:

   ```
   network port reachability show
   ```

   Die Ausgabe des Befehls sieht wie im folgenden Beispiel aus:

```
ClusterA::*> network port reachability show
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ----------------------------------
--------------------
node1_node3
          e0M      Default:Mgmt                        ok
          e10a     Default:Default                     ok
          e10b     -                                   no-reachability
          e10c     Default:Default                     ok
          e10d     -                                   no-reachability
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
node2_node4
          e0M      Default:Mgmt                        ok
          e10a     Default:Default                     ok
          e10b     -                                   no-reachability
          e10c     Default:Default                     ok
          e10d     -                                   no-reachability
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
18 entries were displayed.
```

Im obigen Beispiel wird node2_node4 erst nach dem Austausch des Controllers gestartet. Es verfügt über mehrere Ports, die keine Erreichbarkeit haben und eine Überprüfung der Erreichbarkeit ausstehen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node4 mit einem anderen Status als der Erreichbarkeit `ok`. Führen Sie den folgenden Befehl aus, zuerst auf beliebigen physischen Ports, dann auf beliebigen VLAN-Ports, nacheinander:

   `network port reachability repair -node <node_name> -port <port_name>`

   Die Ausgabe sieht wie das folgende Beispiel aus:

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Wie oben dargestellt, wird eine Warnmeldung für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Wiederachbarkeit der Broadcast-Domain unterscheiden können, wo sie sich derzeit befindet.

Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

```
network port reachability show
```

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Wenn die Konfiguration der Schnittstellengruppe nicht mit dem physischen Portlayout des neuen Controllers übereinstimmt, ändern Sie diese mit den folgenden Schritten.

   a. Sie müssen zunächst physische Ports entfernen, die als Ports für Schnittstellengruppen von ihrer Broadcast-Domain-Mitgliedschaft verwendet werden sollen. Dazu verwenden Sie den folgenden Befehl:

      ```
      network port broadcast-domain remove-ports -broadcast-domain
      <broadcast_domain_name> -ports <node_name:port_name>
      ```

   b. Hinzufügen eines Mitgliedports zu einer Schnittstellengruppe:

      ```
      network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port
      <port_name>
      ```

   c. Die Schnittstellengruppe wird der Broadcast-Domäne automatisch ca. eine Minute nach dem Hinzufügen des ersten Mitgliedports hinzugefügt.

   d. Vergewissern Sie sich, dass die Schnittstellengruppe der entsprechenden Broadcast-Domäne hinzugefügt wurde:

      ```
      network port reachability show -node <node_name> -port <ifgrp>
      ```

      Wenn der Status der Erreichbarkeit der Schnittstellengruppe nicht lautet `ok`, Weisen Sie es der entsprechenden Broadcast-Domain zu:

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. Weisen Sie dem die entsprechenden physischen Ports zu `Cluster` Broadcast-Domäne:

   a. Ermitteln Sie, welche Ports eine Reachability zum haben `Cluster` Broadcast-Domäne:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Reparieren Sie jeden Port mit Erreichbarkeit zum `Cluster` Broadcast-Domäne, wenn ihr Status der Erreichbarkeit nicht lautet `ok`:

      ```
      network port reachability repair -node <node_name> -port <port_name>
      ```

7. Verschieben Sie die verbleibenden physischen Ports in ihre richtigen Broadcast-Domänen mithilfe eines der folgenden Befehle:

   `network port reachability repair -node <node_name> -port <port_name>`

   `network port broadcast-domain remove-port`

   `network port broadcast-domain add-port`

   Vergewissern Sie sich, dass keine unerreichbaren oder unerwarteten Ports vorhanden sind. Überprüfen Sie den Status der Erreichbarkeit aller physischen Ports mithilfe des folgenden Befehls und überprüfen Sie die Ausgabe, um sicherzustellen, dass der Status lautet `ok`:

   `network port reachability show -detail`

8. Stellen Sie alle VLANs wieder her, die möglicherweise verschoben wurden, indem Sie die folgenden Schritte ausführen:

   a. Versetzte VLANs auflisten:

      `cluster controller-replacement network displaced-vlans show`

      Die Ausgabe sollte wie folgt angezeigt werden:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                  Original
      Node        Base Port     VLANs
      ---------   ---------     --------------
      Node1       a0a           822, 823
                  e10a          822, 823
      ```

   b. Stellen Sie VLANs wieder her, die von ihren früheren Basis-Ports verdrängt wurden:

      `cluster controller-replacement network displaced-vlans restore`

      Das folgende Beispiel zeigt die Wiederherstellung von VLANs, die aus der Schnittstellengruppe a0a wieder in dieselbe Schnittstellengruppe verschoben wurden:

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
      -destination-port a0a
      ```

      Das folgende Beispiel zeigt die Wiederherstellung von verlagerten VLANs am Port „e10a“ auf „e10b“:

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
      -destination-port e10b
      ```

Wenn eine VLAN-Wiederherstellung erfolgreich ist, werden die verschobenen VLANs auf dem angegebenen Zielport erstellt. Die VLAN-Wiederherstellung schlägt fehl, wenn der Zielport Mitglied einer Schnittstellengruppe ist oder der Zielport nicht verfügbar ist.

Warten Sie etwa eine Minute, bis neu wiederhergestellte VLANs in ihren entsprechenden Broadcast-Domänen platziert werden.

a. Erstellen Sie bei Bedarf neue VLAN-Ports für VLAN-Ports, die nicht im enthalten sind `cluster controller-replacement network displaced-vlans show` Ausgabe sollte aber auf anderen physischen Ports konfiguriert werden.

9. Löschen Sie alle leeren Broadcast-Domänen, nachdem alle Port-Reparaturen abgeschlossen wurden:

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

10. Überprüfen der Port-Erreichbarkeit:

```
network port reachability show
```

Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn Ports einen anderen Status als diese beiden melden, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

11. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

```
network port show
```

12. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

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

13. Stellen Sie die LIF-Start-Ports wieder her und geben Sie ggf. den Vserver(s) und die Home Ports der logischen Schnittstelle an, die wiederhergestellt werden müssen:

a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

b. LIF-Startports wiederherstellen:

```
displaced-interface restore-home-node -node <node_name> -vserver
<vserver_name> -lif-name <LIF_name>
```

14. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

```
network interface show -fields home-port, status-admin
```

Wiederherstellen der Key-Manager-Konfiguration auf node4

Wenn Sie mithilfe von NetApp Volume Encryption (NVE) und NetApp Aggregate

Encryption (NAE) Volumes auf dem System verschlüsseln, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht synchronisieren, können beim Verschieben der Node2-Aggregate mit ARL Fehler auftreten, da node4 nicht über die erforderlichen Schlüssel verfügt, um verschlüsselte Volumes und Aggregate online zu bringen.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie folgenden Befehl aus node4 aus:

   ```
   security key-manager onboard sync
   ```

2. Vergewissern Sie sich, dass der SVM-KEK-Schlüssel auf node4 als „true“ wiederhergestellt wurde, bevor Sie die Datenaggregate verschieben:

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK
   ```

   Beispiel

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node4    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4

Nachdem Sie die Netzwerkkonfiguration auf node4 überprüft und bevor Sie Aggregate von node3 auf node4 verschieben, müssen Sie überprüfen, ob die NAS-Daten-LIFs, die zu node2 gehören und sich derzeit auf node3 befinden, von node3 nach node4 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node4 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die

LIFs ordnungsgemäß sind und sich in den entsprechenden Ports befinden, nachdem Sie node4 in den Online-Modus versetzt haben.

Schritte

1. Die iSCSI LIFs finden automatisch die richtigen Home Ports mithilfe der Erreichbarkeit. Die FC- und NVMe/FC-SAN-LIFs werden nicht automatisch verschoben. Sie zeigen weiterhin den Home-Port an, an dem sie vor dem Upgrade waren.

   Prüfen Sie die SAN-LIFs auf node4:

   a. Ändern Sie alle iSCSI SAN LIFs, die über einen „down“-Status für die neuen Daten-Ports verfügen:

      ```
      network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down

      network interface modify -vserver <vserver> -lif <iscsi_san_lif> port
      <new_port> node <node>

      network interface modify -vserver <vserver> -lif <iscsi_san_lif>
      ```

   b. Ändern Sie alle FC- und NVMe/FC-SAN-LIFs, die den neuen Controller Zuhause haben, und melden Sie den Betriebsstatus der FCP-Ports am neuen Controller an:

      ```
      network interface modify -vserver <vserver> -lif <fc_san_lif> admin down

      network interface modify -vserver <vserver> -lif <fc_san_lif> port
      <new_port> node <node>
      ```

   ```
   network interface modify -vserver <vserver> -lif <fc_san_lif>
   ```

2. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

3. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen werden die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im

Besitz von node2 befinden, an den neuen Controller node4 verschoben. Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

4. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

   Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

5. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

   `cluster controller-replacement network displaced-interface show`

   Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in node4 wieder her:

   `cluster controller-replacement network displaced-interface restore-home-node`

6. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

   `system controller replace resume`

   Das System führt die folgenden Nachprüfungen durch:

   - Cluster-Quorum-Prüfung
   - Cluster-Zustandsprüfung
   - Aggregatrekonstruktion
   - Aggregatstatus-Prüfung
   - Überprüfung des Festplattenstatus
   - LIF-Statusüberprüfung für Cluster
   - Lautstärkerprüfung

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"

6. "Setzen Sie den SnapMirror Betrieb fort"

Authentifizierungsmanagement mit KMIP-Servern

Sie können KMIP-Server (Key Management Interoperability Protocol) für das Management von Authentifizierungsschlüssel verwenden.

Schritte

1. Hinzufügen eines neuen Controllers:

   ```
   security key-manager external enable
   ```

2. Fügen Sie den Schlüsselmanager hinzu:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um das korrekte Setup zu bestätigen, müssen Sie das HA-Paar aktivieren. Sie müssen außerdem überprüfen, dass Node3 und node4 auf den Storage der jeweils anderen Person zugreifen können und dass keine der logischen Datenschnittstellen zu anderen Nodes im Cluster vorhanden sind. Darüber hinaus müssen Sie bestätigen, dass Node3 zu Aggregaten node1 gehört und dass node4 die Aggregate von node2 besitzt und dass die Volumes für beide Nodes online sind.

Schritte

1. Nach den Tests nach der Prüfung von „node2“ werden das Storage Failover und das Cluster HA-Paar für den node2 Cluster aktiviert. Nach Abschluss des Vorgangs werden beide Nodes als abgeschlossen angezeigt, und das System führt einige Bereinigungsvorgänge aus.
2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   ```
   storage failover show
   ```

   Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

```
cluster::> storage failover show
                  Takeover
Node     Partner  Possible   State Description
-------- -----    -------    ------------------
node3    node4    true       Connected to node4
node4    node3    true       Connected to node3
```

3. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

   ```
   cluster show
   ```

4. Stellen Sie sicher, dass node3 und node4 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

   ```
   storage failover show -fields local-missing-disks, partner-missing-disks
   ```

5. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn keine der Knoten „Node3“ oder „node4“ Daten-LIFs besitzt, die sich im Besitz anderer Nodes im Cluster befinden, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

   ```
   network interface revert
   ```

6. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

   ```
   storage aggregate show -owner-name <node3>
   ```

   ```
   storage aggregate show -owner-name <node4>
   ```

7. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node <node3> -state offline
   ```

   ```
   volume show -node <node4> -state offline
   ```

8. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie im Abschnitt erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor", Und Online-Laufwerk eines der Offline-Volumes, nach Bedarf, durch Verwendung des folgenden Befehls, einmal für jedes Volume:

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. Installieren Sie neue Lizenzen für die neuen Nodes mithilfe des folgenden Befehls für jeden Node:

   ```
   system license add -license-code <license_code,license_code,license_code…>
   ```

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für

Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

10. Entfernen Sie alle alten Lizenzen mithilfe eines der folgenden Befehle von den ursprünglichen Nodes:

    ```
    system license clean-up -unused -expired

    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Alle abgelaufenen Lizenzen löschen:

      ```
      system license clean-up -expired
      ```

    - Alle nicht verwendeten Lizenzen löschen:

      ```
      system license clean-up -unused
      ```

    - Löschen Sie eine bestimmte Lizenz von einem Cluster mit den folgenden Befehlen auf den Nodes:

      ```
      system license delete -serial-number <node1_serial_number> -package *

      system license delete -serial-number <node2_serial_number> -package *
      ```

    Die folgende Ausgabe wird angezeigt:

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    Eingabe `y` Um alle Pakete zu entfernen.

11. Überprüfen Sie, ob die Lizenzen korrekt installiert sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

    ```
    system license show
    ```

    Sie können die Ausgabe mit der im Abschnitt erfassten Ausgabe vergleichen "Bereiten Sie die Knoten für ein Upgrade vor".

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie die Variable auf gesetzt haben `kmip.init.maxwait off` (z.B. in "installieren und booten sie node4, Schritt 24"), müssen Sie die Einstellung der Variable aufheben:

    ```
    set diag; systemshell -node <node_name> -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. Konfigurieren Sie die SPs mit dem folgenden Befehl auf beiden Knoten:

    ```
    system service-processor network modify -node <node_name>
    ```

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen

ONTAP 9.8: Manual Page Reference für detaillierte Informationen zum System `service-processor network modify` Befehl.

14. Informationen zum Einrichten eines Clusters ohne Switches auf den neuen Nodes finden Sie unter "Quellen" Um eine Verbindung zur NetApp Support Site_ zu erhalten, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node3 und node4 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

```
security key-manager external enable
```

b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

```
security key-manager external restore -node new_controller_name
```

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Onboard Key Manager

Konfigurieren Sie NVE oder NAE mit dem Onboard Key Manager.

Schritte

1. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager onboard sync
   ```

Externes Verschlüsselungsmanagement

Konfigurieren Sie NVE oder NAE mit externem Verschlüsselungsmanagement.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore
   ```

   Für diesen Befehl ist die OKM-Passphrase erforderlich

Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder EKM-Server nicht erreicht werden konnten. Stellen Sie diese Volumes mithilfe der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "Überblick über das ARL Upgrade". Informationen über mögliche Ausfälle werden in der Phase des Verfahrens aufgelistet.

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   ```
   storage aggregate relocation show
   ```

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9.8: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 waren, gehören node4 nach Abschluss des Upgrades

Beim Abschluss des Upgrade-Verfahrens sollte die Knoten3 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node die Knoten1 hatten. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Unter den folgenden Umständen kann es nicht gelingen, Aggregate ordnungsgemäß zu verschieben und Node 1 als Home Node anstelle von Knoten3 zu verwenden:

- In Phase 3, wenn Aggregate von node2 auf node3 verschoben werden. Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann wird das Aggregat auf node2 zurückgelassen.
- Nach Stufe 4, wenn node2 durch node4 ersetzt wird. Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node4 als Home-Node statt node3 online.

Sie können das falsche Eigentümerproblem nach Phase 6 beheben, wenn ein Storage-Failover aktiviert wurde, indem Sie die folgenden Schritte durchführen:

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Liste der Aggregate zu erhalten:

   `storage aggregate show -nodes node4 -is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 mit der Ausgabe, die Sie für Knoten 1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links auf node4:

   `storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3`

   Verwenden Sie das nicht `-ndo-controller-upgrade` Parameter während dieser Verschiebung.

4. Vergewissern Sie sich, dass node3 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht über Node3 als Hausbesitzer verfügen, können mit dem gleichen Relocation-Befehl in auf node3 verschoben werden Schritt 3.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, in Panik geraten oder aus- und wieder eingeschaltet werden.

Die Lösung dieser Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikzugänge oder Energiezyklen während der Vorprüfphase

Node1 oder node2 stürzt vor der Pre-Check-Phase ab, während das HA-Paar noch aktiviert ist

Wenn node1 oder node2 vor der Pre-Check-Phase abstürzt, wurden noch keine Aggregate verschoben und die HA-Paar-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzugänge oder Energiezyklen während der ersten Ressourcenfreigabephase

Node1 stürzt während der ersten Resource-Release-Phase ab, während das HA-Paar noch aktiviert ist

Einige oder alle Aggregate wurden von node1 in node2 verschoben und das HA-Paar ist noch aktiviert. Node2 übernimmt das Root-Volume von node1 und alle nicht-Root-Aggregate, die nicht verschoben wurden.

Über diese Aufgabe

Eigentum an Aggregaten, die verschoben wurden, sehen genauso aus wie das Eigentum von nicht-Root-Aggregaten, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat.

Wenn node1 in den eintritt `waiting for giveback` Status, node2 gibt alle node1 nicht-Root-Aggregate zurück.

Schritte

1. Nachdem node1 gestartet wurde, sind alle nicht-Root-Aggregate von node1 zurück in node1 verschoben. Sie müssen eine manuelle Aggregatverschiebung der Aggregate von node1 nach node2 durchführen: `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während der ersten Ressourcen-Release-Phase ab, während das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 schlägt während der ersten Phase der Ressourcenfreigabe fehl, während das HA-Paar noch aktiviert ist

Node1 hat einige oder alle seine Aggregate in node2 verschoben. Das HA-Paar ist aktiviert.

Über diese Aufgabe

Node1 übernimmt alle node2 Aggregate sowie jedes seiner eigenen Aggregate, die auf node2 verschoben wurden. Beim Booten von node2 wird die Aggregatverschiebung automatisch abgeschlossen.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während der ersten Resource-Release-Phase ab und nachdem HA-Paar deaktiviert ist

Node1 übernimmt nicht.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem verbleibenden Upgrade des Node-Paars fort.

Startet während der ersten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node2 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

Node3 übernimmt nach einem Absturz nach einem node2 nicht, da das HA-Paar bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt in der ersten Verifizierungsphase ab, wobei das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der ersten Ressourcen-Wiederholen-Phase

Knoten 2 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Node2 hat einige oder alle seine Aggregate von node1 in node3 verschoben. Node3 stellt Daten von Aggregaten bereit, die verlagert wurden. Das HA-Paar ist deaktiviert und somit gibt es keine Übernahme.

Über diese Aufgabe

Es gibt einen Client-Ausfall für Aggregate, die nicht verschoben wurden. Beim Booten von node2 werden die Aggregate von node1 auf node3 verschoben.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während der ersten Phase zur Ressourcenrückgewinnung während der Aggregatverschiebung ab

Falls node3 abstürzt, während node2 Aggregate zu node3 verschoben wird, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Knoten 3 verlagert wurden, begegnen ein Client-Ausfall, während node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Führen Sie das Controller-Upgrade fort.

Neustarts, Panikspiele oder Energiezyklen während der Nachprüfphase

Node2 oder node3 stürzt während der Post-Check-Phase ab

Das HA-Paar ist deaktiviert, damit dies keine Übernahme ist. Es gibt einen Client-Ausfall für Aggregate, die zum neu gebooteten Node gehören.

Schritte

1. Bringen Sie den Node hoch.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der zweiten Ressourcenfreigabephase

Node3 stürzt während der zweiten Resource-Release-Phase ab

Wenn node3 abstürzt, während node2 Aggregate verschoben, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Node3 verlagert wurden, und Node3 eigene Aggregate stoßen auf Client-Ausfälle, während Node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Node2 stürzt während der zweiten Resource-Release-Phase ab

Wenn node2 während der Aggregatverschiebung abstürzt, wird node2 nicht übernommen.

Über diese Aufgabe

Node3 dient weiterhin den Aggregaten, die verschoben wurden, doch die Aggregate von node2 stoßen auf Client-Ausfälle.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Startet während der zweiten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node3 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node3 abstürzt, wird die Übernahme nicht ausgeführt, da das HA-Paar bereits

deaktiviert ist.

Über diese Aufgabe

Es gibt einen Client-Ausfall für alle Aggregate, bis node3 neu startet.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node4 stürzt während der zweiten Verifikationsphase ab

Wenn node4 während dieser Phase abstürzt, wird die Übernahme nicht durchgeführt. Node3 stellt Daten aus den Aggregaten bereit.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis node4 neu startet.

Schritte

1. bringen sie node4 auf.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------   --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder

Panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
-------   --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports lautet `down`.

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.

Inhalt	Beschreibung
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.13.1 Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und Verwendung der unterstützten ONTAP 9.13.1-Befehle.
"ONTAP 9.14.1 Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und Verwendung der unterstützten ONTAP 9.14.1-Befehle.
"ONTAP 9.15.1 Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und Verwendung der unterstützten ONTAP 9.15.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.

Inhalt	Beschreibung
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe", Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.

Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“

Überblick

Sie können die Controller-Hardware auf einem HA-Paar unterbrechungsfrei aufrüsten, indem Sie die Aggregatverschiebung (Aggregate Relocation, ARL) verwenden und das vorhandene System in das Ersatzsystem konvertieren. Dadurch bleiben das System-Chassis und die Festplatten erhalten.

Dieses Verfahren gilt ausschließlich für die folgenden Upgrade-Konfigurationen: **Not** Verwenden Sie dieses Verfahren, um ein Upgrade zwischen anderen Systemkombinationen durchzuführen.

Vorhandenes System	Austauschsystem	Unterstützte ONTAP-Versionen
AFF A800 [1]	AFF A90 oder AFF A70	9.15.1
AFF A220 als All-SAN-Array (ASA) konfiguriert	ASA A150	9.13.1P1 und höher
AFF A220	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 und höher
AFF A200	AFF A150	9.10.1P15, 9.11.1P11 und höher [2]
AFF C 190	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 und höher

Vorhandenes System	Austauschsystem	Unterstützte ONTAP-Versionen
FAS2620	FAS2820	9.11,1 P7 (FAS2620) [2] 9.13.1 und höher (FAS2820)
FAS2720	FAS2820	9.13.1 und höher
AFF A700 – als ASA konfiguriert	ASA A900	9.13.1P1 und höher
AFF A700	AFF A900	9.10.1P10, 9.11.1P6 und höher
FAS9000	FAS9500	9.10.1P10, 9.11.1P6 und höher

[1] Wenn Sie ein Upgrade auf ein mit ONTAP 9.15.1 eingeführtes System durchführen, konvertiert ONTAP die Storage-Effizienz aller vorhandenen Thin Provisioning Volumes, einschließlich solcher, die die Storage-Effizienz nicht nutzen, und wendet die neuen Storage-Effizienzfunktionen an, die die Hardware-Offload-Funktion nutzen. Dies ist ein automatischer Hintergrundprozess, ohne sichtbare Auswirkungen auf die Leistung des Systems. "Weitere Informationen ."

[2] die Systeme AFF A200 und FAS2620 unterstützen ONTAP Versionen nach 9.11.1 nicht.

NetApp empfiehlt, wenn möglich, auf dem alten und dem Ersatzsystem dieselbe ONTAP-Version zu verwenden.

Die ONTAP-Mindestversionen in der vorstehenden Tabelle sind obligatorisch. Diese ONTAP-Versionen verfügen über die Firmware-Version des Service-Prozessors oder des Baseboard Management Controller (BMC), die erforderlich ist, um während eines Upgrades gemischte Controller-Typen innerhalb eines Chassis zu unterstützen.

Während des Verfahrens migrieren Sie die nicht-Root-Aggregate zwischen den alten Controller-Nodes. Nach der Installation migrieren Sie die nicht-Root-Aggregate von den alten Controller-Nodes zu den Ersatz-Controller-Nodes. Auf die Daten, die auf den Nodes gehostet werden, die Sie aktualisieren, kann während des Upgrades zugegriffen werden.

Über diese Aufgabe

Während dieses Controller-Upgrades führen Sie eines der folgenden Upgrades durch:

Auf dem bestehenden…	Führen Sie folgende Schritte durch…
AFF A800	Tauschen Sie die beiden AFF A800 Controller, NVRAM und alle I/O-Module durch die neuen Controller und I/O-Module aus.
AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720	Tauschen Sie das Controller-Modul an jedem Knoten des alten Controllers gegen das neue Modul aus. [1]
AFF A700 ODER FAS9000	Tauschen Sie den Controller und die NVRAM-Module auf jedem Node des alten Controllers gegen die neuen Module aus. [1]

[1] Sie müssen die I/O-Karten, Datenkabel, Festplatten-Shelfs und Festplatten nicht verschieben, trennen oder neu anschließen.

Dieses Verfahren verwendet eine Methode namens Aggregate Relocation (ARL). ARL profitiert von der HA-Konfiguration und der Cluster Interconnect-Kommunikation, sodass Sie Eigentümerschaft von Aggregaten, die nicht-Root-Aggregate sind, von einem Node zu einem anderen verschieben können, wenn sie Storage

innerhalb desselben Clusters gemeinsam nutzen.

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Sie migrieren beim Fortfahren Daten-LIFs zwischen Nodes im Cluster.

> Die Begriffe **node1** und **node2** werden nur als Hinweis auf Knotennamen in diesem Dokument verwendet. Wenn Sie das Verfahren befolgen, müssen Sie die tatsächlichen Namen Ihrer Knoten ersetzen.

Wichtige Informationen

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie sollten auch lesen und verstehen, die "Richtlinien für Controller Upgrades" Und das "Überblick über das ARL Upgrade" Abschnitte vor Beginn der Aktualisierung.
- Bei diesem Verfahren wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht in einem anderen System verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Sie müssen sich an den technischen Support wenden, wenn die Ersatz-Controller-Hardware zuvor als Teil eines anderen ONTAP Clusters oder als Standalone-System mit einem einzelnen Node verwendet wurde.
- Sie können dieses Verfahren zum Upgrade der Controller Hardware in Clustern mit mehr als zwei Nodes verwenden. Sie müssen jedoch die Verfahren für jedes HA-Paar im Cluster separat durchführen.
- Wenn Sie über einen Switch verfügen, der von der ONTAP-Version und dem Ersatzsystem, auf das Sie aktualisieren, nicht unterstützt wird, finden Sie weitere Informationen unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.
- Dieses Verfahren gilt nur für AFF A800, AFF A200, AFF A220, AFF C190, FAS2620, FAS2720, AFF A700 und FAS9000 Systeme. Für alle anderen Controller-Modelle, die ein Upgrade auf eine AFF A90, AFF A70, AFF A150, FAS2720, AFF A900 erfordern, oder FAS9500-System, siehe "Quellen" einen Link zu den Befehlen „ System Controller Replace“ verwenden, um Controller-Hardware mit ONTAP 9.8 oder höher zu aktualisieren_ und den Befehl „ Aggregate Relocation to manually Upgrade Controller Hardware mit ONTAP 9.8 oder höher “ Inhalt.
- Die ASA Systeme A900, AFF A900 und FAS9500 unterstützen nur eine hohe Netzspannung (200 V bis 240 V). Wenn Ihr AFF A700 oder FAS9000 System mit niedriger Netzspannung (100 V bis 120 V) ausgeführt wird, müssen Sie vor diesem Verfahren die Eingangsspannung der AFF A700 oder FAS9000 konvertieren.
- Wenn Sie ein Upgrade von einer AFF A800, AFF A200, AFF A220, AFF C190, FAS2620, FAS2720, AFF A700 oder FAS9000 System mit Ausfallzeiten können Sie die Controller-Hardware durch Verschieben von Storage aktualisieren oder sich an den technischen Support wenden. Siehe "Quellen" Link zu *Upgrade by moving Volumes or Storage*.

Automatisierung des Controller-Upgrades

Dieses Verfahren enthält die Schritte für das automatisierte Verfahren. Hierbei werden die automatische Festplattenzuordnung und die Überprüfung der Erreichbarkeit von Netzwerk-Ports verwendet, um das Upgrade des Controllers zu vereinfachen.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

Dieser Inhalt beschreibt, wie Sie ein Upgrade von Storage Controllern in einem HA-Paar

durchführen, ohne dabei alle vorhandenen Daten und Festplatten zu beeinträchtigen. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Sie können dieses Verfahren unter folgenden Umständen verwenden:

- Sie führen eines der folgenden Controller-Upgrades aus:

Alter Controller	Ersatz-Controller
AFF A800	AFF A70 und AFF A90
AFF A220 als ASA konfiguriert	ASA A150
AFF A220, AFF A200 oder AFF C190	AFF A150
FAS2720 oder FAS2720	FAS2820
AFF A700 – als ASA konfiguriert	ASA A900
AFF A700	AFF A900
FAS9000	FAS9500

- Sie haben mit Ihrem NetApp Vertriebsmitarbeiter verifiziert, dass Sie die Hardware für das Controller-Upgrade erhalten haben:
  - Zwei AFF A90 oder zwei AFF A70-Controller und alle für das Upgrade erforderlichen I/O-Module. Die erforderliche Länge von 100-GbE-Kabeln.
  - ASA Controller A150, AFF A150 oder FAS2820
  - ASA Controller- und NVRAM-Module A900, AFF A900 oder FAS9500 sowie die für das Upgrade erforderlichen Teile
- Sie verwenden die minimale ONTAP-Version für Ihr Upgrade. Weitere Informationen finden Sie unter "Überblick".
- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind erfahren in der Verwaltung von ONTAP und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.

Sie können dieses Verfahren unter folgenden Umständen nicht verwenden:

- Sie verwenden die FlexArray Virtualisierungssoftware auf den Systemen AFF A800, AFF A700 oder FAS9000.
- Sie verwenden einen gemeinsamen Switch für Cluster-Interconnect und Ethernet Attached Storage.

Informationen zum Upgrade von MetroCluster IP-Konfigurationen auf AFF A800, AFF A700 oder FAS9000 Systemen finden Sie unter "Quellen" Link zum Inhalt *MetroCluster Upgrade and Expansion*.

Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu ONTAP 9 zugreifen können.

Die erforderlichen Tools und Dokumentationen

Sie müssen über ein Erdungsband verfügen, um das Upgrade durchführen zu können, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren.

Bei einem AFF A800 Upgrade auf eine AFF A90 oder AFF A70 stellen Sie sicher, dass die 100-GbE-Kabel eine Länge von mindestens einem Meter haben.

Siehe "Quellen" Um auf die Liste der Referenzdokumente und Referenzsites zuzugreifen, die für dieses Upgrade erforderlich sind.

Richtlinien für Controller Upgrades

Ob Sie die Aggregatverschiebung (ARL, Aggregate Relocation) und die alten System-Chassis- und -Festplatten beibehalten können, hängt von der System-Upgrade-Konfiguration und der ONTAP-Version ab.

Unterstützte Upgrades für ARL

Controller Upgrades werden für bestimmte Systemkonfigurationen unterstützt. Eine Liste der unterstützten Systeme und ONTAP-Mindestversionen finden Sie unter "Überblick".

Wenn Sie ein neues AFF A150, FAS2820, AFF A900 oder FAS9500 als vollständiges System einschließlich eines neuen Gehäuses erhalten haben, lesen Sie bitte "Quellen" Um eine Verbindung zu den Befehlen „System Controller Replace“ zu herstellen, um die Controller Hardware mit ONTAP 9.8 oder höher zu aktualisieren_.

Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise und SnapLock Compliance Volumes konfiguriert sind.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren.

Switch Attached-Cluster

Wenn Sie Nodes in einem Cluster aktualisieren, das mit einem Cluster-Switch verbunden ist, müssen Sie überprüfen, ob die auf dem Switch ausgeführte Version von Make, Model, Firmware, RCF und ONTAP mit denen identisch ist, die nach dem Upgrade auf dem Ersatz-Controller ausgeführt werden. Falls erforderlich, müssen Sie das Switch-Upgrade durchführen, bevor Sie die Controller mithilfe des in dieser Dokumentation beschriebenen ARL-Verfahrens aktualisieren.

Fehlerbehebung

Falls beim Upgrade der Controller Probleme auftreten, lesen Sie den "Fehlerbehebung" Abschnitt am Ende des Verfahrens für weitere Informationen und mögliche Lösungen.

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Überblick über das ARL Upgrade

Bevor Sie die Nodes mit ARL aktualisieren, sollten Sie unbedingt verstehen, wie das Verfahren funktioniert. In diesem Inhalt wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und dann für die ursprünglichen und die neuen Nodes eine Reihe von Schritten ausführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Schritte
"Phase 1: Upgrade vorbereiten"	In Phase 1 überprüfen Sie, ob Sie über die richtige Hardware für Ihr Upgrade verfügen, führen Vorabprüfungen durch und korrigieren bei Bedarf die Eigentümerschaft für Aggregate. Sie müssen bestimmte Informationen aufzeichnen, wenn Sie Storage Encryption mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate

Stufe	Schritte
"Phase 2: Ressourcen verlagern und Knoten in den Ruhestand zurücknehmen 1"	In Phase 2 verschieben Sie Node1-nicht-Root-Aggregate und NAS-Daten-LIFs von Node1 zu Node2. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie erfassen Node1-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node1. Sie können sich auch später beim Verfahren auf den Netzboot node1 vorbereiten. Gesamteigentum am Ende von Phase 2: • Node2 ist der aktuelle Besitzer von node1 Aggregaten • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten
"Stufe 3: Starten Sie Node1 mit den Ersatz-Systemmodulen"	In Phase 3 starten Sie node1 mit aktualisierten Systemmodulen und überprüfen die aktualisierte node1-Installation. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1 Aggregate und NAS-Daten-LIFs von node2 auf die aktualisierte Node1 verschoben und Sie überprüfen, ob die SAN-LIFs auf node1 vorhanden sind. Gesamteigentum am Ende von Stufe 3: • Aktualisierter node1 ist der Haupteigentümer und aktueller Besitzer von node1-Aggregaten • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten
"Phase 4: Ressourcen verlagern und Knoten zurücknehmen 2"	Während Phase 4 verschieben Sie Aggregate und NAS-Daten-LIFs von Knoten 2 auf die aktualisierte Knoten 1 und Mustern Knoten 2 aus. Gesamteigentum am Ende von Stufe 4: • Der aktualisierte Knoten 1 ist der Hausbesitzer und der aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehörten • Der aktualisierte Knoten 1 ist der aktuelle Besitzer von node2 Aggregaten
"Stufe 5: Installieren Sie die Ersatz-Systemmodule auf Knoten 2"	In Phase 5 installieren Sie die neuen Systemmodule, die Sie für den aktualisierten Knoten 2 erhalten haben, und dann Netboot Knoten 2. Gesamteigentum am Ende von Stufe 5: • Der aktualisierte Node1 ist der Hausbesitzer und der aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Upgrade node2 ist der Hausbesitzer und der aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.

Stufe	Schritte
"Stufe 6: Starten Sie Node2 mit den Ersatz-Systemmodulen"	In Phase 6 starten Sie Knoten 2 mit aktualisierten Systemmodulen und überprüfen die aktualisierte Installation von Knoten 2. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Außerdem werden node1-Aggregate und NAS-Daten-LIFs von node1 auf die aktualisierte Node2 verschoben und Sie überprüfen, ob die SAN-LIFs auf node2 vorhanden sind.
"Phase 7: Das Upgrade abschließen"	In Phase 7 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden. Und wenn die neuen Nodes verschlüsselt sind, konfigurieren und einrichten Sie Storage Encryption oder NVE. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 überprüfen Sie, ob Sie über die richtige Hardware für Ihr Upgrade verfügen, führen Vorabprüfungen durch und korrigieren bei Bedarf die Eigentümerschaft für Aggregate. Wenn Sie Storage Encryption mit dem Onboard Key Manager managen, erfassen Sie bestimmte Informationen auch und können die SnapMirror Beziehungen stilllegen.

Schritte

1. "Überprüfen Sie die Upgrade-Hardware"
2. "Bereiten Sie die Knoten für ein Upgrade vor"
3. "Managen Sie die Storage-Verschlüsselung mit dem Onboard Key Manager"

Überprüfen Sie die Upgrade-Hardware

Vergewissern Sie sich vor dem Upgrade, dass Sie die richtige Hardware für das Upgrade haben. Je nach Upgrade müssen Sie für jedes upgradeende HA-Paar zwei Controller-Module oder zwei Controller-Module und zwei NVRAM-Module für das Ersatzsystem besitzen. Sollten Teile fehlen, wenden Sie sich an den technischen Support oder an Ihren NetApp Ansprechpartner.

Wenn Sie ein Upgrade …	Ersatzsystem muss …
AFF A800	Zwei Controller-Module, zwei NVRAMs und neue I/O-Module
AFF A220 als ASA auf ASA A150 konfiguriert	Zwei Controller-Module
AFF A220, AFF A200 oder AFF C190 auf AFF A150	Zwei Controller-Module
FAS2720 oder FAS2720 zu FAS2720	Zwei Controller-Module
AFF A700 als ASA zu ASA A900 konfiguriert	Zwei Controller und zwei NVRAM-Module

Wenn Sie ein Upgrade …	Ersatzsystem muss …
AFF A700 AUF AFF A900	Zwei Controller und zwei NVRAM-Module
FAS9000 auf FAS9500 Systeme	Zwei Controller und zwei NVRAM-Module

Bereiten Sie die Knoten für ein Upgrade vor

Der Prozess des Controller-Austauschs beginnt mit einer Reihe von Vorabprüfungen. Sie sammeln auch Informationen über die ursprünglichen Nodes, die Sie später verwenden können. Falls erforderlich, ermitteln Sie den Typ der verwendeten Self-Encrypting Drives.

Schritte

1. Listen Sie die Firmware-Version des Service-Prozessors (SP) oder des Baseboard Management Controller (BMC) auf, die auf dem alten Controller ausgeführt wird:

   ```
   service-processor show
   ```

   Vergewissern Sie sich, dass Sie über eine unterstützte SP- oder BMC-Firmware-Version verfügen:

Alter Controller	SP oder BMC	Mindestversion der Firmware
AFF A800	BMC	10.9
AFF A220	BMC	11,9P1
AFF A200	SP	5.11P1
AFF C 190	BMC	11,9P1
FAS2620	SP	5.11P1
FAS2720	BMC	11,9P1

2. Starten Sie den Controller-Ersatzprozess, indem Sie den folgenden Befehl im erweiterten Berechtigungsmodus der ONTAP-Befehlszeile eingeben:

   ```
   set -privilege advanced
   ```

   ```
   system controller replace start -nodes node_names
   ```

   Es wird eine Ausgabe wie im folgenden Beispiel angezeigt. In der Ausgabe wird die auf dem Cluster ausgeführte ONTAP-Version angezeigt:

```
Warning:
1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller
replacement supports only ARL based procedures.

Do you want to continue? {y|n}: y
```

3. Wählen Sie `y`. Sie sehen die folgende Ausgabe:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

In der Vorabprüfungen-Phase führt das System die folgende Liste der Überprüfungen im Hintergrund aus.

Pre-Check	Beschreibung
Cluster-Integritätsprüfung	Überprüft alle Nodes im Cluster, um sicherzustellen, dass sie sich in einem ordnungsgemäßen Zustand befinden.
Statusprüfung Der Aggregatverschiebung	Überprüft, ob eine Aggregatverschiebung bereits erfolgt. Wenn eine weitere Aggregatverschiebung erfolgt, schlägt die Prüfung fehl.
Modellname Prüfen	Überprüft, ob die Controller-Modelle bei diesem Verfahren unterstützt werden. Wenn die Modelle nicht unterstützt werden, schlägt die Aufgabe fehl.
Cluster-Quorum-Prüfung	Überprüft, ob die zu ersetzenden Nodes sich in Quorum befinden. Wenn sich die Knoten nicht im Quorum befinden, schlägt die Aufgabe fehl.

Pre-Check	Beschreibung
Überprüfung Der Bildversion	Überprüft, ob die zu ersetzenden Nodes dieselbe Version von ONTAP ausführen. Wenn sich die ONTAP-Image-Versionen unterscheiden, schlägt die Aufgabe fehl. Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version von ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation als Netzboot einsetzen. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.
HA-Statusüberprüfung	Überprüft, ob beide Nodes, die ersetzt werden, in einer HA-Paar-Konfiguration mit Hochverfügbarkeit vorhanden sind. Wenn das Speicher-Failover für die Controller nicht aktiviert ist, schlägt die Aufgabe fehl.
Aggregatstatus-Prüfung	Wenn die Nodes ersetzt werden, eigene Aggregate, für die sie nicht der Home-Inhaber sind, schlägt die Aufgabe fehl. Die Nodes sollten nicht im Besitz von nicht lokalen Aggregaten sein.
Überprüfung Des Festplattenstatus	Wenn zu ersetzende Knoten keine oder fehlerhafte Festplatten haben, schlägt die Aufgabe fehl. Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.
LIF-Statusüberprüfung von Daten	Überprüft, ob für einen der zu ersetzenden Nodes keine lokalen Daten-LIFs vorhanden sind. Die Nodes sollten keine Daten-LIFs enthalten, für die sie nicht der Home-Inhaber sind. Wenn einer der Nodes nicht-lokale Daten-LIFs enthält, schlägt die Aufgabe fehl.
LIF-Status des Clusters	Überprüft, ob die Cluster-LIFs für beide Nodes aktiv sind. Wenn die Cluster-LIFs ausgefallen sind, schlägt die Aufgabe fehl.
ASUP-Statusprüfung	Wenn AutoSupport-Benachrichtigungen nicht konfiguriert sind, schlägt die Aufgabe fehl. Bevor Sie mit dem Austausch des Controllers beginnen, müssen Sie AutoSupport aktivieren.
CPU-Auslastungs-Prüfung	Überprüft, ob die CPU-Auslastung bei allen zu ersetzenden Nodes mehr als 50 % beträgt. Wenn die CPU-Nutzung über einen erheblichen Zeitraum mehr als 50 % beträgt, schlägt die Aufgabe fehl.
Aggregatrekonstruktion	Überprüft, ob bei beliebigen Datenaggregaten eine Rekonstruktion durchgeführt wird. Wenn die Aggregatrekonstruktion ausgeführt wird, schlägt die Aufgabe fehl.
Knoten Affinität Job Überprüfung	Überprüft, ob Jobs mit Knotenorientierung ausgeführt werden. Wenn Knotenaffinitätsjobs ausgeführt werden, schlägt die Prüfung fehl.

4. Wenn der Controller-Ersatzvorgang gestartet und die Vorabprüfungen abgeschlossen sind, wird der Vorgang angehalten. In diesem Fall können Sie die Ausgabedaten sammeln, die Sie zu einem späteren Zeitpunkt im Controller-Upgrade-Prozess benötigen könnten.
5. Führen Sie den folgenden Befehlssatz aus, wie durch das Verfahren zum Austausch des Controllers auf der Systemkonsole gesteuert.

   Führen Sie die Befehle an dem seriellen Port aus, der mit den einzelnen Nodes verbunden ist, und speichern Sie die Ausgabe der Befehle einzeln:

- `vserver services name-service dns show`
- `network interface show -curr-node local -role cluster,intercluster,node-mgmt,cluster-mgmt,data`
- `network port show -node local -type physical`
- `service-processor show -node local -instance`
- `network fcp adapter show -node local`
- `network port ifgrp show -node local`
- `system node show -instance -node local`
- `run -node local sysconfig`
- `run -node local sysconfig -ac`
- `run -node local aggr status -r`
- `vol show -fields type`
- `run local aggr options data_aggregate_name`
- `vol show -fields type , space-guarantee`
- `storage aggregate show -node local`
- `volume show -node local`
- `storage array config show -switch switch_name`
- `system license show -owner local`
- `storage encryption disk show`
- `security key-manager onboard show-backup`
- `security key-manager external show`
- `security key-manager external show-status`
- `network port reachability show -detail -node local`

Wenn NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) den Onboard Key Manager verwendet, halten Sie die Schlüsselmanager-Passphrase bereit, um später im Verfahren die Neusynchronisierung des Schlüsselmanagers abzuschließen.

6. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:
   - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
   - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

"Weitere Informationen zu unterstützten Self-Encrypting Drives".

Korrigieren Sie die Aggregateigentümer bei Ausfall einer ARL-Vorabprüfung

Wenn die aggregierte Statusprüfung fehlschlägt, müssen Sie Aggregate des Partner-Node an den Node „Home-Owner“ zurückgeben und den Vorabprüfvorgang erneut initiieren.

Schritte

1. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

   `storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *`

2. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Nachdem Sie fertig sind

Sie müssen den Controller-Ersatzprozess neu starten:

`system controller replace start -nodes node_names`

Lizenz

Jeder Knoten im Cluster muss über eine eigene NetApp-Lizenzdatei (NLF) verfügen.

Wenn Sie nicht über eine Lizenzdatei verfügen, stehen dem neuen Controller derzeit lizenzierte Funktionen im Cluster zur Verfügung. Wenn Sie jedoch nicht lizenzierte Funktionen auf dem Controller verwenden, unterläuft dies möglicherweise die Einhaltung Ihrer Lizenzvereinbarung. Daher sollten Sie nach Abschluss des Upgrades die Lizenzdatei für den neuen Controller installieren.

Siehe "Quellen" Um eine Verknüpfung zur *NetApp Support-Website* zu erstellen, auf der Sie Ihre Lizenzdatei erhalten können. Die NLFs sind im Abschnitt *My Support* unter *Softwarelizenzen* verfügbar. Wenn der Standort nicht über die benötigten NLFs verfügt, wenden Sie sich an Ihren NetApp Ansprechpartner.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Management der Storage-Verschlüsselung mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung der Schlüssel verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager onboard show-backup` Befehl.

Stilllegen der SnapMirror Beziehungen (optional)

Bevor Sie mit dem Verfahren fortfahren, müssen Sie bestätigen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   Wenn der Status „Übertragen“ lautet, müssen Sie diese Transfers abbrechen: `snapmirror abort -destination-vserver vserver_name`

   Der Abbruch schlägt fehl, wenn sich die SnapMirror-Beziehung nicht im Zustand „Übertragen“ befindet.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Phase 2. Verschieben von Ressourcen und Ausmustern von Knoten1

Phase-2-Übersicht

Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2

verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie zeichnen auch node1-Informationen für die spätere Verwendung im Verfahren auf und tauschen dann die entsprechenden node1-Systemmodule aus, entfernen node1 und starten den aktualisierten node1.

Schritte

1. "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2"
2. "Verschiebung ausgefallener oder Vetos von Aggregaten"
3. "Node1 ausmustern"
4. "Ersetzen Sie die node1-Systemmodule"
5. "Netzboot Nr. 1"

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2

Bevor Sie Node1 durch die Ersatzmodule für Ihr System-Upgrade ersetzen können, müssen Sie die nicht-Root-Aggregate und NAS-Daten-LIFs von Node1 zu Node2 verschieben, bevor Sie die node1-Ressourcen auf Node1, der auf dem Ersatzsystem ausgeführt wird, wieder wiederherstellen können. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können.

Bevor Sie beginnen

Der Vorgang sollte bereits angehalten werden, wenn Sie mit der Aufgabe beginnen. Sie müssen den Vorgang manuell fortsetzen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Sie müssen während des Upgrades keine SAN-LIFs für den Cluster- oder Systemzustand verschieben. Sie müssen überprüfen, ob die LIFs in gutem Zustand und an den entsprechenden Ports angeschlossen sind, nachdem Sie node1 als Ersatzsystem online geschaltet haben.

Der Home-Inhaber für die Aggregate und LIFs wird nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Wiederaufnahme der Vorgänge für die Aggregatverschiebung und die LIF-Verschiebung von NAS-Daten:

   ```
   system controller replace resume
   ```

   Alle Aggregate ohne Root-Root-Root-Root-Daten und LIFs werden von node1 auf node2 migriert.

   Der Vorgang angehalten, damit Sie überprüfen können, ob alle node1-Aggregate und LIFs für nicht-SAN-Daten in node2 migriert wurden.

2. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

```
system controller replace show-details
```

3. Wenn der Vorgang noch angehalten wird, vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind, damit ihr Status bei node2 lautet:

   ```
   storage aggregate show -node node2 -state online -root false
   ```

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

   ```
   cluster::> storage aggregate show -node node2 state online -root false

   Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
   ---------  -------  ---------  -----  ------ -----  ------
   --------------
   aggr_1     744.9GB  744.8GB    0%     online     5  node2
   raid_dp,normal
   aggr_2     825.0GB  825.0GB    0%     online     1  node2
   raid_dp,normal
   2 entries were displayed.
   ```

   Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

   ```
   storage aggregate online -aggregate aggr_name
   ```

4. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 verwenden und seine Ausgabe überprüfen:

   ```
   volume show -node node2 -state offline
   ```

   Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

   Der *vserver_name* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

5. Wenn irgendeine LIFs inaktiv sind, setzen Sie den Administratorstatus der LIFs auf `up` Mit dem folgenden Befehl, so wie es für jedes LIF ist:

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   nodename -status-admin up
   ```

Verschiebung ausgefallener oder Vetos von Aggregaten

Falls Aggregate nicht verschoben oder ein Vetos ausfällt, müssen sie die Aggregate manuell verschieben oder, falls erforderlich, die Vetos oder Zielprüfungen überschreiben.

Über diese Aufgabe

Der Umzugsvorgang wird aufgrund des Fehlers angehalten.

Schritte

1. Überprüfen Sie die EMS-Protokolle (Event Management System), um festzustellen, warum das Aggregat nicht verschoben oder gegen ein Vetos eingesetzt wurde.
2. Verschiebung ausgefallener oder Vetos von Aggregaten:

   ```
   storage aggregate relocation start -node node1 -destination node2 -aggregate
   -list aggr_name -ndo-controller-upgrade true
   ```

3. Geben Sie bei der entsprechenden Aufforderung ein `y`.
4. Sie können die Verschiebung mit einer der folgenden Methoden erzwingen:

Option	Beschreibung
Veto-Prüfungen werden überschrieben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true`
Zielprüfungen überschreiben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true`

Node1 ausmustern

Um node1 auszumustern, setzen Sie den automatisierten Vorgang fort, um das HA-Paar mit node2 zu deaktivieren und node1 ordnungsgemäß herunterzufahren.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

2. Vergewissern Sie sich, dass node1 angehalten wurde:

   ```
   system controller replace show-details
   ```

   Nachdem node1 vollständig angehalten wurde, sollte node1 an DER LOADER>-Eingabeaufforderung sein. Um die LOADER>-Eingabeaufforderung anzuzeigen, stellen Sie eine Verbindung mit der seriellen Konsole von node1 her.

Ersetzen Sie die node1-Systemmodule

Ersetzen Sie die AFF A800 Controller-Module

An dieser Stelle ist node1 ausgefallen und alle Daten werden von node2 bereitgestellt. Da sich Node1 und Node2 im gleichen Chassis befinden und durch denselben Satz an Netzteilen mit Strom versorgt werden, schalten Sie das Chassis NICHT aus. Sie müssen

darauf achten, nur das Knoten 1-Controller-Modul zu entfernen. Normalerweise ist node1 Controller A, der sich auf der linken Seite des Chassis befindet, wenn man sich die Controller von der Rückseite des Systems ansieht. Das Controller-Etikett befindet sich direkt über dem Controller-Modul auf dem Chassis.

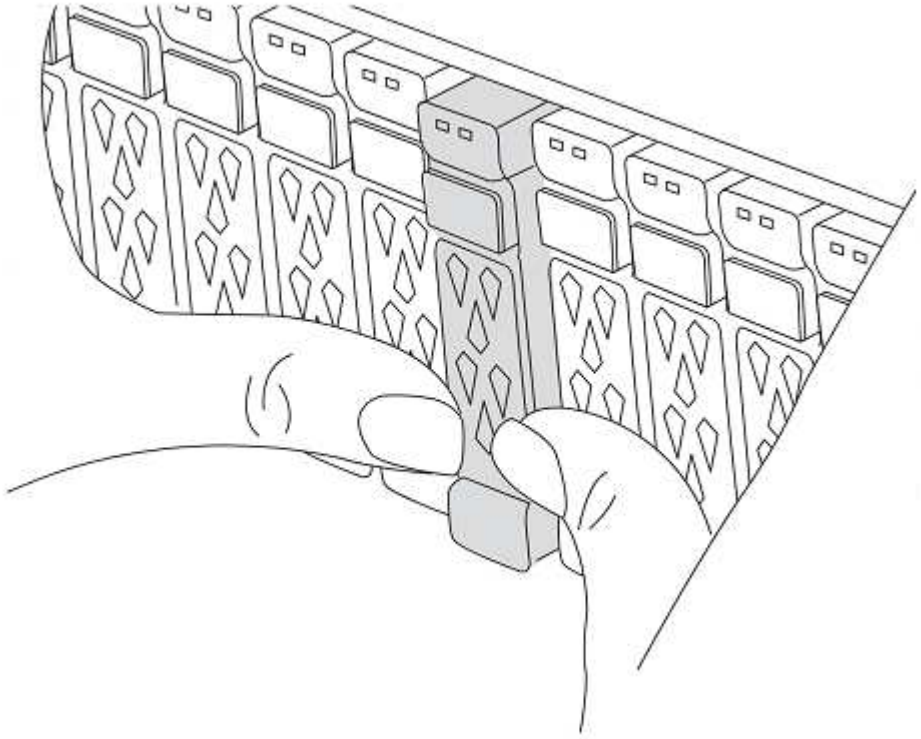
Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Bereiten Sie vor, das AFF A800 Controller-Modul zu entfernen

Schritte

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



2. Gehen Sie zur Rückseite des Gehäuses.

Entfernen Sie das AFF A800 Controller-Modul

Entfernen Sie das Kabelverwaltungsgerät vom AFF A800 Controller-Modul, und bewegen Sie den Controller leicht aus dem Gehäuse.

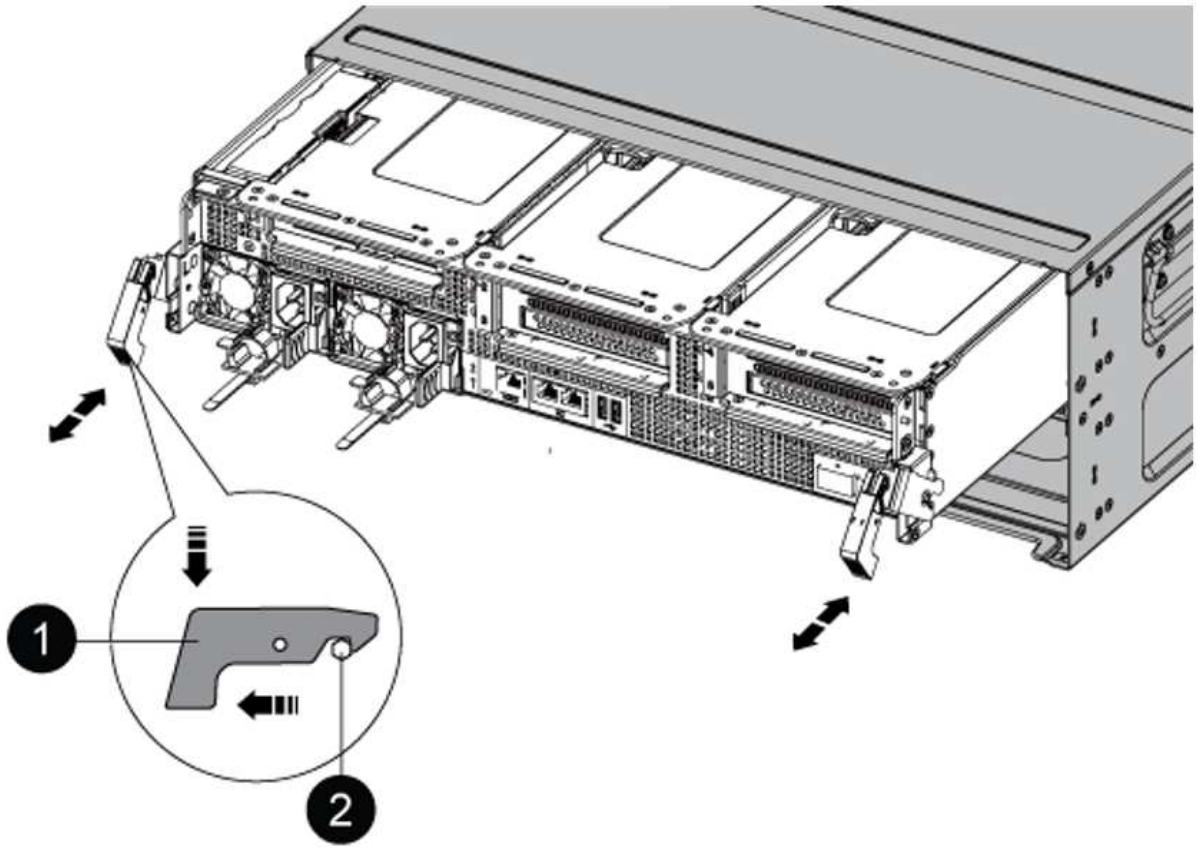
Schritte

1. Trennen Sie die Netzteile des node1-Controller-Moduls von der Quelle.
2. Lösen Sie die Netzkabelhalter, und ziehen Sie anschließend die Kabel von den Netzteilen ab.
3. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel an das Kabelmanagement-Gerät gebunden sind, und ziehen Sie dann die Systemkabel und SFP- und QSFP-Module (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.

Lassen Sie die Kabel im Kabelverwaltungs-Gerät so, dass bei der Neuinstallation des Kabelverwaltungsgeräts die Kabel organisiert sind.

4. Entfernen Sie das Kabelführungs-Gerät aus dem Controller-Modul und legen Sie es beiseite.
5. Drücken Sie beide Verriegelungsriegel nach unten, und drehen Sie dann beide Verriegelungen gleichzeitig nach unten.

   Das Controller-Modul wird leicht aus dem Chassis entfernt.



1	Verriegelungsverschluss
2	Sicherungsstift

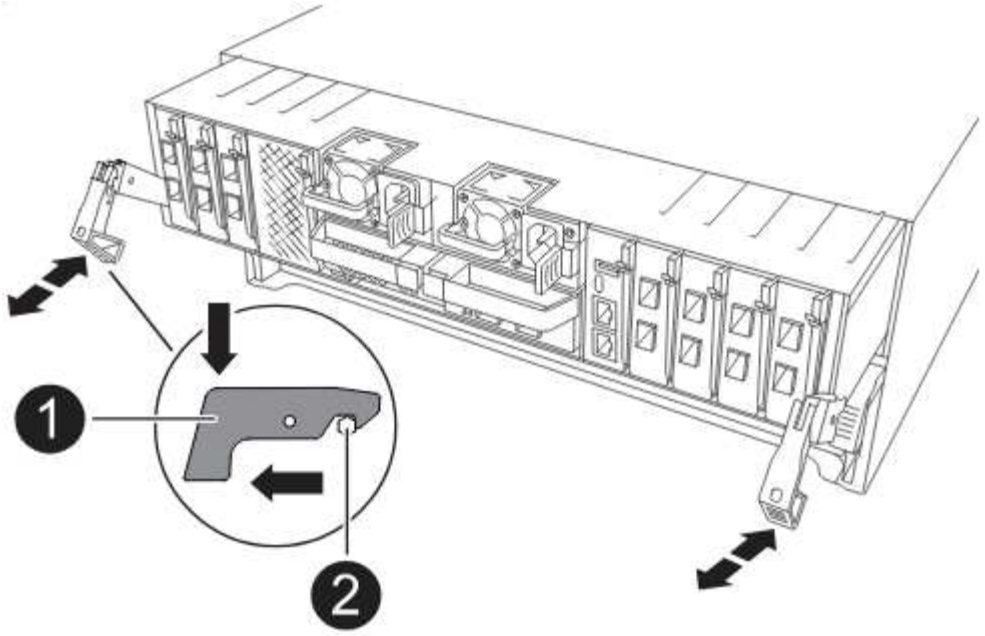
Installieren Sie das Controller-Modul AFF A90 oder AFF A70

Installieren, verkabeln und verbinden Sie das AFF A90- oder AFF A70-Controller-Modul in Knoten 1.

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.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.



2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

> Da das Chassis bereits EINGESCHALTET ist, startet Node 1 die BIOS-Initialisierung, gefolgt von AUTOBOOT, sobald Sie das neue Controller-Modul einsetzen. Um diesen AUTOBOOT ZU vermeiden, empfiehlt NetApp, die seriellen und die Konsolenkabel anzuschließen, bevor Sie das Controller-Modul einsetzen.

3. Schieben Sie das Steuermodul bei geöffnetem Nockengriff fest hinein, bis es auf die Mittelplatine trifft und vollständig eingesetzt ist. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Schließen Sie den Nockengriff in die verriegelte Position.

> Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten.

   Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node1 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.

6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

   ```
   set-defaults
   ```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

   ```
   saveenv
   ```

An dieser Stelle ist node1 ausgefallen und alle Daten werden von node2 bereitgestellt. Da sich Node1 und Node2 im gleichen Chassis befinden und durch denselben Satz an Netzteilen mit Strom versorgt werden, schalten Sie das Chassis NICHT aus. Sie müssen darauf achten, nur das Knoten 1-Controller-Modul zu entfernen. Normalerweise ist node1 Controller A, der sich auf der linken Seite des Chassis befindet, wenn man sich die Controller von der Rückseite des Systems ansieht. Das Controller-Etikett befindet sich direkt über dem Controller-Modul auf dem Chassis.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Entfernen Sie das Controller-Modul AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720

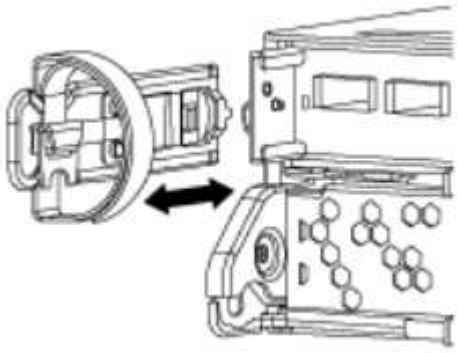
Um auf Komponenten im Controller zuzugreifen, entfernen Sie das Controller-Modul aus dem System und entfernen Sie dann die Abdeckung am Controller-Modul.

Schritte

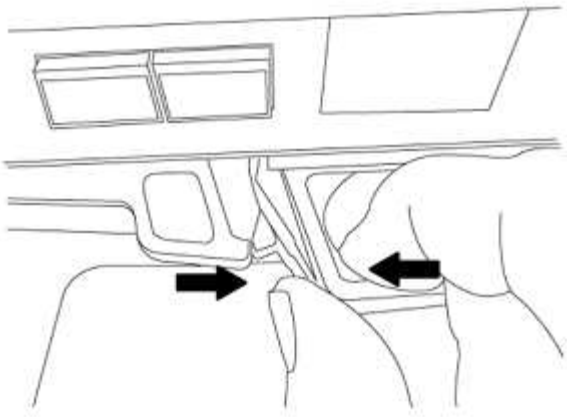
1. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel am Kabelführungsgerät befestigt sind, und ziehen Sie dann die Systemkabel und SFPs (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.

   Lassen Sie die Kabel im Kabelverwaltungs-Gerät so, dass bei der Neuinstallation des Kabelverwaltungsgeräts die Kabel organisiert sind.

2. Entfernen Sie die Kabelführungsgeräte von der linken und rechten Seite des Controller-Moduls und stellen Sie sie zur Seite.



3. Drücken Sie die Verriegelung am Nockengriff, bis sie loslässt, öffnen Sie den Nockengriff vollständig, um das Controller-Modul aus der Mittelplatine zu lösen, und ziehen Sie das Controller-Modul anschließend mit zwei Händen aus dem Gehäuse heraus.



4. Drehen Sie das Controller-Modul um und legen Sie es auf eine flache, stabile Oberfläche.

Installieren Sie das Controller-Modul ASA A150, AFF A150 oder FAS2820

Installieren, verkabeln und verbinden Sie das ASA A150-, AFF A150- oder FAS2820-Controller-Modul in Knoten1.

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.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

   Da das Gehäuse bereits EINGESCHALTET ist, startet node1 die BIOS-Initialisierung, gefolgt von AUTOBOOT, sobald es vollständig eingesetzt ist. Um den node1-Boot zu unterbrechen, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird, wird empfohlen, die serielle Konsole und die Verwaltungskabel mit dem node1-Controller-Modul zu verbinden.

3. Schieben Sie das Steuermodul bei geöffnetem Nockengriff fest hinein, bis es auf die Mittelplatine trifft und vollständig eingesetzt ist. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Schließen Sie den Nockengriff in die verriegelte Position.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node1 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

```
set-defaults
```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

```
saveenv
```

Ersetzen Sie den AFF A700- oder FAS9000-Controller und die NVRAM-Module

An dieser Stelle ist node1 ausgefallen und alle Daten werden von node2 bereitgestellt. Da sich Node1 und Node2 im gleichen Chassis befinden und durch denselben Satz an Netzteilen mit Strom versorgt werden, schalten Sie das Chassis NICHT aus. Achten Sie darauf, nur das Node1-Controller-Modul und das node1-NVRAM-Modul zu entfernen. Normalerweise ist node1 Controller A, der sich auf der linken Seite des Chassis befindet, wenn man sich die Controller von der Rückseite des Systems ansieht. Das Controller-Etikett befindet sich direkt über dem Controller-Modul auf dem Chassis.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

Trennen Sie das AFF A700- oder FAS9000-Controller-Modul von Knoten1, und entfernen Sie es.

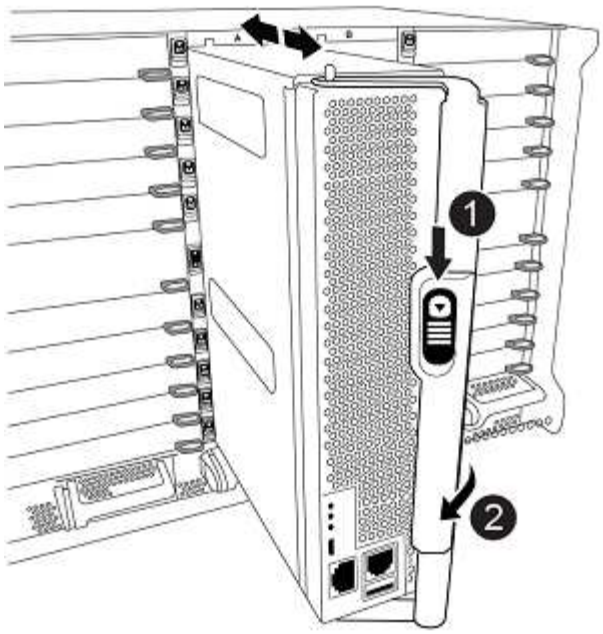
Schritte

1. Trennen Sie gegebenenfalls das Konsolenkabel und das Managementkabel vom Knoten 1-Controller-Modul.

Wenn Sie an node1 arbeiten, entfernen Sie nur die Konsole und E0M-Kabel von node1. Sie dürfen während dieses Vorgangs keine anderen Kabel oder Anschlüsse an node1 oder node2 entfernen oder austauschen.

2. Entriegeln und entfernen Sie das Controller-Modul A aus dem Gehäuse.

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



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse.

   Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder FAS9000 NVRAM-Modul

Entsperren und entfernen Sie das AFF A700 oder FAS9000 NVRAM-Modul aus Knoten1.

Das AFF A700 oder FAS9000 NVRAM-Modul befindet sich in Steckplatz 6 und hat die doppelte Höhe der anderen Module im System.

Schritte

1. Entriegeln und entfernen Sie das NVRAM-Modul aus Steckplatz 6 der Node1.

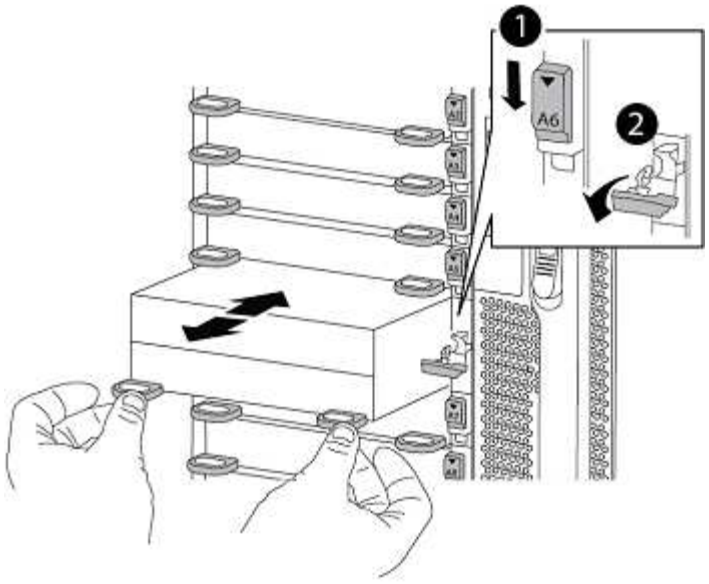
   a. Drücken Sie die Taste mit der Nummerierung und dem Buchstaben.

      Die Nockentaste bewegt sich vom Gehäuse weg.

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

      Das NVRAM-Modul geht aus dem Chassis aus und verschiebt ein paar Zentimeter.

   c. Entfernen Sie das NVRAM-Modul aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



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

Installieren Sie die NVRAM- und Controller-Module ASA A900, AFF A900 oder FAS9500

Installieren, verkabeln und verbinden Sie die NVRAM-Module ASA A900, AFF A900 oder FAS9500 in Knoten 1.

Bei der Installation müssen Sie Folgendes beachten:

- Verschieben Sie alle Leereinfüllmodule in den Steckplätzen 6-1 und 6-2 vom alten NVRAM-Modul in das neue NVRAM-Modul.
- Verschieben Sie das coredump-Gerät NICHT aus dem AFF A700 NVRAM-Modul in das ASA A900- oder AFF A900 NVRAM-Modul.
- Verschieben Sie alle Flash Cache Module, die im FAS9000 NVRAM-Modul installiert sind, auf das FAS9500 NVRAM-Modul.

Bevor Sie beginnen

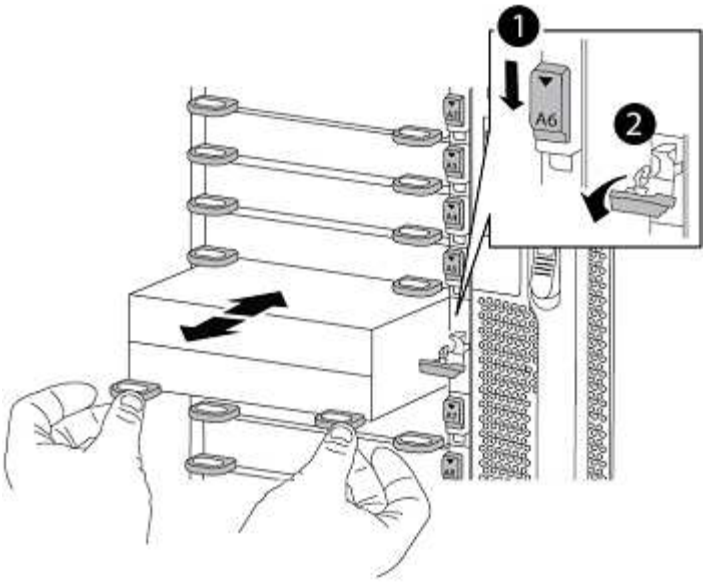
Wenn du nicht bereits geerdet bist, beground dich richtig.

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500 in Steckplatz 6 von Knoten1.

Schritte

1. Richten Sie das NVRAM-Modul an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie das NVRAM-Modul vorsichtig in den Steckplatz, 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 NVRAM-Moduls.



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

Installieren Sie das Controller-Modul ASA A900, AFF A900 oder FAS9500 auf Knoten1.

Gehen Sie wie folgt vor, um das Controller-Modul ASA A900, AFA A900 oder FAS9500 in Knoten1 zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung A im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.

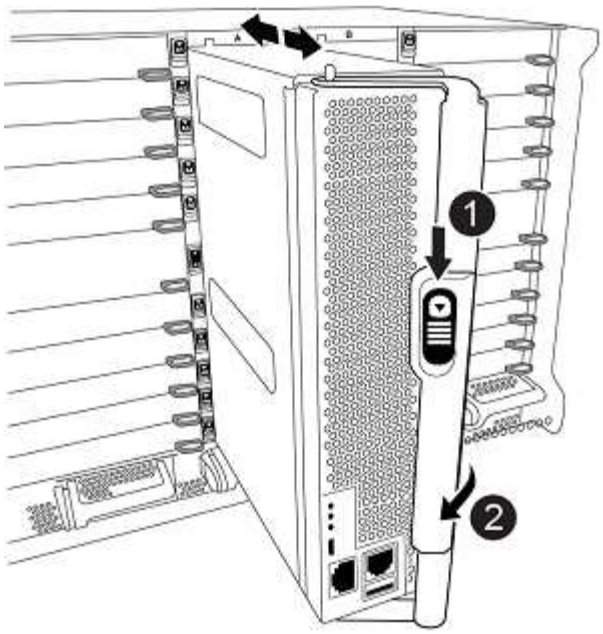
2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

   Da das Gehäuse bereits EINGESCHALTET ist, startet node1 die BIOS-Initialisierung, gefolgt von AUTOBOOT, sobald es vollständig eingesetzt ist. Um den node1-Boot zu unterbrechen, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird, wird empfohlen, die serielle Konsole und die Verwaltungskabel mit dem node1-Controller-Modul zu verbinden.

3. 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.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.



1	Verriegelungsverschluss am CAM-Griff
2	Nockengriff in der nicht entriegeln Position

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node1 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

   ```
   set-defaults
   ```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

   ```
   saveenv
   ```

Netzboot Nr. 1

Nach dem Austausch der entsprechenden Ersatz-Systemmodule müssen Sie netboot node1. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf Netzboot fügen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver hinzu, auf den das System zugreifen kann.

Es ist nicht möglich, die auf dem Boot-Medium des Ersatz-Controller-Moduls installierte ONTAP-Version zu

überprüfen, es sei denn, sie ist in einem Gehäuse installiert und eingeschaltet. Die ONTAP-Version auf dem Ersatz-System-Boot-Medium muss mit der ONTAP-Version auf dem alten System übereinstimmen, das Sie aktualisieren, und sowohl die primären als auch die Backup-Boot-Images auf dem Boot-Medium müssen übereinstimmen. Informationen zur Überprüfung der unterstützten ONTAP-Mindestversion für Ihr Upgrade finden Sie unter "Überblick".

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.

Sie können den Netzboot auch über die USB-Boot-Option ausführen. Weitere Informationen finden Sie im Knowledge Base-Artikel "So verwenden Sie den Boot_Recovery-LOADER-Befehl zum Installieren von ONTAP für die Ersteinrichtung eines Systems".

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Laden Sie die für Ihr System erforderlichen Systemdateien und die korrekte Version von ONTAP von *NetApp Support Site* herunter. Siehe "Quellen" Link zur NetApp Support Site_.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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. Siehe "Quellen" Um eine Verknüpfung zur NetApp Support Site_ zu erhalten, um die Dateien zum Ausführen des Netzboots des Systems herunterzuladen.
2. Laden Sie die entsprechende ONTAP Software aus dem Bereich zum Software Download 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 enthalten `<ontap_version>_image.tgz`.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Ist der Domain-Name (DNS) (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

6. Ausführen des Netzboots auf Knoten 1:

   `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis der Knoten 1 auf dem Ersatz-Controller-Modul gestartet wird und die Optionen des Startmenüs wie unten gezeigt angezeigt werden:

```
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.

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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

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` Zu den Aufforderungen, bis der Node im Wartungsmodus und mit der Eingabeaufforderung angehalten wird `*>`.
13. Vergewissern Sie sich, dass Controller und Chassis als konfiguriert sind `ha`:

    `ha-config show`

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

14. Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

    `ha-config modify controller ha`

    `ha-config modify chassis ha`

15. Überprüfen Sie die `ha-config` Einstellungen:

    `ha-config show`

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

16. Stopp-Nr. 1:

    `halt`

    Node1 sollte an der LOADER-Eingabeaufforderung angehalten werden.

17. Überprüfen Sie in node2 das Systemdatum, die Uhrzeit und die Zeitzone:

    `date`

18. Überprüfen Sie bei node1 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    `show date`

19. Legen Sie bei Bedarf das Datum auf Knoten 1 fest:

    `set date` *`mm/dd/yyyy`*

    Legen Sie das entsprechende UTC-Datum auf Knoten 1 fest.

20. Überprüfen Sie bei node1 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

21. Stellen Sie bei Bedarf die Zeit auf node1 ein:

```
set time hh:mm:ss
```

> Legen Sie die entsprechende UTC-Zeit auf node1 fest.

22. Legen Sie die Partner-System-ID auf node1 fest:

```
setenv partner-sysid node2_sysid
```

Für node1, die `partner-sysid` Muss der von node2 sein. Sie können die System-ID node2 vom beziehen `node show -node node2` Befehlsausgabe auf node2.

a. Einstellungen speichern:

```
saveenv
```

23. Überprüfen Sie bei node1 an der LOADER-Eingabeaufforderung den `partner-sysid` Für Knoten 1:

```
printenv partner-sysid
```

Phase 3: Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Phase-3-Übersicht

In Phase 3 verbinden Sie die gemeinsam genutzten Cluster-HA- und Speicherverbindungen für die externen Shelfs, falls vorhanden, starten Sie Knoten 1 mit den aktualisierten Systemmodulen und überprüfen Sie die aktualisierte Installation von Knoten 1. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1 Aggregate und NAS-Daten-LIFs von node2 auf die aktualisierte Node1 verschoben und Sie überprüfen, ob die SAN-LIFs auf node1 vorhanden sind.

Schritte

1. "Kabelnode1 für Shared Cluster-HA-Storage (nur AFF A800 Upgrade)"
2. "Starten Sie Knoten 1 mit den Ersatz-Systemmodulen"
3. "Überprüfen Sie die Installation node1"
4. "Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her"
5. "Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1"

Kabelnode1 für Shared Cluster-HA und Storage (nur AFF A800 Upgrade)

Alle Cluster-, HA-, Storage- und Datenverbindungen, die zuvor mit dem AFF A800 Knoten 1 verbunden waren, sollten jetzt mit der neu installierten AFF A90 oder AFF A70 Knoten 1 verbunden werden.

Die folgende Tabelle zeigt die Auslastung der Switch-Ports für Cluster-Konfigurationen mit zwei Nodes ohne Switch.

Port	AFF A800 Node	AFF A90-Knoten	AFF A70-Knoten
Cluster	e0a	e1a	e1a
Cluster	e1a	E7a (e1b verwenden, wenn kein e7a vorhanden ist)	e1b
HA	e0b	Nicht verbinden	Nicht verbinden
HA	e1b	Nicht verbinden	Nicht verbinden
SAS-Storage-Ports (sofern vorhanden und verwendet)	Jeder verfügbare Port	Jeder verfügbare Port	Jeder verfügbare Port
Ethernet-Storage-Ports für NS224-Shelfs	Jeder verfügbare Port	Weitere Informationen finden Sie unter Verbindungszuordnung für Ethernet-Speicher	Weitere Informationen finden Sie unter Verbindungszuordnung für Ethernet-Speicher

Bei einem Switch Attached-Cluster sollten sich die identischen Cluster-Ports auf den AFF A90- oder AFF A70-Nodes auf demselben Switch befinden. Beispiel: Nach Abschluss des Upgrades sollte e1a auf node1 und e1a auf node2 mit einem Cluster-Switch verbunden werden. Gleichermaßen sollte der zweite Cluster-Port beider Nodes mit dem zweiten Cluster-Switch verbunden sein. Cross-Verbindung von gemeinsam genutzten Cluster-HA-Ports, wobei e1a von node1 mit SwitchA und e1a von node2 mit SwitchB verbunden ist, verhindert HA-Kommunikationsfehler.

Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Node1 mit den Ersatzmodulen ist nun startbereit. In diesem Abschnitt werden die Schritte beschrieben, die zum Starten von Knoten 1 mit den Ersatzmodulen für die folgenden Upgrade-Konfigurationen erforderlich sind:

Vorhandener Knoten 1-Controller	Ersatz-Knoten 1-Systemmodule
AFF A800	AFF A90 oder AFF A70 [1]
AFF A220 als ASA konfiguriert	AFF A150-Controller-Modul [1]
AFF A220 AFF A200 AFF C 190	AFF A150-Controller-Modul [1]
FAS2620 FAS2720	FAS2820 Controller-Modul [1]
AFF A700 – als ASA konfiguriert	ASA A900-Controller und NVRAM-Module [2]
AFF A700	AFF A900-Controller und NVRAM-Module [2]
FAS9000	FAS9500 Controller- und NVRAM-Module [2]

[1] beim Austausch von Controller-Modulen verschieben Sie alle Verbindungen vom alten zum Ersatz-Controller-Modul.

[2] beim Austauschen des Controllers und der NVRAM-Module verschieben Sie nur die Konsole und die Managementverbindungen.

Schritte

1. (Nur AFF A800 Upgrade) wechseln Sie an der Eingabeaufforderung des LOADERS in den Wartungsmodus:

   `boot_ontap maint`

   a. Beantworten Sie `yes` die Bestätigungsaufforderung.

   b. Zeigen Sie den Status der 100-GbE-Schnittstellen an:

      `storage port show.`

      Alle mit NS224-Shelfs oder Storage-Switches verbundenen 100-GbE-Ports sollten als Ports gemeldet werden `storage` , wie im Beispiel-Output unten dargestellt.

```
*> storage port show
Port Type Mode    Speed(Gb/s) State    Status  VLAN ID
---- ---- ------- ----------- -------- ------- -------
e8a  ENET storage 100 Gb/s    enabled  online  30
e8b  ENET storage 100 Gb/s    enabled  online  30
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

   a. Beenden des Wartungsmodus:

      `halt`

2. Wenn Sie NSE-Laufwerke (NetApp Storage Encryption) installiert haben, führen Sie die folgenden Schritte durch.

   Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

   a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	**Dann…**
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

   FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

   Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

3. Starten Sie den Knoten im Startmenü:

   ```
   boot_ontap menu
   ```

4. Weisen Sie die alten node1-Festplatten dem Ersatznode1 neu zu, indem Sie „22/7“ eingeben und die versteckte Option auswählen `boot_after_controller_replacement` Wenn der Node im Boot-Menü angehalten wird.

   Nach einer kurzen Verzögerung werden Sie aufgefordert, den Namen des Node einzugeben, der ersetzt wird. Wenn gemeinsam genutzte Festplatten vorhanden sind (auch Advanced Disk Partitioning (ADP) oder partitionierte Festplatten), werden Sie aufgefordert, den Node-Namen des HA-Partners einzugeben.

   Diese Eingabeaufforderungen sind möglicherweise in den Konsolenmeldungen verborgen. Wenn Sie keinen Node-Namen eingeben oder einen falschen Namen eingeben, werden Sie aufgefordert, den Namen erneut einzugeben.

   > Wenn `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` Und oder `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` Fehler auftreten, führen Sie die folgenden Schritte aus:
   >
   > a. Halten Sie den Node an der LOADER-Eingabeaufforderung an.
   > b. Überprüfen und setzen Sie die Speicherverschlüsselung Bootargs in erwähnt Schritt 2.
   > c. Starten Sie an der LOADER-Eingabeaufforderung:
   >
   >    ```
   >    boot_ontap
   >    ```

   Das folgende Beispiel kann als Referenz verwendet werden:

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

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)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

Die im vorhergehenden Beispiel gezeigten System-IDs sind Beispiel-IDs. Die tatsächlichen System-IDs der Nodes, die Sie aktualisieren, unterscheiden sich.

Zwischen der Eingabe von Node-Namen an der Eingabeaufforderung und der Eingabeaufforderung für die Anmeldung wird der Node mehrmals neu gebootet, um die Umgebungsvariablen wiederherzustellen, die Firmware auf den im System verwendeten Karten zu aktualisieren und für andere ONTAP Updates zu sorgen.

Überprüfen Sie die Installation node1

Nachdem Sie node1 mit dem Ersatz-Controller-Modul gestartet haben, überprüfen Sie, ob es richtig installiert ist.

Nur bei AFF A800-Upgrades weisen Sie die physischen Ports des vorhandenen Knoten1 dem Ersatznode1 zu, da sich die physischen Ports zwischen der AFF A800 und dem AFF A90- oder AFF A70-Controller ändern.

Bei allen anderen Upgrades werden die physischen Ports nicht geändert, sodass Sie die physischen Ports des alten Knoten1 nicht dem Ersatznode1 zuordnen müssen.

Über diese Aufgabe

Sie müssen warten, bis Knoten 1 dem Quorum beitreten und dann den Controller-Austauschvorgang fortsetzen.

An diesem Punkt in der Prozedur sollte der Upgrade-Vorgang des Controllers angehalten sein, da node1 versucht hat, Quorum automatisch beizutreten.

Schritte

1. Vergewissern Sie sich, dass node1 dem Quorum beigetreten ist:

   ```
   cluster show -node node1 -fields health
   ```

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node1 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

   Wenn node1 nach dem Booten noch nicht dem Quorum beigetreten ist, warten Sie fünf Minuten, und überprüfen Sie es erneut. Je nach Cluster-Verbindung kann es einige Zeit dauern, bis der Scan der Erreichbarkeit von Ports abgeschlossen und LIFs an die jeweiligen Home Ports verschoben werden.

   Wenn node1 nach fünf Minuten immer noch nicht im Quorum ist, können Sie den Cluster-Port des neuen Knotens ändern, indem Sie ihn mit dem Diagnoseberechtigungsbefehl in „Cluster ipspace“ platzieren `network port modify <port_name> -ipspace Cluster`.

3. Wechseln in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

4. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand wie zuvor in node1 befand, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

   ```
   system controller replace show

   system controller replace show-details
   ```

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Controller-Ersatzvorgang hält für Eingriffe mit der folgenden Meldung an:

```
Cluster::*> system controller replace show
Node          Status                      Error-Action
------------  --------------------------
-------------------------------------
Node1         Paused-for-intervention     Follow the instructions given
in
                                          Step Details
Node2         None

Step Details:
---------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:


1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.
2 entries were displayed.
```

> In diesem Verfahren wurde Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node1_ umbenannt.

7. Wenn sich der Controller-Austausch im Status „Pause“ befindet, fahren Sie mit fort Stellen Sie die Netzwerkkonfiguration auf node1 wieder her.

Stellen Sie die Netzwerkkonfiguration auf node1 wieder her

Nachdem Sie bestätigt haben, dass node1 sich im Quorum befindet und mit node2 kommunizieren kann, überprüfen Sie, dass node1 VLANs, Interface Groups und Broadcast-Domains auf node1 gesehen werden. Überprüfen Sie außerdem, ob alle node1-Netzwerk-Ports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Zum Verknüpfen mit dem Inhalt *Network Management*.

Schritte

1. Listen Sie alle physischen Ports auf, die auf Upgrade-Knoten1 stehen:

   ```
   network port show -node node1
   ```

   Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. In dieser Ausgabe sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um die Entscheidung zu erleichtern, welche Ports als Ports für Schnittstellengruppen, als VLAN-Basis-Ports oder als eigenständige physische Ports zum Hosten von LIFs verwendet werden sollten.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node1 auflisten:

   ```
   network port reachability show -node node1
   ```

   Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ------------------------------------
---------------------
Node1
          a0a      Default:Default                      ok
          a0a-822  Default:822                          ok
          a0a-823  Default:823                          ok
          e0M      Default:Mgmt                         ok
          e1a      Cluster:Cluster                      ok
          e1b      -                                    no-reachability
          e2a      -                                    no-reachability
          e2b      -                                    no-reachability
          e3a      -                                    no-reachability
          e3b      -                                    no-reachability
          e7a      Cluster:Cluster                      ok
          e7b      -                                    no-reachability
          e9a      Default:Default                      ok
          e9a-822  Default:822                          ok
          e9a-823  Default:823                          ok
          e9b      Default:Default                      ok
          e9b-822  Default:822                          ok
          e9b-823  Default:823                          ok
          e9c      Default:Default                      ok
          e9d      Default:Default                      ok
20 entries were displayed.
```

In den vorhergehenden Beispielen wurde node1 nach dem Austausch des Controllers gestartet. Die Ports, die „nicht-Erreichbarkeit“ anzeigen, verfügen über keine physische Verbindung. Sie müssen alle Ports mit einem anderen Status als reparieren `ok`.

> Während des Upgrades sollten sich die Netzwerkports und ihre Konnektivität nicht ändern. Alle Ports sollten sich in den richtigen Broadcast-Domänen befinden, und die Erreichbarkeit des Netzwerkports sollte sich nicht ändern. Bevor Sie jedoch LIFs von node2 zurück auf node1 verschieben, müssen Sie die Erreichbarkeit und den Integritätsstatus der Netzwerk-Ports überprüfen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node1 mit einem anderen Status als der Erreichbarkeit `ok` Mit dem folgenden Befehl in der folgenden Reihenfolge:

   `network port reachability repair -node` *`node_name`* `-port` *`port_name`*

   a. Physische Ports

   b. VLAN-Ports

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node1 -port e1b
```

```
Warning: Repairing port "node1:e1b" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Eine Warnmeldung, wie im vorhergehenden Beispiel dargestellt, wird für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Erreichbarkeit der Broadcast-Domäne unterscheiden können, in der sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

```
network port reachability show
```

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Überprüfen der Port-Erreichbarkeit:

   ```
   network port reachability show
   ```

   Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn ein Port einen anderen Status als diese beiden meldet, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

6. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

   ```
   network port show
   ```

7. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

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

8. Stellen Sie die LIF-Home-Ports wieder her und geben Sie ggf. den Vserver und die LIF-Home-Ports an, die Sie mit folgenden Schritten wiederherstellen müssen:

   a. Führen Sie alle vertriebenen LIFs auf:

      ```
      displaced-interface show
      ```

   b. LIF-Home-Knoten und Home-Ports wiederherstellen:

```
displaced-interface restore-home-node -node node_name -vserver vserver_name
-lif-name LIF_name
```

9. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

```
network interface show -fields home-port,status-admin
```

Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her

Wenn Sie NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) zur Verschlüsselung von Volumes auf dem System verwenden, das Sie aktualisieren, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht neu synchronisieren, wenn Sie die node1-Aggregate mithilfe von ARL von node2 zur aktualisierten node1 verschieben, können Ausfälle auftreten, da node1 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie den folgenden Befehl aus node1:

```
security key-manager onboard sync
```

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node1 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node1 -fields restored -key
-type SVM-KEK
```

Beispiel

```
::> security key-manager key query -node node1 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node1    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1

Nachdem Sie die Netzwerkkonfiguration auf Knoten 1 überprüft und bevor Sie Aggregate von Knoten 2 zu Knoten 1 verschieben, überprüfen Sie, ob die NAS-Daten-LIFs, die zu Knoten 1 gehören, die sich derzeit auf Knoten 2 befinden, von Knoten 2 zu Knoten 1 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN LIFs auf Knoten1 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Nachdem Sie node1 in den Online-Modus versetzt haben, müssen Sie überprüfen, ob sich die LIFs in einem ordnungsgemäßen Zustand und auf den entsprechenden Ports befinden.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Durchführen einer Prüfung der Netzwerkfähigkeit:

   ```
   network port reachability show -node node1
   ```

   Vergewissern Sie sich, dass alle verbundenen Ports, einschließlich der Schnittstellengruppe und VLAN-Ports, ihren Status als anzeigen `OK`.

3. Wenn Sie ein AFF A800 Upgrade auf ein AFF A70 oder AFF A90 durchführen möchten, müssen Sie die FCP SAN LIFs neu zuweisen. Bei allen anderen System-Upgrades fahren Sie fort mit Schritt 4:

   a. Neuzuweisung von FCP-SAN-LIFs für FCP- oder FC-NVMe-Datenzugriff an die korrekten Home Ports:

      ```
      network interface show -vserver <vserver_hosting_fcp_lifs>
      ```

   b. Bei LIFs, deren aktueller Node als aktualisierter node1 angegeben wird und der aktuelle Port den Status „oper“ als „-“ meldet (da der Port auf dem AFF A800 Node vorhanden war, jedoch nicht auf dem AFF A90 Node vorhanden ist), ändern Sie den aktuellen Port, bevor er online geschaltet werden kann.

      Überprüfen Sie, ob die physische Konnektivität zum FC-Zielport hergestellt ist, an den die FC-LIF verschoben werden muss:

i. Legen Sie den LIF-Status auf „down“ fest:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

ii. Ändern Sie den Home Port des LIF:

```
network interface modify -vserver <vserver_name> -lif <lif_name> - home-
node <node1> -home-port <FC_target_port>
```

iii. Legen Sie den LIF-Status auf „up“ fest:

```
network interface modify -vserver <vserver> -lif <lif_name> -status-admin
up
```

Wiederholen Sie die Teilschritte a und b für jede FC-SAN-LIF, die sich als Home in Knoten 1 befindet.

4. Umzugsvorgang fortsetzen:

```
system controller replace resume
```

Das System führt folgende Prüfungen durch:

- Cluster-Zustandsprüfung
- LIF-Statusüberprüfung für Cluster

Nach Durchführung dieser Prüfungen verschiebt das System die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, in die neue Knoten1.

Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

5. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

```
system controller replace show-details
```

Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

6. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

```
cluster controller-replacement network displaced-interface show
```

Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in node1 wieder her:

```
cluster controller-replacement network displaced-interface restore-home-node
```

7. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

```
system controller replace resume
```

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung

- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster
- Lautstärkerprüfung

Phase 4. Verschieben von Ressourcen und Ausmustern von Knoten2

Phase-4-Übersicht

Während Phase 4 verschieben Sie Aggregate und NAS-Daten-LIFs von Knoten 2 auf die aktualisierte Knoten 1 und Mustern Knoten 2 aus.

Schritte

1. "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs von Knoten 2 auf Knoten 1"
2. "Node2 ausmustern"

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs von Knoten 2 auf Knoten 1

Bevor Sie Knoten 2 durch das Ersatz-Systemmodul ersetzen können, müssen Sie zunächst die nicht-Root-Aggregate, die im Besitz von Knoten 2 sind, in Knoten 1 verschieben.

Bevor Sie beginnen

Nach den Nachprüfungen aus der vorherigen Phase wird automatisch die Ressourcenfreigabe für node2 gestartet. Die Aggregate außerhalb des Root-Bereichs und LIFs für nicht-SAN-Daten werden von node2 in die neue Knoten1 migriert.

Über diese Aufgabe

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. An dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in die neue Knoten1 migriert werden.

Der Home-Inhaber für die Aggregate und LIFs werden nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind und ihren Status auf node1:

   ```
   storage aggregate show -node node1 -state online -root false
   ```

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node1 online sind:

```
cluster::> storage aggregate show -node node1 state online -root false

Aggregate     Size        Available   Used%   State   #Vols  Nodes
RAID     Status
----------    ---------   ---------   ------  -----   -----  ------
-------  ------
aggr_1        744.9GB     744.8GB     0%      online      5  node1
raid_dp  normal
aggr_2        825.0GB     825.0GB     0%      online      1  node1
raid_dp  normal
2 entries were displayed.
```

Wenn die Aggregate offline gegangen sind oder in node1 fremd geworden sind, stellen Sie sie mit dem folgenden Befehl auf der neuen node1, einmal für jedes Aggregat online:

`storage aggregate online -aggregate` *`aggr_name`*

2. Überprüfen Sie, ob alle Volumes auf node1 online sind, indem Sie den folgenden Befehl auf node1 verwenden und seine Ausgabe überprüfen:

   `volume show -node node1 -state offline`

   Wenn ein Volume auf node1 offline ist, stellen Sie sie mit dem folgenden Befehl auf node1 für jedes Volume online:

   `volume online -vserver` *`vserver-name`* `-volume` *`volume-name`*

   Der *`vserver-name`* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

3. Überprüfen Sie, ob die LIFs zu den richtigen Ports verschoben wurden und über den Status von verfügen `up`. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`nodename`* `- status-admin up`

4. Überprüfen Sie, ob auf node2 keine Daten-LIFs mehr vorhanden sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

   `network interface show -curr-node` *`node2`* `-role data`

Node2 ausmustern

Um node2 außer Betrieb zu nehmen, schalten Sie node2 zunächst ordnungsgemäß aus und entfernen Sie es aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

```
system controller replace resume
```

Der Knoten wird automatisch angehalten.

Nachdem Sie fertig sind

Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5. Installieren Sie die Ersatz-Systemmodule auf Knoten 2

Phase-5-Übersicht

In Phase 5 installieren Sie die neuen Systemmodule, die Sie für den aktualisierten Knoten 2 erhalten haben, und dann Netboot Knoten 2.

Schritte

1. "Installieren Sie die Ersatz-Systemmodule auf Knoten 2"
2. "Netzboot Nr. 2"

Installieren Sie die Ersatz-Systemmodule auf Knoten 2

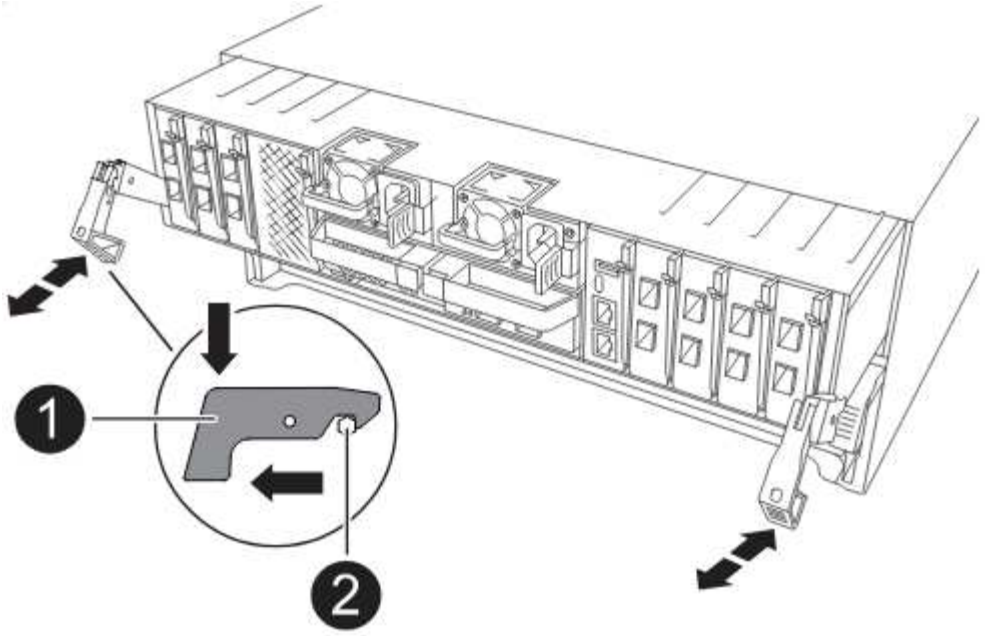
Installieren Sie das AFF A90- oder AFF A70-Modul auf Knoten 2

Installieren Sie das AFF A90- oder AFF A70-Controller-Modul, das Sie für das Upgrade auf Knoten2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

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.

> Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.



2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

> Da das Gehäuse bereits EINGESCHALTET ist, startet node1 die BIOS-Initialisierung, gefolgt von AUTOBOOT, sobald es vollständig eingesetzt ist. Um den node1-Boot zu unterbrechen, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird, wird empfohlen, die serielle Konsole und die Verwaltungskabel mit dem node1-Controller-Modul zu verbinden.

3. Schieben Sie das Steuermodul bei geöffnetem Nockengriff fest hinein, bis es auf die Mittelplatine trifft und vollständig eingesetzt ist. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Schließen Sie den Nockengriff in die verriegelte Position.

> Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node1 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

```
set-defaults
```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

```
saveenv
```

Installieren Sie das ASA A150, AFF A150 oder FAS2820 Controller-Modul auf Knoten2

Installieren Sie das ASA A150, AFF A150 oder FAS2820 Controller-Modul, das Sie für das Upgrade auf Knoten2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

Bevor Sie beginnen

- Wenn du nicht bereits geerdet bist, beground dich richtig.
- Trennen Sie alle Kabel, einschließlich Konsole, Management, SAS Storage und Datennetzwerkkabel, vom entfernten Controller.

Schritte

1. Richten Sie das Ende des Controller-Moduls an Schacht B im Chassis aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Bay B befindet sich auf dem Chassis unten.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu später beim Verfahren aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem node2-Controller-Modul.

   Da das Chassis bereits eingeschaltet ist, startet node2, sobald es vollständig eingesetzt ist. Um das Booten von node2 zu vermeiden, empfiehlt NetApp, die Konsole und die Managementkabel an das node2-Controller-Modul anzuschließen, bevor Sie das Controller-Modul vollständig in den Steckplatz einsetzen.

3. 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.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node2 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node2 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.

Installieren Sie ASA A900, AFF A900 oder FAS9500 NVRAM und Controller-Module auf Knoten2

Installieren Sie die ASA A900, AFF A900 oder FAS9500 NVRAM- und Controller-Module, die Sie für das Upgrade auf Node2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

Bei der Installation müssen Sie Folgendes beachten:

- Verschieben Sie alle Leereinfüllmodule in den Steckplätzen 6-1 und 6-2 vom alten NVRAM-Modul in das neue NVRAM-Modul.
- Verschieben Sie das coredump-Gerät NICHT aus dem AFF A700 NVRAM-Modul in das ASA A900- oder AFF A900 NVRAM-Modul.
- Verschieben Sie alle Flash Cache Module, die im FAS9000 NVRAM-Modul installiert sind, auf das FAS9500 NVRAM-Modul.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500 in Steckplatz 6 von Knoten2.

Schritte

1. Richten Sie das NVRAM-Modul an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie das NVRAM-Modul vorsichtig in den Steckplatz, 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 NVRAM-Moduls.

Installieren Sie das Controller-Modul ASA A900, AFF A900 oder FAS9500 in Knoten2

Installieren, verkabeln und verbinden Sie das ASA A900-, AFF A900- oder FAS9500-Controller-Modul in Knoten2.

Schritte

1. Richten Sie das Ende des Controller-Moduls an Schacht B im Chassis aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Das Bay-Etikett befindet sich auf dem Chassis direkt über dem Controller-Modul.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu später beim Verfahren aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem node2-Controller-Modul.

   Da das Chassis bereits eingeschaltet ist, startet node2, sobald es vollständig eingesetzt ist. Um das Booten von node2 zu vermeiden, wird empfohlen, die Konsole und die Managementkabel mit dem node2-Controller-Modul zu verbinden, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird.

3. 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.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.

5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node2 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie das AUTOBOOT nicht rechtzeitig unterbrechen und node2 startet den Boot-Vorgang, warten Sie auf die Eingabeaufforderung und drücken Sie Strg-C, um zum Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option `8` , um den Node neu zu booten und DAS AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung LOADER> von node2 die Standardumgebungsvariablen fest:

   `set-defaults`

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

   `saveenv`

Netzboot Nr. 2

Nachdem Sie die entsprechenden Node2-Ersatzsystemmodule ausgetauscht haben, müssen Sie sie möglicherweise mit dem Netzboot starten. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf den Netzboot legen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver, auf den das System zugreifen kann.

Es ist nicht möglich, die auf dem Boot-Medium des Ersatz-Controller-Moduls installierte ONTAP-Version zu überprüfen, es sei denn, sie ist in einem Gehäuse installiert und eingeschaltet. Die ONTAP-Version auf dem Ersatz-System-Boot-Medium muss mit der ONTAP-Version auf dem alten System identisch sein, das Sie aktualisieren, und sowohl das primäre als auch das Backup-Boot-Image müssen 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.

Sie können den Netzboot auch über die USB-Boot-Option ausführen. Weitere Informationen finden Sie im Knowledge Base-Artikel "So verwenden Sie den Boot_Recovery-LOADER-Befehl zum Installieren von ONTAP für die Ersteinrichtung eines Systems".

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Laden Sie die für Ihr System erforderlichen Systemdateien und die korrekte Version von ONTAP von *NetApp Support Site* herunter. Siehe "Quellen" Link zur NetApp Support Site_.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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. Siehe "Quellen" Um eine Verknüpfung zur NetApp Support Site_ zu erhalten, um die Dateien zum Ausführen des Netzboots des Systems herunterzuladen.
2. Laden Sie die entsprechende ONTAP Software im Bereich Software Download der NetApp Support Website 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 enthalten `<ontap_version>_image.tgz`.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie müssen 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 DHCP (Dynamic Host Configuration Protocol) lautet…	**Dann…**
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Ist der Domain-Name (DNS) (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

6. Ausführen eines Netzboots auf Knoten 2:

```
netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel
```

> Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis node2 jetzt auf dem Ersatz-Controller-Modul ausgeführt wird, um zu starten und die Boot-Menüoptionen anzuzeigen, wie in der folgenden Ausgabe 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)?
```

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.

   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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

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 Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
13. Vergewissern Sie sich, dass Controller und Chassis als konfiguriert sind `ha`:

    ```
    ha-config show
    ```

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

14. Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

    ```
    ha-config modify controller ha

    ha-config modify chassis ha
    ```

15. Stopp-Nr. 2:

    ```
    halt
    ```

    Node2 sollte an DER Loader>-Eingabeaufforderung angehalten werden.

16. Überprüfen Sie auf Knoten 1 das Systemdatum, die Uhrzeit und die Zeitzone:

    ```
    date
    ```

17. Überprüfen Sie bei node2 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    `show date`

18. Legen Sie bei Bedarf das Datum auf node2 fest:

    `set date mm/dd/yyyy`

    Setzen Sie das entsprechende UTC-Datum auf node2.

19. Überprüfen Sie bei node2 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    `show time`

20. Stellen Sie bei Bedarf die Zeit auf node2 ein:

    `set time hh:mm:ss`

    Legen Sie die entsprechende UTC-Zeit auf node2 fest.

21. Legen Sie die Partner-System-ID auf node2 fest:

    `setenv partner-sysid node1_sysid`

    Für node2, die `partner-sysid` Muss der Knoten 1 sein, den Sie aktualisieren.

    a. Einstellungen speichern:

       `saveenv`

22. Überprüfen Sie in node2 an der LOADER-Eingabeaufforderung den `partner-sysid` Für Knoten 2:

    `printenv partner-sysid`

Phase 6. Starten Sie Knoten2 mit den Ersatz-Systemmodulen

Phase-6-Übersicht

In Phase 6 starten Sie Knoten 2 mit aktualisierten Systemmodulen und überprüfen die aktualisierte Installation von Knoten 2. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1-Aggregate und NAS-Daten-LIFs von node1 auf die aktualisierte Node2 verschoben und Sie überprüfen, ob die SAN-LIFs auf node2 vorhanden sind.

1. "Starten Sie Knoten2 mit den Ersatz-Systemmodulen"
2. "Überprüfen Sie die Installation node2"
3. "Wiederherstellen der Key-Manager-Konfiguration auf node2"

4. "Verschieben Sie Aggregate und NAS-Daten-LIFs zurück auf node2"

Starten Sie Knoten2 mit den Ersatz-Systemmodulen

Node2 mit den Ersatzmodulen ist nun startbereit. Bei der Aktualisierung durch Austausch der Systemmodule werden nur die Konsolen- und Managementverbindungen verschoben. In diesem Abschnitt werden die Schritte beschrieben, die zum Starten von Knoten2 mit den Ersatzmodulen für die folgenden Upgrade-Konfigurationen erforderlich sind:

Vorhandener Knoten 2 Controller	Ersatz-Knoten2-Systemmodule
AFF A800	AFF A90 oder AFF A70
AFF A220 als ASA konfiguriert	Controller-Modul ASA A150
AFF A220 AFF A200 AFF C 190	Controller-Modul AFF A150
FAS2620 FAS2720	FAS2820 Controller-Modul
AFF A700 – als ASA konfiguriert	ASA A900-Controller und NVRAM-Module
AFF A700	AFF A900-Controller und NVRAM-Module
FAS9000	FAS9500 Controller- und NVRAM-Module

Schritte

1. Wenn Sie NetApp Storage Encryption (NSE) Laufwerke installiert haben, führen Sie die folgenden Schritte aus.

   Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

   a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

   FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

   b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

2. Starten Sie den Knoten im Startmenü:

   ```
   boot_ontap menu
   ```

3. Weisen Sie die alten Node2-Festplatten dem Ersatznode2 zu, indem Sie „22/7“ eingeben und die versteckte Option auswählen `boot_after_controller_replacement` Wenn der Node im Boot-Menü angehalten wird.

   Nach einer kurzen Verzögerung werden Sie aufgefordert, den Namen des Node einzugeben, der ersetzt wird. Wenn gemeinsam genutzte Festplatten vorhanden sind (auch Advanced Disk Partitioning (ADP) oder partitionierte Festplatten), werden Sie aufgefordert, den Node-Namen des HA-Partners einzugeben.

   Diese Eingabeaufforderungen sind möglicherweise in den Konsolenmeldungen verborgen. Wenn Sie keinen Node-Namen eingeben oder einen falschen Namen eingeben, werden Sie aufgefordert, den Namen erneut einzugeben.

   > Wenn `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` Und oder `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` Fehler auftreten, führen Sie die folgenden Schritte aus:
   >
   > a. Halten Sie den Node an der LOADER-Eingabeaufforderung an.
   > b. Prüfen und setzen Sie die Storage Encryption Boot-Optionen zurück, die in erwähnt sind Schritt 1.
   > c. Starten Sie an der LOADER-Eingabeaufforderung:
   >
   >    ```
   >    boot_ontap
   >    ```

   Das folgende Beispiel kann als Referenz verwendet werden:

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

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)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

Die im vorhergehenden Beispiel gezeigten System-IDs sind Beispiel-IDs. Die tatsächlichen System-IDs der Nodes, die Sie aktualisieren, unterscheiden sich.

Zwischen der Eingabe von Node-Namen an der Eingabeaufforderung und der Eingabeaufforderung für die Anmeldung wird der Node mehrmals neu gebootet, um die Umgebungsvariablen wiederherzustellen, die Firmware auf den im System verwendeten Karten zu aktualisieren und für andere ONTAP Updates zu sorgen.

Überprüfen Sie die Installation node2

Sie müssen die Installation von node2 mit den Ersatz-Systemmodulen überprüfen. Da keine Änderung an physischen Ports erfolgt, sind Sie nicht erforderlich, die physischen Ports von der alten node2 auf den Ersatz-Knoten2 zuzuordnen.

Über diese Aufgabe

Nachdem Sie node1 mit dem Ersatz-Systemmodul gestartet haben, überprüfen Sie, ob es richtig installiert ist. Sie müssen warten, bis Node2 dem Quorum Beitritt und dann den Vorgang zum Austausch des Controllers fortsetzen.

An diesem Punkt des Verfahrens wird die Operation angehalten, während node2 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node2 dem Quorum beigetreten ist:

   ```
   cluster show -node node2 -fields health
   ```

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node2 Teil desselben Clusters wie node1 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Wechseln in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

4. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand wie zuvor in node2 befindet, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

   ```
   system controller replace show
   ```

   ```
   system controller replace show-details
   ```

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Controller-Ersatzvorgang hält für Eingriffe mit der folgenden Meldung an:

```
Cluster::*> system controller replace show
Node          Status                       Error-Action
------------  ---------------------------
-----------------------------------
Node2         Paused-for-intervention      Follow the instructions given
in
                                           Step Details
Node1         None

Step Details:
-----------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:


1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.
2 entries were displayed.
```

In diesem Verfahren wurde der Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node2_ umbenannt.

7. Wenn sich der Controller-Austausch im Status „Pause“ befindet, fahren Sie mit fort Stellen Sie die Netzwerkkonfiguration auf node2 wieder her.

Stellen Sie die Netzwerkkonfiguration auf node2 wieder her

Nachdem Sie bestätigt haben, dass node2 sich im Quorum befindet und mit node1 kommunizieren kann, überprüfen Sie, dass node1 VLANs, Interface Groups und Broadcast-Domains auf node2 gesehen werden. Überprüfen Sie außerdem, ob alle node2-Netzwerk-Ports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Zum Verknüpfen mit dem Inhalt *Network Management*.

Schritte

1. Listen Sie alle physischen Ports auf Upgrade-Knoten2 auf:

```
network port show -node node2
```

Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. In dieser Ausgabe sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um die Entscheidung zu erleichtern, welche Ports als Ports für Schnittstellengruppen, als VLAN-Basis-Ports oder als eigenständige physische Ports zum Hosten von LIFs verwendet werden sollten.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Netzwerk-Port-Erreichbarkeit aller Ports auf node2 auflisten:

```
network port reachability show -node node2
```

Die Ausgabe sollte dem folgenden Beispiel ähnlich sein. Die Port- und Broadcast-Namen variieren.

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability               Reachability
Status
--------- -------- ------------------------------------
---------------------
Node1
          a0a      Default:Default                     ok
          a0a-822  Default:822                         ok
          a0a-823  Default:823                         ok
          e0M      Default:Mgmt                        ok
          e1a      Cluster:Cluster                     ok
          e1b      -                                   no-reachability
          e2a      -                                   no-reachability
          e2b      -                                   no-reachability
          e3a      -                                   no-reachability
          e3b      -                                   no-reachability
          e7a      Cluster:Cluster                     ok
          e7b      -                                   no-reachability
          e9a      Default:Default                     ok
          e9a-822  Default:822                         ok
          e9a-823  Default:823                         ok
          e9b      Default:Default                     ok
          e9b-822  Default:822                         ok
          e9b-823  Default:823                         ok
          e9c      Default:Default                     ok
          e9d      Default:Default                     ok
20 entries were displayed.
```

Im vorherigen Beispiel wurde node2 nach dem Austausch des Controllers gestartet und dem Quorum

beigetreten. Es verfügt über mehrere Ports, die keine Erreichbarkeit haben und eine Überprüfung der Erreichbarkeit ausstehen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node2 mit einem anderen Status als der Erreichbarkeit `ok` Mit dem folgenden Befehl in der folgenden Reihenfolge:

   `network port reachability repair -node node_name -port port_name`

   a. Physische Ports
   b. VLAN-Ports

   Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

   ```
   Cluster ::> reachability repair -node node2 -port e9d
   ```

   ```
   Warning: Repairing port "node2:e9d" may cause it to move into a
   different broadcast domain, which can cause LIFs to be re-homed away
   from the port. Are you sure you want to continue? {y|n}:
   ```

   Eine Warnmeldung, wie im vorhergehenden Beispiel dargestellt, wird für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Erreichbarkeit der Broadcast-Domäne unterscheiden können, in der sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

   Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

   `network port reachability show`

   Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Überprüfen der Port-Erreichbarkeit:

   `network port reachability show`

   Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn ein Port einen anderen Status als diese beiden meldet, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

6. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

   `network port show`

7. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

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

8. Stellen Sie die LIF-Home-Ports wieder her und geben Sie ggf. den Vserver und die LIF-Home-Ports an, die Sie mit folgenden Schritten wiederherstellen müssen:
   a. Führen Sie alle vertriebenen LIFs auf:

      ```
      displaced-interface show
      ```

   b. LIF-Home-Knoten und Home-Ports wiederherstellen:

      ```
      displaced-interface restore-home-node -node node_name -vserver vserver_name
      -lif-name LIF_name
      ```

9. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

   ```
   network interface show -fields home-port,status-admin
   ```

Wiederherstellen der Key-Manager-Konfiguration auf node2

Wenn Sie mit NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) Volumes auf dem System, das ein Upgrade ausführt, wird die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert. Wenn Sie den Key-Manager nicht neu synchronisieren, wenn Sie die node2-Aggregate mithilfe von ARL vom aktualisierten Node1 zum aktualisierten Node2 verschieben, können Ausfälle auftreten, da node2 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie den folgenden Befehl aus node2:

   ```
   security key-manager onboard sync
   ```

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node2 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

   ```
   ::> security key-manager key query -node node2 -fields restored -key
   -type SVM-KEK
   ```

Beispiel

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node2    svm1      ""           000000000000000002000000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Verschieben Sie Aggregate und NAS-Daten-LIFs zurück auf node2

Nachdem Sie die Netzwerkkonfiguration auf Node2 überprüft und bevor Sie Aggregate von Node1 zu Node2 verschieben, überprüfen Sie, ob die NAS-Daten-LIFs, die zu Node2 gehören, die sich derzeit auf Node1 befinden, von Node1 zu Node2 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN LIFs auf Knoten2 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Nachdem Sie node2 in den Online-Modus versetzt haben, müssen Sie überprüfen, ob sich die LIFs in einem ordnungsgemäßen Zustand und auf den entsprechenden Ports befinden.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt folgende Prüfungen durch:

- Cluster-Zustandsprüfung
- LIF-Statusüberprüfung für Cluster

Nach Durchführung dieser Überprüfungen verlagert das System die nicht-Root-Aggregate und NAS-Daten-LIFs zurück auf node2, das jetzt auf dem Ersatz-Controller ausgeführt wird.

Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

3. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

   Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

4. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

   `cluster controller-replacement network displaced-interface show`

   Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in node2 wieder her:

   `cluster controller-replacement network displaced-interface restore-home-node`

5. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

   `system controller replace resume`

   Das System führt die folgenden Nachprüfungen durch:

   - Cluster-Quorum-Prüfung
   - Cluster-Zustandsprüfung
   - Aggregatrekonstruktion
   - Aggregatstatus-Prüfung
   - Überprüfung des Festplattenstatus
   - LIF-Statusüberprüfung für Cluster
   - Lautstärkerprüfung

Phase 7: Schließen Sie das Upgrade ab

Phase-7-Übersicht

In Phase 7 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

1. "Authentifizierungsmanagement mit KMIP-Servern"

2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

Authentifizierungsmanagement mit KMIP-Servern

Ab ONTAP 9.10.1 können Sie KMIP-Server (Key Management Interoperability Protocol) verwenden, um Authentifizierungsschlüssel zu managen.

Schritte

1. Hinzufügen eines neuen Controllers:

   ```
   security key-manager external enable
   ```

2. Fügen Sie den Schlüsselmanager hinzu:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um die korrekte Einrichtung zu überprüfen, überprüfen Sie, ob das HA-Paar aktiviert ist. Außerdem überprüfen Sie, ob Node 1 und Node 2 auf den Storage zugreifen können und ob keine der Daten-LIFs gehören, die zu anderen Nodes im Cluster gehören. Außerdem überprüfen Sie, ob alle Datenaggregate auf den richtigen Home Nodes vorhanden sind und ob die Volumes für beide Nodes online sind. Wenn einer der neuen Nodes über einen Unified Target Adapter verfügt, müssen Sie alle Port-Konfigurationen wiederherstellen. Darüber hinaus muss die Verwendung des Adapters geändert werden.

Schritte

1. Nach den Tests nach der Prüfung von „node2“ werden das Storage Failover und das Cluster HA-Paar für den node2 Cluster aktiviert. Nach Abschluss des Vorgangs werden beide Nodes als abgeschlossen angezeigt, und das System führt einige Bereinigungsvorgänge aus.
2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   ```
   storage failover show
   ```

Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

```
cluster::> storage failover show
                           Takeover
Node        Partner        Possible      State Description
----------  -----------    ------------  ------------------
node1       node2          true          Connected to node2
node2       node1          true          Connected to node1
```

3. Vergewissern Sie sich, dass node1 und node2 zum gleichen Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

   `cluster show`

4. Vergewissern Sie sich, dass node1 und node2 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

   `storage failover show -fields local-missing-disks,partner-missing-disks`

5. Vergewissern Sie sich, dass weder node1 noch node2 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

   `network interface show`

   Wenn weder Node1 noch node2 Daten-LIFs Eigentümer anderer Nodes im Cluster sind, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

   `network interface revert`

6. Vergewissern Sie sich, dass die Aggregate den jeweiligen Home-Nodes gehören.

   `storage aggregate show -owner-name node1`

   `storage aggregate show -owner-name node2`

7. Legen Sie fest, ob Volumes offline sind:

   `volume show -node node1 -state offline`

   `volume show -node node2 -state offline`

8. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie im Abschnitt erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor", Und Online-Laufwerk eines der Offline-Volumes, nach Bedarf, durch Verwendung des folgenden Befehls, einmal für jedes Volume:

   `volume online -vserver vserver_name -volume volume_name`

9. Installieren Sie neue Lizenzen für die neuen Nodes mithilfe des folgenden Befehls für jeden Node:

   `system license add -license-code license_code,license_code,license_code…`

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für

Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

10. Entfernen Sie alle alten Lizenzen mithilfe eines der folgenden Befehle von den ursprünglichen Nodes:

    `system license clean-up -unused -expired`

    `system license delete -serial-number` *`node_serial_number`* `-package` *`licensable_package`*

    - Alle abgelaufenen Lizenzen löschen:

      `system license clean-up -expired`

    - Alle nicht verwendeten Lizenzen löschen:

      `system license clean-up -unused`

    - Löschen Sie eine bestimmte Lizenz von einem Cluster mit den folgenden Befehlen auf den Nodes:

      `system license delete -serial-number` *`node1_serial_number`* `-package *`
      `system license delete -serial-number` *`node2_serial_number`* `-package *`

    Die folgende Ausgabe wird angezeigt:

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    Eingabe `y` Um alle Pakete zu entfernen.

11. Überprüfen Sie, ob die Lizenzen korrekt installiert sind, indem Sie den folgenden Befehl verwenden und seine Ausgabe überprüfen:

    `system license show`

    Sie können die Ausgabe mit der Ausgabe vergleichen, die Sie im erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt.

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie den festgelegt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel: In *Boot node2 mit den Ersatz-Systemmodulen* "Schritt 1"), Sie müssen die Einstellung der Variable aufheben:

    `set diag; systemshell -node` *`node_name`* `-command sudo kenv -u -p kmip.init.maxwait`

13. Konfigurieren Sie die SPs mit dem folgenden Befehl auf beiden Knoten:

    `system service-processor network modify -node` *`node_name`*

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen *ONTAP 9: Manual Page Reference* für detaillierte Informationen zum System `service-processor`

`network modify` Befehl.

14. Informationen zum Einrichten eines Clusters ohne Switches auf den neuen Nodes finden Sie unter "Quellen" Um eine Verbindung zur NetApp Support Site_ zu erhalten, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node1 und node2 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   `security key-manager external restore -node new_controller_name`

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Onboard Key Manager

Konfigurieren Sie NVE oder NAE mit dem Onboard Key Manager.

Schritte

1. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager onboard sync
   ```

Externes Verschlüsselungsmanagement

Konfigurieren Sie NVE oder NAE mit externem Verschlüsselungsmanagement.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore
   ```

   Für diesen Befehl ist die OKM-Passphrase erforderlich

Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder EKM-Server nicht erreicht werden konnten. Stellen Sie diese Volumes mithilfe der wieder online `volume online` Befehl.

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder externe Schlüsselverwaltungsserver nicht erreicht werden konnten. Stellen Sie diese Volumes mit der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

```
snapmirror resume -destination-vserver vserver_name
```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "Überblick über das ARL Upgrade". Informationen über mögliche Ausfälle werden in der Phase des Verfahrens aufgelistet.

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   ```
   storage aggregate relocation show
   ```

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 verwendet wurden, sind nach Abschluss des Upgrades Eigentum von node2

Beim Ende des Upgrade-Verfahrens sollte die Knoten1 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node node1 verwendet wurden. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Falls Aggregate nicht korrekt verschoben werden können, d. h. Node 2 statt Knoten 1, wird unter den folgenden Umständen als Home Node verwendet:

- In Phase 3, wenn Aggregate von node2 auf node1 verschoben werden.

  Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann bleibt das Aggregat auf node2 zurück.

- Nach Phase 4, wenn node2 durch die neuen Systemmodule ersetzt wird.

  Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node1 als Home-Node statt node2 online.

Nach Phase 6 können Sie das falsche Eigentümerproblem beheben, nachdem Sie das Storage-Failover aktiviert haben, indem Sie die folgenden Schritte durchführen:

Schritte

1. Erhalten Sie eine Liste von Aggregaten:

   `storage aggregate show -nodes node2 -is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 mit der Ausgabe, die Sie für Knoten 1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links hinter Knoten2:

   `storage aggregate relocation start -node node2 -aggr aggr_node_1 -destination node1`

   Verwenden Sie während dieser Verschiebung keinen Parameter für -ndo-Controller-Upgrade.

4. Vergewissern Sie sich, dass node1 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht den Knoten1 als Hausbesitzer haben, können mit dem gleichen Relocation-Befehl in Schritt 3 auf node1 umgezogen werden.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, Panik oder ein aus- und Wiedereinschalten durchlaufen.

Die Lösung dieser Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikzugänge oder Energiezyklen während der Vorprüfphase

Node1 oder node2 stürzt vor der Pre-Check-Phase ab, während das HA-Paar noch aktiviert ist

Wenn node1 oder node2 vor der Pre-Check-Phase abstürzt, wurden noch keine Aggregate verschoben und die HA-Paar-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzugänge oder Energiezyklen während der ersten Ressourcenfreigabephase

Node1 stürzt während der ersten Resource-Release-Phase ab, während das HA-Paar noch aktiviert ist

Einige oder alle Aggregate wurden von node1 in node2 verschoben und das HA-Paar ist noch aktiviert. Node2 übernimmt das Root-Volume von node1 und alle nicht-Root-Aggregate, die nicht verschoben wurden.

Über diese Aufgabe

Eigentum an Aggregaten, die verschoben wurden, sehen genauso aus wie das Eigentum von nicht-Root-Aggregaten, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat.

Wenn node1 in den eintritt `waiting for giveback` Status, node2 gibt alle node1 nicht-Root-Aggregate zurück.

Schritte

1. Nachdem node1 gestartet wurde, sind alle nicht-Root-Aggregate von node1 zurück in node1 verschoben. Sie müssen eine manuelle Aggregatverschiebung der Aggregate von node1 nach node2 durchführen: `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während der ersten Ressourcen-Release-Phase ab, während das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 schlägt während der ersten Phase der Ressourcenfreigabe fehl, während das HA-Paar noch aktiviert ist

Node1 hat einige oder alle seine Aggregate in node2 verschoben. Das HA-Paar ist aktiviert.

Über diese Aufgabe

Node1 übernimmt alle node2 Aggregate sowie jedes seiner eigenen Aggregate, die auf node2 verschoben wurden. Beim Booten von node2 wird die Aggregatverschiebung automatisch abgeschlossen.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während der ersten Resource-Release-Phase ab und nachdem HA-Paar deaktiviert ist

Node1 übernimmt nicht.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Setzen Sie den mit dem Rest des Upgrade-Vorgangs für das Node-Paar fort.

Startet während der ersten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node2 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

Node1 übernimmt nicht nach einem Absturz nach node2, da das HA-Paar bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der ersten Ressourcen-Wiederholen-Phase

Knoten 2 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Node2 hat einige oder alle seine Aggregate von node1 in node1 verschoben. Node1 liefert Daten von Aggregaten, die verschoben wurden. Das HA-Paar ist deaktiviert und somit gibt es keine Übernahme.

Über diese Aufgabe

Es gibt einen Client-Ausfall für Aggregate, die nicht verschoben wurden. Beim Booten von node2 werden die Aggregate von node1 auf node1 verschoben.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Knoten 1 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Wenn node1 abstürzt, während node2 Aggregate zu node1 verschoben wird, wird die Aufgabe nach dem Booten von node1 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, aber Aggregate, die bereits in Knoten 1 verlagert wurden, begegnen ein Client-Ausfall, während node1 gebootet wird.

Schritte

1. Knoten 1 aufbring.
2. Führen Sie das Controller-Upgrade fort.

Neustarts, Panikspiele oder Energiezyklen während der Nachprüfphase

Node1 oder node2 stürzt während der Nachprüfphase ab

Das HA-Paar ist deaktiviert, damit dies keine Übernahme ist. Es gibt einen Client-Ausfall für Aggregate, die zum neu gebooteten Node gehören.

Schritte

1. Bringen Sie den Node hoch.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der zweiten Ressourcenfreigabephase

Node1 stürzt während der zweiten Resource-Release-Phase ab

Wenn node1 abstürzt, während node2 Aggregate verschoben wird, wird die Aufgabe nach dem Booten von node1 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, aber Aggregate, die bereits in Node1 verlagert wurden und Node1 eigene Aggregate, begegnen Client-Ausfällen, während node1 gebootet wird.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Node2 stürzt während der zweiten Resource-Release-Phase ab

Wenn node2 während der Aggregatverschiebung abstürzt, wird node2 nicht übernommen.

Über diese Aufgabe

Node1 dient weiterhin den Aggregaten, die verschoben wurden, aber die Aggregate von node2 stoßen auf Client-Ausfälle.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Startet während der zweiten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node1 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node1 abstürzt, wird die Übernahme nicht ausgeführt, da das HA-Paar bereits deaktiviert ist.

Über diese Aufgabe

Es gibt einen Client-Ausfall für alle Aggregate, bis node1 neu gebootet wird.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node2 abstürzt, wird die Übernahme nicht durchgeführt. Node1 dient Daten aus den Aggregaten.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits so lange verschoben wurden bis nach einem Neustart von node2.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------  --------- -----------------
node1    node2     false     Unknown
node2    node1     false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder Panic:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------  --------- -----------------
node1    node2     -         Unknown
node2    node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports lautet `down`.

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.

Inhalt	Beschreibung
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.

Inhalt	Beschreibung
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe", Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.

Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen

Überblick

Dieses Verfahren beschreibt das Upgrade der Controller-Hardware mithilfe von Aggregate Relocation (ARL) für die folgenden Systemkonfigurationen:

Methode	ONTAP-Version	Unterstützte Systeme
Wird Verwendet `system controller replace` Befehle	9.8 oder höher	"Link zur unterstützten Systemmatrix"

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Außerdem migrieren Sie Daten-logische Schnittstellen (LIFs) und weisen Sie die Netzwerk-Ports auf dem neuen Controller den Schnittstellengruppen zu, während Sie fortfahren.

In diesen Informationen verwendete Terminologie

In dieser Information werden die ursprünglichen Knoten „node1“ und „node2“ genannt und die neuen Knoten „node3“ und „node4“ genannt. Während des beschriebenen Verfahrens wird node1 durch node3 ersetzt und node2 durch node4 ersetzt. Die Begriffe "node1", "node2", "node3" und "node4" werden nur verwendet, um

zwischen den ursprünglichen und den neuen Knoten zu unterscheiden. Wenn Sie das Verfahren befolgen, müssen Sie die richtigen Namen Ihrer ursprünglichen und neuen Knoten ersetzen. In der Realität ändern sich jedoch die Namen der Nodes nicht: node3 hat den Namen node1 und node4 hat nach dem Upgrade der Controller-Hardware den Namen node2.

Während dieser Informationen bezieht sich der Begriff „Systeme mit FlexArray-Virtualisierungssoftware“ auf Systeme, die zu diesen neuen Plattformen gehören. Der Begriff „V-Series System“ bezieht sich auf getrennte Hardwaresysteme, die an Storage Arrays angeschlossen werden können.

Wichtige Informationen:

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie müssen auch lesen und verstehen, die "Richtlinien für das Controller-Upgrade mit ARL" Und das "Überblick über das ARL Upgrade" Abschnitte vor Beginn der Aktualisierung.
- Bei dieser Vorgehensweise wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn Sie zuvor die Ersatz-Controller-Hardware verwendet haben, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP im 7-Mode ausgeführt wurde.
- Sie können mithilfe von ARL ein unterbrechungsfreies, vereinfachtes Controller-Upgrade auf einen neuen Controller mit einer neueren ONTAP Version durchführen als die auf dem Cluster ausgeführte Version. Die ONTAP Versionskombinationen für alte und neue Controller werden durch das NDU Trittfrequenzmodell der ONTAP Software bestimmt. Wenn beispielsweise ein Controller ausgeführt ONTAP wird und 9.8 zwar die letzte unterstützte Version für diesen Controller ist, können Sie ein Upgrade auf einen neuen Controller mit einer ONTAP-Version später als ONTAP 9.8 durchführen.

  Dieses Upgrade-Verfahren gilt in erster Linie für Upgrade-Szenarien, in denen das ersetzte Controller-Modell auch spätere ONTAP-Versionen nicht unterstützt, und der neue Controller ältere ONTAP Versionen nicht unterstützt.

- Mit diesem Verfahren können Sie die Controller-Hardware in Clustern mit mehr als zwei Nodes aktualisieren. Sie müssen jedoch für jedes Hochverfügbarkeitspaar (HA) im Cluster separat vorgehen.
- Dieses Verfahren gilt für FAS Systeme, V-Series Systeme, AFF Systeme und Systeme mit FlexArray Virtualisierungssoftware. FAS Systeme, die nach ONTAP 9.5 freigegeben wurden, können an Speicher-Arrays angebunden werden, wenn die erforderliche Lizenz installiert ist. Weitere Informationen zu den Modellen Storage Array und V-Series finden Sie unter "Quellen" Zu verlinken auf „Hardware Universe_“ und „V-Series Supportmatrix“.
- Dieses Verfahren gilt für Systeme mit einer NetApp MetroCluster Konfiguration mit 4 Nodes oder höher. Da sich die MetroCluster-Konfigurationsstandorte an zwei physisch unterschiedlichen Standorten befinden können, muss das automatisierte Controller-Upgrade für ein HA-Paar einzeln an jedem MetroCluster Standort durchgeführt werden.
- Bei Systemen außerhalb von MetroCluster, z. B. HA-Cluster, ist das ARL-Upgrade die einzige unterstützte Prozedur.
- Wenn Sie ein Upgrade von einem AFF A320 System durchführen, können Sie das Upgrade der Controller-Hardware durch Volume-Verschiebung durchführen oder den technischen Support kontaktieren. Siehe "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Automatisierung des Controller-Upgrades

Während eines Controller-Upgrades wird der Controller durch einen anderen Controller ersetzt, auf dem eine neuere oder leistungsstärkere Plattform läuft. In früheren Versionen

dieses Inhalts enthielten Anweisungen für einen unterbrechungsfreien Controller-Update, der vollständig manuell ausgeführt wurde. Dieser Inhalt enthält die Schritte für das neue automatisierte Verfahren, bei dem automatische Überprüfungen der Netzwerkanschlüsse eingesetzt werden, um das Upgrade-Erlebnis für die Controller weiter zu vereinfachen.

Der manuelle Prozess war langwierig und komplex, aber in diesem vereinfachten Verfahren können Sie ein Controller-Update mithilfe von Aggregatverschiebung implementieren, sodass effizientere, unterbrechungsfreie Upgrades für HA-Paare möglich sind. Vor allem in Bezug auf Validierung, Sammlung von Informationen und Nachprüfungen sind deutlich weniger manuelle Schritte erforderlich.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

Dieser Inhalt beschreibt, wie Sie die Storage Controller in einem HA-Paar mit neuen Controllern upgraden, ohne die vorhandenen Daten und Festplatten zu verwenden. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Sie können diese Inhalte unter folgenden Umständen verwenden:

- Sie verwenden ONTAP 9.8 oder höher.
- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind in der Verwaltung von ONTAP erfahren und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.
- Wenn Sie eine MetroCluster Konfiguration aktualisieren, handelt es sich um eine FC-Konfiguration mit vier oder mehr Nodes und auf allen Nodes wird ONTAP 9.8 oder höher ausgeführt.

  Informationen zum Aktualisieren von MetroCluster IP-Konfigurationen finden Sie unter "Quellen" Zum Verlinken auf den Inhalt *MetroCluster Upgrade und Expansion*.

Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

die folgende Tabelle zeigt die unterstützte Modellmatrix für das Controller-Upgrade.

Alter Controller	Ersatz-Controller
FAS8020[3], FAS8040[3], FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
FAS8060[4], FAS8080[4]	FAS9500
AFF8020[3], AFF8040[3], AFF8060, AFF8080	AFF A300, AFF A400, AFF A700, AFF A800[1]
AFF8060[4], AFF8080[4]	AFF A900
FAS8200	FAS8300[2], FAS8700, FAS9000, FAS9500
FAS8300, FAS8700, FAS9000	FAS9500
AFF A300	AFF A400[2], AFF A700, AFF A800[1], AFF A900
AFF A320[4]	AFF A400
AFF A400, AFF A700	AFF A900

Wenn die Kombination aus dem Controller-Upgrade-Modell nicht in der oben stehenden Tabelle aufgeführt ist, wenden Sie sich an den technischen Support.

[1]die zusätzlichen Schritte, die für AFF A800 Systeme erforderlich sind, finden Sie im Schritt mit der Referenz A800 in Abschnitt "UTA/UTA2-Ports in node3, Schritt 23, prüfen und konfigurieren", Oder "UTA/UTA2-Ports in node4, Schritt 23, prüfen und konfigurieren".

[2]Wenn Sie in einer 2-Node-Cluster-Konfiguration ein Upgrade von einer AFF A300 auf eine AFF A400 oder ein FAS8200 auf ein FAS8300 System durchführen, müssen Sie für das Controller-Upgrade temporäre Cluster-Ports auswählen. Die AFF A400- und FAS8300-Systeme sind in zwei Konfigurationen erhältlich – als Ethernet-Bundle, bei dem die Ports der Mezzanine-Karte Ethernet-Typ und als FC-Bundle enthalten sind. Dort befinden sich die Mezzanine-Ports vom FC-Typ.

- Bei einer AFF A400 oder einer FAS8300 mit Ethernet-Konfiguration können Sie jeden der beiden Mezzanine-Ports als temporäre Cluster-Ports verwenden.
- Bei einer AFF A400 oder einem FAS8300 mit FC-Typ-Konfiguration müssen Sie eine 10-GbE-Netzwerkschnittstellenkarte mit vier Ports (Teilenummer X1147A) hinzufügen, um temporäre Cluster Ports bereitstellen zu können.
- Nach Abschluss eines Controller-Upgrades mithilfe von temporären Cluster-Ports können Sie Cluster-LIFs unterbrechungsfrei zu e3a und e3b migrieren, 100-GbE-Ports auf einem AFF A400 System sowie e0c und e0d, 100-GbE-Ports auf einem FAS8300 System.

[3]für FAS8020, FAS8040, AFF8020 und AFF8040 System-Upgrades zu den in der Tabelle oben aufgeführten Zielaustausch-Controllern müssen die Ersatz-Controller dieselbe ONTAP-Version wie der alte Controller ausführen. Hinweis: FAS8020, FAS8040, AFF8020 und AFF8040 Systeme unterstützen ONTAP Versionen nicht später als ONTAP 9.8.

[4]die folgende Tabelle zeigt die minimal- und später unterstützten ONTAP-Versionen für diese Controller-Upgrade-Kombinationen.

Alter Controller		**Ersatz-Controller**	
System	ONTAP-Version	System	ONTAP-Version
AFF A320	9.9.1 oder höher	AFF A400	9.9.1 oder höher
AFF8060	9.8P13 oder höher Patches	AFF A900	9.10.1 bis 9.12.1
AFF8080	9.8P10 oder höher Patches	AFF A900	9.10.1 bis 9.12.1
FAS8060	9.8P13 oder höher Patches	FAS9500	9.10.1P3 bis 9.12.1
FAS8080	Patches ab 9.8P12	FAS9500	9.10.1P3 bis 9.12.1

Für die in der vorherigen Tabelle aufgeführten Upgrade-Kombinationen:

- Es ist nicht erforderlich, dieselbe ONTAP-Version auf den vorhandenen Controllern und Ersatz-Controllern zu verwenden. Das Upgrade der ONTAP Software wird bei dem Controller-Upgrade durchgeführt.
- Wenn Sie ein Upgrade durchführen, müssen Sie einen Ersatz-Controller mit einer unterstützten ONTAP-Version und Patch-Ebene installieren.
- Nach dem Starten des Vorgangs und dem Upgrade des ersten Node ist es nicht möglich, das Controller-Upgrade abzubrechen oder wieder auszuführen.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu ONTAP 9 zugreifen können.

Die erforderlichen Tools und Dokumentationen

Sie müssen über spezielle Tools verfügen, um die neue Hardware zu installieren, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren.

Für die Durchführung des Upgrades benötigen Sie die folgenden Tools:

- Erdungsband
- #2 Kreuzschlitzschraubendreher

Wechseln Sie zum "Quellen" Abschnitt für den Zugriff auf die Liste der für dieses Upgrade erforderlichen Referenzdokumente und Referenzsites

Richtlinien für das Controller-Upgrade mit ARL

Um zu verstehen, ob Sie mithilfe von ARL ein Upgrade für ein Controller-Paar mit ONTAP 9.8 oder höher durchführen können, hängt von der Plattform und der Konfiguration der ursprünglichen Controller sowie von Ersatz-Controllern ab.

Unterstützte Upgrades für ARL

Wenn Sie ein Node-Paar mit diesem ARL-Verfahren für ONTAP 9.8 oder höher aktualisieren, müssen Sie sicherstellen, dass ARL auf den Original- und Austausch-Controllern ausgeführt werden kann.

Sie müssen die Größe aller definierten Aggregate und die Anzahl der Festplatten überprüfen, die vom ursprünglichen System unterstützt werden. Dann müssen Sie die Aggregatgröße und Anzahl der unterstützten Festplatten mit der Aggregatgröße und der Anzahl der vom neuen System unterstützten Festplatten vergleichen. Siehe "Quellen" Link zum *Hardware Universe*, wo diese Information verfügbar ist. Die Aggregatgröße und die Anzahl der vom neuen System unterstützten Festplatten müssen gleich oder größer sein als die Aggregatgröße und Anzahl der vom ursprünglichen System unterstützten Festplatten.

Sie müssen in den Cluster-Mischregeln validieren, ob neue Nodes zusammen mit den vorhandenen Nodes Teil des Clusters werden können, wenn der ursprüngliche Controller ersetzt wird. Weitere Informationen zu Regeln für die Kombination von Clustern finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

> Informationen zum Upgrade eines Systems, das interne Laufwerke unterstützt (z. B. eine FAS2700 oder AFF A250), aber KEINE internen Laufwerke enthält, finden Sie unter "Quellen" Und verwenden Sie das Verfahren in der *Aggregate Relocation, um den für Ihre Version von ONTAP korrekten Controller-Hardware*-Inhalt manuell zu aktualisieren.

Wenn Sie ein System mit mehr als zwei Cluster-Ports pro Node, wie z. B. einem FAS8080 oder AFF8080 System, haben Sie vor dem Upgrade die Cluster-LIFs zu zwei Cluster-Ports pro Node zu migrieren und neu zu starten. Wenn Sie das Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node durchführen, fehlen möglicherweise nach dem Upgrade Cluster-LIFs auf dem neuen Controller.

Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise und SnapLock Compliance Volumes konfiguriert sind.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren.

Upgrades werden für ARL nicht unterstützt

Sie können die folgenden Aktualisierungen nicht ausführen:

- Zum Austausch von Controllern, die die mit den ursprünglichen Controllern verbundenen Platten-Shelfs nicht unterstützen

  Siehe "Quellen" Um Informationen zur Hardware Universe Festplattenunterstützung zu erhalten.

- Um Controller der Einstiegsklasse mit internen Laufwerken zu erhalten, beispielsweise eine FAS 2500.

  Informationen zum Upgrade von Controllern der Einstiegsklasse mit internen Laufwerken finden Sie unter "Quellen" Link zu *Upgrade durch Verschiebung von Volumes oder Storage* und Vorgang *Upgrade eines Node-Paares, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.

Fehlerbehebung

Falls beim Upgrade der Controller Probleme auftreten, finden Sie weitere Informationen im "Fehlerbehebung" Abschnitt am Ende des Verfahrens für weitere Informationen und mögliche Lösungen.

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Bevor Sie ein Upgrade auf einer Fabric-MetroCluster-Konfiguration starten, müssen Sie den Zustand der MetroCluster-Konfiguration überprüfen, um den korrekten Betrieb zu überprüfen.

Schritte

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

   `metrocluster check run`

   ```
   metrocluster_siteA::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

2. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ergebnisse anzeigen:

   `metrocluster check show`

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
metrocluster_siteA::*> metrocluster check show
Last Checked On: 4/7/2019 21:15:05
Component            Result
---------------      -------
nodes                ok
lifs                 ok
config-replication   ok
aggregates           warning
clusters             ok
connections          not-applicable
volumes              ok
7 entries were displayed.
```

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

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

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

   ```
   system health alert show
   ```

Prüfen Sie auf MetroCluster-Konfigurationsfehler

Sie können das Active IQ Config Advisor Tool auf der NetApp Support-Website verwenden, um häufige Konfigurationsfehler zu überprüfen.

Wenn Sie keine MetroCluster-Konfiguration haben, können Sie diesen Abschnitt überspringen.

Über diese Aufgabe

Active IQ 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.

1. Laden Sie die herunter "Active IQ Config Advisor" Werkzeug.
2. Führen Sie Active IQ Config Advisor aus, überprüfen Sie die Ausgabe und folgen Sie seinen Empfehlungen, um eventuelle Probleme zu beheben.

Überprüfung von UmschalttaFunktionen, Healing und Switchback

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

Siehe "Quellen" Verbinden mit Inhalten für *MetroCluster Management and Disaster Recovery* und Verwenden der genannten Verfahren für ausgehandelte Umschaltung, Heilung und Umschalten.

Überblick über das ARL Upgrade

Bevor Sie die Nodes mit ARL aktualisieren, sollten Sie unbedingt verstehen, wie das Verfahren funktioniert. In diesem Inhalt wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und dann für die ursprünglichen und die neuen Nodes eine Reihe von Schritten ausführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Beschreibung
"Stufe 1: Upgrade vorbereiten"	In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Sie müssen bestimmte Informationen aufzeichnen, wenn Sie Storage-Verschlüsselung mithilfe des OKM managen und Sie die SnapMirror Beziehungen stilllegen möchten. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate. • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate.

Stufe	Beschreibung
"Stufe 2: Knoten1 verschieben und ausmustern"	Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie erfassen Node1-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node1. Sie können sich auch später beim Verfahren auf den Netzboot node3 und node4 vorbereiten. Gesamteigentum am Ende von Phase 2: • Node2 ist der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 3: Installieren und booten Sie node3"	Während Phase 3 installieren und booten Sie node3, überprüfen, ob die Cluster- und Node-Management-Ports von node1 auf node3 online geschaltet sind und überprüfen Sie die Installation node3. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Falls erforderlich, stellen Sie die FC- oder UTA/UTA2-Konfiguration auf node3. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind. Gesamteigentum am Ende von Stufe 3: • Node3 ist der Hausbesitzer und der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 4: Knoten2 verschieben und ausmustern"	Während Phase 4 werden Aggregate und NAS-Daten-LIFs von Knoten 2 auf Knoten 3 verschoben. Sie erfassen auch node2-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node2. Gesamteigentum am Ende von Stufe 4: • Node3 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehörten. • Node2 ist der Hausbesitzer von node2 Aggregaten. • Node3 ist der aktuelle Besitzer von node2 Aggregaten.

Stufe	Beschreibung
"Phase 5: installieren und booten sie node4"	In Phase 5 installieren und booten Sie node4, überprüfen, ob die Cluster- und Node-Management-Ports von node2 auf node4 online geschaltet sind, und überprüfen Sie die Installation von node4. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Falls erforderlich, stellen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 ein. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind. Gesamteigentum am Ende von Stufe 5: • Node3 ist der Hausbesitzer und aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Node4 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Phase 6: Schließen Sie das Upgrade ab"	In Phase 6 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden. Und wenn die neuen Nodes verschlüsselt sind, konfigurieren und einrichten Sie Storage Encryption oder NVE. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Außerdem zeichnen Sie bestimmte Informationen auf, wenn Sie Storage-Verschlüsselung mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten.

Schritte

1. "Bereiten Sie die Knoten für ein Upgrade vor"
2. "Management der Storage-Verschlüsselung mit dem Onboard Key Manager"

Bereiten Sie die Knoten für ein Upgrade vor

Der Prozess des Controller-Austauschs beginnt mit einer Reihe von Vorabprüfungen. Sie sammeln auch Informationen über die ursprünglichen Nodes, die Sie später verwenden können. Falls erforderlich, ermitteln Sie den Typ der verwendeten Self-Encrypting Drives.

Schritte

1. Starten Sie den Controller-Ersatzprozess, indem Sie den folgenden Befehl in die ONTAP-Befehlszeile eingeben:

   ```
   system controller replace start -nodes node_names
   ```

- Ab ONTAP 9.10.1 ist das auf NSO basierende automatisierte Upgrade-Verfahren (Automated Negotiated Switchover) Standard für eine MetroCluster FC-Konfiguration mit vier Nodes. Wenn Sie eine MetroCluster-FC-Konfiguration mit vier Nodes aktualisieren, treten Sie in das auf `system controller replace start` Befehl, Sie müssen das NSO-basierte Verfahren, das gestartet wird, durch Festlegen des verhindern `-nso` Parameter an `false`:

  `system controller replace start -nodes node_names -nso false`

- Der `system controller replace start` Befehl kann nur auf der erweiterten Berechtigungsebene ausgeführt werden:

  `set -privilege advanced`

Sie sehen die folgende Ausgabe:

```
Warning:
1. Current ONTAP version is 9.x
Before starting controller replacement operation, ensure that the new
controllers are running the version 9.x

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

Do you want to continue? {y|n}: y
```

2. Drücken Sie `y`, Sie sehen die folgende Ausgabe:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

Das System führt die folgenden Vorabprüfungen durch. Notieren Sie die Ausgabe jeder Vorabprüfung zur Verwendung im weiteren Verlauf des Verfahrens:

Pre-Check	Beschreibung
Cluster-Integritätsprüfung	Überprüft alle Nodes im Cluster, um sicherzustellen, dass sie sich in einem ordnungsgemäßen Zustand befinden.
MCC Cluster Check	Überprüft, ob es sich bei dem System um eine MetroCluster-Konfiguration handelt. Der Vorgang erkennt automatisch, ob es sich um eine MetroCluster Konfiguration handelt oder nicht, und führt die spezifischen Vorabprüfungen und Verifizierungsüberprüfungen durch. Es wird nur eine MetroCluster FC-Konfiguration mit 4 Nodes unterstützt. Bei 2-Node-MetroCluster-Konfiguration und 4-Node-MetroCluster IP-Konfiguration schlägt die Prüfung fehl. Wenn die MetroCluster-Konfiguration im Umschaltzustand ist, schlägt die Prüfung fehl.
Statusprüfung Der Aggregatverschiebung	Überprüft, ob eine Aggregatverschiebung bereits erfolgt. Wenn eine weitere Aggregatverschiebung erfolgt, schlägt die Prüfung fehl.
Modellname Prüfen	Überprüft, ob die Controller-Modelle bei diesem Verfahren unterstützt werden. Wenn die Modelle nicht unterstützt werden, schlägt die Aufgabe fehl.
Cluster-Quorum-Prüfung	Überprüft, ob die zu ersetzenden Nodes sich in Quorum befinden. Wenn sich die Knoten nicht im Quorum befinden, schlägt die Aufgabe fehl.
Überprüfung Der Bildversion	Überprüft, ob die zu ersetzenden Nodes dieselbe Version von ONTAP ausführen. Wenn sich die ONTAP-Image-Versionen unterscheiden, schlägt die Aufgabe fehl. Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version von ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation als Netzboot einsetzen. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.
HA-Statusüberprüfung	Überprüft, ob beide Nodes, die ersetzt werden, in einer HA-Paar-Konfiguration mit Hochverfügbarkeit vorhanden sind. Wenn das Speicher-Failover für die Controller nicht aktiviert ist, schlägt die Aufgabe fehl.
Aggregatstatus-Prüfung	Wenn die Nodes ersetzt werden, eigene Aggregate, für die sie nicht der Home-Inhaber sind, schlägt die Aufgabe fehl. Die Nodes sollten nicht im Besitz von nicht lokalen Aggregaten sein.
Überprüfung Des Festplattenstatus	Wenn zu ersetzende Knoten keine oder fehlerhafte Festplatten haben, schlägt die Aufgabe fehl. Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.
LIF-Statusüberprüfung von Daten	Überprüft, ob für einen der zu ersetzenden Nodes keine lokalen Daten-LIFs vorhanden sind. Die Nodes sollten keine Daten-LIFs enthalten, für die sie nicht der Home-Inhaber sind. Wenn einer der Nodes nicht-lokale Daten-LIFs enthält, schlägt die Aufgabe fehl.
LIF-Status des Clusters	Überprüft, ob die Cluster-LIFs für beide Nodes aktiv sind. Wenn die Cluster-LIFs ausgefallen sind, schlägt die Aufgabe fehl.

Pre-Check	Beschreibung
ASUP-Statusprüfung	Wenn ASUP Benachrichtigungen nicht konfiguriert sind, schlägt die Aufgabe fehl. Sie müssen AutoSupport aktivieren, bevor Sie mit dem Austausch des Controllers beginnen.
CPU-Auslastungs-Prüfung	Überprüft, ob die CPU-Auslastung bei allen zu ersetzenden Nodes mehr als 50 % beträgt. Wenn die CPU-Nutzung über einen erheblichen Zeitraum mehr als 50 % beträgt, schlägt die Aufgabe fehl.
Aggregatrekonstruktion	Überprüft, ob bei beliebigen Datenaggregaten eine Rekonstruktion durchgeführt wird. Wenn die Aggregatrekonstruktion ausgeführt wird, schlägt die Aufgabe fehl.
Knoten Affinität Job Überprüfung	Überprüft, ob Jobs mit Knotenorientierung ausgeführt werden. Wenn Knotenaffinitätsjobs ausgeführt werden, schlägt die Prüfung fehl.

3. Wenn der Controller-Ersatzvorgang gestartet und die Vorabprüfungen abgeschlossen sind, hält der Vorgang die Aktivierung ein, damit Sie die Ausgabeinformationen, die Sie später bei der Konfiguration von node3 benötigen könnten, sammeln können.

Wenn Sie ein System mit mehr als zwei Cluster-Ports pro Node, wie z. B. einem FAS8080 oder AFF8080 System, haben Sie vor dem Upgrade die Cluster-LIFs zu zwei Cluster-Ports pro Node zu migrieren und neu zu starten. Wenn Sie das Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node durchführen, fehlen möglicherweise nach dem Upgrade Cluster-LIFs auf dem neuen Controller.

4. Führen Sie den folgenden Befehlssatz aus, wie durch das Verfahren zum Austausch des Controllers auf der Systemkonsole gesteuert.

   Führen Sie von dem seriellen Port aus, der mit jedem Node verbunden ist, und speichern Sie die Ausgabe der folgenden Befehle einzeln:

   - `vserver services name-service dns show`
   - `network interface show -curr-node local -role cluster,intercluster,node-mgmt,cluster-mgmt,data`
   - `network port show -node local -type physical`
   - `service-processor show -node local -instance`
   - `network fcp adapter show -node local`
   - `network port ifgrp show -node local`
   - `system node show -instance -node local`
   - `run -node local sysconfig`
   - `storage aggregate show -node local`
   - `volume show -node local`
   - `storage array config show -switch switch_name`
   - `system license show -owner local`

- `storage encryption disk show`
- `security key-manager onboard show-backup`
- `security key-manager external show`
- `security key-manager external show-status`
- `network port reachability show -detail -node local`

> Wenn NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) mit dem Onboard Key Manager (OKM) verwendet wird, halten Sie die Passphrase bereit, um später im Verfahren die Neusynchronisierung des Schlüsselmanagers abzuschließen.

5. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:
   - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
   - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

   > FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
   >
   > SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

   "Weitere Informationen zu unterstützten Self-Encrypting Drives".

Korrigieren Sie die Aggregateigentümer bei Ausfall einer ARL-Vorabprüfung

Wenn die aggregierte Statusprüfung fehlschlägt, müssen Sie Aggregate des Partner-Node an den Node „Home-Owner“ zurückgeben und den Vorabprüfvorgang erneut initiieren.

Schritte

1. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

   `storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *`

2. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Nachdem Sie fertig sind

Sie müssen den Controller-Ersatzprozess neu starten:

`system controller replace start -nodes node_names`

Lizenz

Einige Funktionen erfordern Lizenzen, die als *Packages* ausgegeben werden, die eine oder mehrere Funktionen enthalten. Jeder Node im Cluster muss über seinen eigenen Schlüssel für jede Funktion im Cluster verfügen.

Wenn Sie keine neuen Lizenzschlüssel haben, stehen dem neuen Controller derzeit lizenzierte Funktionen im Cluster zur Verfügung. Durch die Verwendung nicht lizenzierter Funktionen auf dem Controller können Sie jedoch möglicherweise die Einhaltung Ihrer Lizenzvereinbarung verschließen. Sie sollten daher nach Abschluss des Upgrades den neuen Lizenzschlüssel oder die neuen Schlüssel für den neuen Controller installieren.

Siehe "Quellen" Link zur *NetApp-Support-Website*, auf der Sie neue 28-stellige Lizenzschlüssel für ONTAP erhalten können. Die Schlüssel sind im Abschnitt „*My Support*“ unter „*Software licenses*“ verfügbar. Wenn auf der Website nicht die erforderlichen Lizenzschlüssel vorhanden sind, können Sie sich an Ihren NetApp Ansprechpartner wenden.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Management der Storage-Verschlüsselung mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung der Schlüssel verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager`

`onboard show-backup` Befehl.

Stilllegen der SnapMirror Beziehungen (optional)

Bevor Sie mit dem Verfahren fortfahren, müssen Sie bestätigen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   Wenn der Status „Übertragen“ lautet, müssen Sie diese Transfers abbrechen: `snapmirror abort -destination-vserver vserver_name`

   Der Abbruch schlägt fehl, wenn sich die SnapMirror-Beziehung nicht im Zustand „Übertragen“ befindet.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Stufe 2: Knoten1 verschieben und ausmustern

Phase-2-Übersicht

Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie zeichnen auch die erforderlichen node1-Informationen auf, nehmen Node1 außer Betrieb und bereiten den Netzboot node3 und node4 später im Verfahren vor.

Schritte

1. "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2"
2. "Verschiebung ausgefallener oder Vetos von Aggregaten"
3. "Node1 ausmustern"
4. "Vorbereitungen für den Netzboot"

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2

Bevor Sie node1 durch Node3 ersetzen können, müssen Sie die nicht-Root-Aggregate und NAS-Daten-LIFs von node1 auf node2 verschieben, bevor Sie die Ressourcen von node1 schließlich in node3 verschieben.

Bevor Sie beginnen

Der Vorgang sollte bereits angehalten werden, wenn Sie mit der Aufgabe beginnen. Sie müssen den Vorgang

manuell fortsetzen.

Über diese Aufgabe

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. In dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in node3 migriert werden.

> Der Home-Inhaber für die Aggregate und LIFs wird nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Wiederaufnahme der Vorgänge für die Aggregatverschiebung und die LIF-Verschiebung von NAS-Daten:

   `system controller replace resume`

   Alle Aggregate ohne Root-Root-Root-Root-Daten und LIFs werden von node1 auf node2 migriert.

   Der Vorgang angehalten, damit Sie überprüfen können, ob alle node1-Aggregate und LIFs für nicht-SAN-Daten in node2 migriert wurden.

2. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

3. Wenn der Vorgang noch angehalten wird, vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind, damit ihr Status bei node2 lautet:

   `storage aggregate show -node node2 -state online -root false`

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

   ```
   cluster::> storage aggregate show -node node2 state online -root false

   Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
   ---------  -------  ---------  -----  ------ -----  ------
   --------------
   aggr_1     744.9GB  744.8GB    0%     online     5  node2
   raid_dp,normal
   aggr_2     825.0GB  825.0GB    0%     online     1  node2
   raid_dp,normal
   2 entries were displayed.
   ```

   Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

   `storage aggregate online -aggregate aggr_name`

4. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 verwenden und seine Ausgabe überprüfen:

`volume show -node node2 -state offline`

Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

`volume online -vserver vserver_name -volume volume_name`

Der `vserver_name` Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

5. Wenn irgendeine LIFs inaktiv sind, setzen Sie den Administratorstatus der LIFs auf `up` Mit dem folgenden Befehl, so wie es für jedes LIF ist:

`network interface modify -vserver vserver_name -lif LIF_name -home-node nodename -status-admin up`

Verschiebung ausgefallener oder Vetos von Aggregaten

Falls Aggregate nicht verschoben oder ein Vetos ausfällt, müssen sie die Aggregate manuell verschieben oder, falls erforderlich, die Vetos oder Zielprüfungen überschreiben.

Über diese Aufgabe

Der Umzugsvorgang wird aufgrund des Fehlers angehalten.

Schritte

1. Überprüfen Sie die EMS-Protokolle (Event Management System), um festzustellen, warum das Aggregat nicht verschoben oder gegen ein Vetos eingesetzt wurde.
2. Verschiebung ausgefallener oder Vetos von Aggregaten:

`storage aggregate relocation start -node node1 -destination node2 -aggregate -list aggr_name -ndo-controller-upgrade true`

3. Geben Sie bei der entsprechenden Aufforderung ein `y`.
4. Sie können die Verschiebung mit einer der folgenden Methoden erzwingen:

Option	Beschreibung
Veto-Prüfungen werden überschrieben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true`
Zielprüfungen überschreiben	Verwenden Sie den folgenden Befehl: `storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true`

Node1 ausmustern

Um „node1“ außer Betrieb zu nehmen, setzen Sie den automatischen Vorgang fort, um

das HA-Paar mit node2 zu deaktivieren und node1 ordnungsgemäß herunterzufahren. Später im Verfahren entfernen Sie Knoten 1 aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

2. Vergewissern Sie sich, dass node1 angehalten wurde:

   ```
   system controller replace show-details
   ```

Nachdem Sie fertig sind

Sie können Node1 nach Abschluss des Upgrades außer Betrieb nehmen. Siehe "Ausmustern des alten Systems".

Vorbereitungen für den Netzboot

Nachdem Sie später noch Node3 und node4 physisch gerast haben, müssen Sie sie eventuell als Netzboot Netboot eingesetzt werden. Der Begriff „Netzboot“ bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf den Netzboot legen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver, auf den das System zugreifen kann.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Siehe "Quellen" Um eine Verknüpfung zur NetApp Support-Website zu erhalten und die erforderlichen Systemdateien für Ihre Plattform und die richtige Version von ONTAP herunterzuladen.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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. Rufen Sie die NetApp Support Site auf, um die Dateien zum Netzboot des Systems herunterzuladen.
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. 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 FAS/AFF8000 Serie	Extrahieren Sie den Inhalt des `<ontap_version>_image.tgz` Datei zum Zielverzeichnis:
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz` Sie müssen den Inhalt des nicht extrahieren `<ontap_version>_image.tgz` Datei:

Sie verwenden die Informationen in den Verzeichnissen in "Phase 3".

Phase 3: Installieren und booten Sie node3

Phase-3-Übersicht

Während Phase 3 installieren und booten Sie node3, überprüfen, ob die Cluster- und Node-Management-Ports von node1 auf node3 online geschaltet sind und überprüfen Sie die Installation node3. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Falls erforderlich, stellen Sie die FC- oder UTA/UTA2-Konfiguration auf node3. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Schritte

1. "Installieren und booten Sie node3"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest"
3. "Überprüfen Sie die Installation von node3"
4. "Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3"
5. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3"

Installieren und booten Sie node3

Sie müssen node3 im Rack installieren, Verbindungen von node1 zu node3, Boot node3 übertragen und ONTAP installieren. Sie müssen dann eine der freien Festplatten von

node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die zuvor nicht in node2 verschoben wurden, wie in diesem Abschnitt beschrieben neu zuweisen.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Außerdem müssen Sie überprüfen, ob die SAN-LIFs erfolgreich in Knoten 3 verschoben wurden.

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Wichtig:

- Wenn Sie ein mit Storage Arrays verbundenes V-Series System oder ein System über FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Upgrades erforderlich Schritt 1 Bis Schritt 21, Dann verlassen Sie diesen Abschnitt und folgen Sie den Anweisungen im "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Abschnitte nach Bedarf, geben Sie Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 23.
- Wenn Sie ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und anschließend mit den fortfahren "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Geben Sie Abschnitte ein, und geben Sie Befehle an der Cluster-Eingabeaufforderung ein.

Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

   Wenn sich Node1 und Node2 in einem separaten Chassis befanden, können Sie Node3 in denselben Rack-Standort wie node1 platzieren. Wenn sich Node1 jedoch im selben Chassis mit node2 befand, müssen Sie den Node3 in seinen eigenen Regalbereich legen, vorzugsweise in der Nähe der Position von node1.

2. Installieren Sie node3 im Rack und befolgen Sie die Anweisungen *Installation und Setup* für Ihr Node-Modell.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im selben Chassis durchführen, installieren sie node4 sowohl im Chassis als auch in node3. Wenn Sie dies nicht tun, verhält sich der Node, wenn Sie node3 booten, wie in einer Dual-Chassis-Konfiguration. Und wenn Sie node4 booten, wird der Interconnect zwischen den Nodes nicht gestartet.

3. Kabelnode3, Verschieben der Verbindungen von node1 nach node3.

   Verkabeln Sie die folgenden Verbindungen mithilfe des *Installations- und Setup-Leitfadens* oder der *Installationsanforderungen für die FlexArray-Virtualisierung und Referenz* für die node3-Plattform, des entsprechenden Festplatten-Shelf-Dokuments und „ High Availability Management_“.

   Siehe "Quellen" Link zu den Installationsanforderungen für die FlexArray-Virtualisierung und „ Reference_“ und „ High Availability Management_“.

   - Konsole (Remote-Management-Port)

- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Möglicherweise müssen Sie die Interconnect-Karte oder die Cluster Interconnect-Kabelverbindung von node1 zu node3 nicht verschieben, da die meisten Plattform-Modelle über ein einzigartiges Interconnect-Kartenmodell verfügen. Für die MetroCluster Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node1 auf node3 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Einschalten Sie den Netzstrom auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im gleichen Chassis durchführen, wird node4 auch neu gebootet. Allerdings kann man den node4-Stiefel bis später ignorieren.

   > Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

   ```
   WARNING: The battery is unfit to retain data during a power outage. This
   is likely because the battery is discharged but could be due to other
   temporary conditions.
   When the battery is ready, the boot process will complete and services
   will be engaged.
   To override this delay, press 'c' followed by 'Enter'
   ```

5. Wenn die Warnmeldung in angezeigt wird Schritt 4, Nehmen Sie die folgenden Aktionen:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

   > **Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.**

   > Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

   > Sie müssen 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 DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Ist der Domain-Name (DNS) (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Netzboot auf Node3 durchführen:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` Im Abschnitt "Vorbereitungen für den Netzboot".

Unterbrechen Sie den Startvorgang nicht.

8. im Startmenü Option wählen `(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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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. Vervollständigen Sie die folgenden Teilschritte, um das Controller-Modul neu zu starten:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie den Wartungsmodus aus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12.] Überprüfen Sie, ob Controller und Chassis als ha konfiguriert sind:

    `ha-config show`

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn Controller und Chassis nicht als ha konfiguriert sind, verwenden Sie zum Korrigieren der Konfiguration die folgenden Befehle:

    `ha-config modify controller ha`

    `ha-config modify chassis ha`

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

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

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

14. Wartungsmodus beenden:

```
halt
```

Unterbrechen Sie DAS AUTOBOOT, indem Sie an der Eingabeaufforderung der Boot-Umgebung Strg-C drücken.

15. auf node2 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

```
date
```

16. prüfen Sie das Datum in node3 mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

17. Geben Sie bei Bedarf das Datum auf node3 ein:

```
set date mm/dd/yyyy
```

18. auf node3 überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

19. Ggf. Die Zeit auf node3 einstellen:

```
set time hh:mm:ss
```

20. legen Sie im Boot-Loader die Partner-System-ID auf node3 fest:

```
setenv partner-sysid node2_sysid
```

Für Knoten 3, `partner-sysid` Muss der von node2 sein.

a. Einstellungen speichern:

```
saveenv
```

21. Überprüfen Sie den `partner-sysid` Für Knoten 3:

```
printenv partner-sysid
```

22. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Beschreibung
Verfügt über Festplatten und keinen Back-End-Speicher	Gehen Sie zu Schritt 23
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Weiter mit Abschnitt "Einstellen der FC- oder UTA/UTA2-Konfiguration auf node3" Und vervollständigen Sie die Unterabschnitte in diesem Abschnitt. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 23. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

23. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

    Wenn Ihr System über ein Tape-SAN verfügt, müssen Sie das Zoning für die Initiatoren benötigen. Ändern Sie gegebenenfalls die integrierten Ports an den Initiator, indem Sie auf das verweisen "Konfigurieren von FC-Ports auf node3". Weitere Anweisungen zum Zoning finden Sie in der Dokumentation des Storage-Arrays und des Zoning.

24. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

25. Ändern Sie die WWPN-Werte (Worldwide Port Name) in den Host- oder Volume-Gruppen, die mit Array-LUNs auf dem Speicher-Array verknüpft sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

26. Wenn Ihre Konfiguration ein Switch-basiertes Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
27. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.

    Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

    a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

   Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

28. Boot-Node im Startmenü:

    ```
    boot_ontap menu
    ```

    Wenn Sie keine FC- oder UTA/UTA2-Konfiguration haben, führen Sie sie aus "UTA/UTA2-Ports in node4, Schritt 15, prüfen und konfigurieren" Damit node4 die Platten von node2 erkennen kann.

29. [[Schritt29]] für eine MetroCluster-Konfiguration, V-Series Systeme und Systeme mit FlexArray-Virtualisierungssoftware, die mit Storage-Arrays verbunden ist, müssen Sie die FC- oder UTA/UTA2-Ports auf node3 einrichten und konfigurieren, um die mit dem Node verbundenen Festplatten zu erkennen. Um diese Aufgabe abzuschließen, gehen Sie zu Abschnitt "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest".

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest

Wenn node3 integrierte FC-Ports, Onboard Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschnitt ausfüllen Konfigurieren Sie FC-Ports auf node3, Der Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren, Oder beide Abschnitte.

Unter Umständen bezieht sich bei den Marketingmaterialien von NetApp der Begriff UTA2 auf Adapter und Ports des konvergierten Netzwerkadapters (CNA). Allerdings verwendet die CLI den Begriff CNA.

- Wenn node3 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie zur springen "Überprüfen Sie die Installation von node3" Abschnitt.
- Wenn Sie jedoch ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware mit Storage-Arrays haben und node3 keine integrierten FC-Ports, Onboard UTA/UTA-Ports oder eine UTA/UTA2-Karte hat, kehren Sie zum Abschnitt *Installation und Boot-Knoten3* zurück und setzen Sie den Abschnitt unter fort "Schritt 23".

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node3
- UTA/UTA2-Ports in node3 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node3

Wenn node3 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in Betrieb nehmen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node1 haben, die Sie im Abschnitt gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder eine UTA/UTA2-Karte verfügt, konfigurieren Sie sie in UTA/UTA2-Ports in node3 prüfen und konfigurieren.

> Wenn Ihr System über Speicherfestplatten verfügt, geben Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle ein. Wenn Sie über ein „V-Series System“ oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus die entsprechenden Befehle ein.

1. Vergleichen Sie die FC-Einstellungen auf node3 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
2. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…

Festplatten sind vorhanden	Ändern Sie im Wartungsmodus (Option 5 im Startmenü) die FC-Ports auf node3 nach Bedarf:
	• So programmieren Sie Zielanschlüsse:
	`ucadmin modify -m fc -t target adapter`
	• So programmieren Sie Initiator-Ports:
	`ucadmin modify -m fc -t initiator adapter`
	`-t` Ist der FC4-Typ: Target oder Initiator.

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie im Wartungsmodus (Option 5 im Startmenü) die FC-Ports auf node3 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

3. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen mit dem folgenden Befehl und überprüfen Sie die Ausgabe: `ucadmin show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen mit dem folgenden Befehl und überprüfen Sie die Ausgabe: `ucadmin show`

4. Wartungsmodus beenden:

   ```
   halt
   ```

5. Booten Sie das System über die LOADER-Eingabeaufforderung:

   ```
   boot_ontap menu
   ```

6. nach Eingabe des Befehls warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
7. Wählen Sie die Option `5` Wählen Sie im Bootmenü für den Wartungsmodus aus.
8. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, fahren Sie mit dem Abschnitt fort UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen Sie den Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren Und gehen Sie zum Abschnitt "Überprüfen Sie die Installation von node3".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, fahren Sie mit dem Abschnitt fort UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen Sie den Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren Und kehren Sie zum Abschnitt *Installieren und Booten node3* zurück und fahren Sie bei fort "Schritt 23".

UTA/UTA2-Ports in node3 prüfen und konfigurieren

Wenn node3 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie möglicherweise neu konfigurieren, je nachdem, wie Sie das aktualisierte System verwenden möchten.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

Wenn Sie einen Unified Target Adapter (UTA/UTA2)-Port für FC verwenden möchten, müssen Sie zuerst überprüfen, wie der Port konfiguriert ist.

> Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

Sie können das verwenden `ucadmin show` Befehl zum Überprüfen der aktuellen Portkonfiguration:

```
*> ucadmin show
         Current  Current    Pending   Pending      Admin
Adapter  Mode     Type       Mode      Type         Status
-------  -------  -------    --------  ----------   --------
0e       fc       target     -         initiator    offline
0f       fc       target     -         initiator    offline
0g       fc       target     -         initiator    offline
0h       fc       target     -         initiator    offline
1a       fc       target     -         -            online
1b       fc       target     -         -            online
6 entries were displayed.
```

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht gleichzeitige NIC- und FCoE-Traffic über die gleiche 10-GbE-SFP+-Schnittstelle und unterstützt FC-Ziele.

UTA/UTA2-Ports befinden sich möglicherweise auf einem Adapter oder auf dem Controller und verfügen über die folgenden Konfigurationen. Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf der node3 überprüfen und gegebenenfalls ändern:

- UTA-/UTA2-Karten, die bestellt werden, werden vor dem Versand konfiguriert, um die von Ihnen geforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden vor dem Versand konfiguriert, um die Persönlichkeit zu erhalten, die Sie anfordern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein V-Series System verfügen oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt an der Eingabeaufforderung im Wartungsmodus Befehle ein. Sie müssen sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit konfiguriert sind, indem Sie auf node3 den folgenden Befehl eingeben:

Wenn das System…	Dann…
Festplatten sind vorhanden	Keine Aktion erforderlich.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
         Current  Current     Pending   Pending    Admin
Adapter  Mode     Type        Mode      Type       Status
-------  -------  ---------   -------   --------   ---------
0e       fc       initiator   -         -          online
0f       fc       initiator   -         -          online
0g       cna      target      -         -          online
0h       cna      target      -         -          online
0e       fc       initiator   -         -          online
0f       fc       initiator   -         -          online
0g       cna      target      -         -          online
0h       cna      target      -         -          online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Untersuchung der Ausgabe des `ucadmin show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.
4. Nehmen Sie eine der folgenden Aktionen:

Wenn die UTA/UTA2-Ports…	Dann…
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. [[Auto_check3_schritt 5]]Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

6. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

7. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` Ist der Persönlichkeitsmodus, `fc` Oder `cna`.
   - `-t` Ist der Typ FC4, `target` Oder `initiator`.

   > Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

8. Überprüfen Sie die Einstellungen:

   `ucadmin show`

9. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`ucadmin show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
*> ucadmin show
         Current    Current     Pending  Pending     Admin
Adapter  Mode       Type        Mode     Type        Status
-------  --------   ----------  -------  --------    --------
1a       fc         initiator   -        -           online
1b       fc         target      -        initiator   online
2a       fc         target      cna      -           online
2b       fc         target      cna      -           online
*>
```

10. Platzieren Sie alle Zielports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

11. Anschluss verkabeln.
12. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Überprüfen Sie die Installation von node3".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zum Abschnitt *Installieren und Starten von node3* zurück, und fahren Sie bei fort "Schritt 23".

13. Wartungsmodus beenden:

```
halt
```

14. Boot-Knoten in Boot-Menü durch Ausführen `boot_ontap menu`. Wenn Sie ein Upgrade auf eine A800 durchführen, gehen Sie zu Schritt 23.
15. Gehen Sie auf node3 zum Boot-Menü und wählen Sie mit 22/7 die versteckte Option aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node1 ein, um die Festplatten von node1 node3 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
```

```
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes
.
<output truncated>
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
<output truncated>
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
```

```
<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:
```

Im obigen Beispiel der Konsolenausgabe werden Sie von ONTAP aufgefordert, den Namen des Partner-Node anzugeben, wenn das System ADP-Festplatten (Advanced Disk Partitioning) verwendet.

16. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, Es zeigt an, dass das System die FC- oder UTA/UTA2-Ports wieder in den Ziel-Modus zurückgesetzt hat und somit keine Disketten sehen kann. Um dies zu beheben, fahren Sie mit fort Schritt 17 Bis Schritt 22Oder gehen Sie zu Abschnitt "Überprüfen Sie die Installation von node3".
17. Drücken Sie während des AUTOBOOTS Strg-C, um den Knoten an der Eingabeaufforderung LOADER> anzuhalten.
18. wechseln Sie an der LOADER-Eingabeaufforderung in den Wartungsmodus:

    `boot_ontap maint`

19.] im Wartungsmodus werden alle zuvor festgelegten Initiator-Ports angezeigt, die sich jetzt im Zielmodus befinden:

    `ucadmin show`

    Ändern Sie die Ports zurück in den Initiatormodus:

    `ucadmin modify -m fc -t initiator -f adapter name`

20. Überprüfen Sie, ob die Ports in den Initiatormodus geändert wurden:

    `ucadmin show`

21. Wartungsmodus beenden:

    `halt`

Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das auch externe Festplatten unterstützt, gehen Sie zu Schritt 22.

Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das sowohl interne als auch externe Festplatten, wie z. B. ein AFF A800 System, unterstützt, finden Sie unter Schritt 23.

22. Starten Sie an der LOADER-Eingabeaufforderung:

```
boot_ontap menu
```

Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her.

Dies gilt nur, wenn das Root-Volume NetApp-Volume-Verschlüsselung verwendet.

a. Zurück zum speziellen Startmenü:

```
LOADER> boot_ontap menu
```

```
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)? 10
```

a. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

b. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

d. Geben Sie bei Aufforderung die Backup-Daten ein.

Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

e. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 22 Bis das System ordnungsgemäß gebootet wird.

23. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. AFF A800 Systeme), setzen Sie das node1-Aggregat als Root-Aggregat ein, um zu bestätigen, dass node3 aus dem Root-Aggregat von node1 bootet. Zum Festlegen des Root-Aggregats rufen Sie das Boot-Menü auf und wählen dann Option `5` Um in den Wartungsmodus zu wechseln.

Die folgenden Teilschritte müssen in der angegebenen Reihenfolge ausgeführt werden; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.

Im folgenden Verfahren wird node3 vom Root-Aggregat von node1 gestartet:

a. Wechseln in den Wartungsmodus:

```
boot_ontap maint
```

b. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node1 Aggregat:

```
aggr status -r
```

c. Überprüfen Sie den Status des node1-Aggregats:

```
aggr status
```

d. Bei Bedarf das node1 Aggregat online bringen:

```
aggr_online root_aggr_from_node1
```

e. Verhindern Sie, dass das node3 vom ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node3
```

f. Legen Sie das node1-Root-Aggregat als das neue Root-Aggregat für node3 fest:

```
aggr options aggr_from_node1 root
```

g. Überprüfen Sie, ob das Root-Aggregat von node3 offline ist und das Root-Aggregat für die von node1 hergebrachten Festplatten online ist und in den Root-Status eingestellt ist:

```
aggr status
```

Wenn der vorherige Unterschritt nicht ausgeführt wird, kann node3 vom internen Root-Aggregat booten, oder es kann dazu führen, dass das System eine neue Cluster-Konfiguration übernimmt oder Sie aufgefordert werden, eine zu identifizieren.

Im Folgenden wird ein Beispiel für die Befehlsausgabe angezeigt:

```
---------------------------------------------------------------
Aggr                  State    Status             Options

aggr0_nst_fas8080_15 online   raid_dp, aggr      root, nosnap=on
                              fast zeroed
                              64-bit

aggr0                 offline  raid_dp, aggr      diskroot
                              fast zeroed
                              64-bit
---------------------------------------------------------------
```

Überprüfen Sie die Installation von node3

Sie müssen überprüfen, ob die physischen Ports von node1 den physischen Ports auf node3 korrekt zugeordnet sind. Dadurch kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Abhängig vom Modell der Nodes kann das physische Port-Layout variieren. Wenn der neue Node gestartet wird, versucht ONTAP, zu ermitteln, welche Ports die Cluster LIFs hosten sollten, damit es automatisch zu Quorum kommt.

Wenn die physischen Ports auf node1 nicht direkt den physischen Ports auf node3 zugeordnet werden, wird der folgende Abschnitt angezeigt Stellen Sie die Netzwerkkonfiguration auf node3 wieder her Muss zur Reparatur der Netzwerkverbindung verwendet werden.

Nach der Installation und dem Booten von node3 müssen Sie überprüfen, ob die Installation korrekt ist. Sie müssen warten, bis Knoten 3 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen.

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node3 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node3 dem Quorum beigetreten ist:

   `cluster show -node node3 -fields health`

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node3 Teil desselben Clusters wie node2 ist und dass er sich in einem

ordnungsgemäßen Zustand befindet:

```
cluster show
```

3. Führen Sie abhängig von der ONTAP-Version auf dem zu aktualisierenden HA-Paar eine der folgenden Aktionen durch:

Lautet Ihre ONTAP Version…	Dann…
9.8 bis 9.11.1	Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören: `::> network connections listening show -vserver Cluster`
9.12.1 oder höher	Überspringen Sie diesen Schritt und gehen Sie zu Schritt 5.

Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Wiederholen Sie Schritt 3, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

5. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set advanced
```

6. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand wie zuvor in node1 befand, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

```
system controller replace show

system controller replace show-details
```

7. Wenn Sie auf einem MetroCluster System arbeiten, überprüfen Sie, ob der ersetzte Controller für die

MetroCluster-Konfiguration ordnungsgemäß konfiguriert ist. Die MetroCluster-Konfiguration sollte sich in einem ordnungsgemäßen Zustand befinden. Siehe "Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration".

Konfigurieren Sie die Intercluster-LIFs auf MetroCluster-Node-Node3 neu, und überprüfen Sie Cluster-Peering, um die Kommunikation zwischen den MetroCluster-Nodes wiederherzustellen, bevor Sie mit Schritt 6 fortfahren.

Überprüfen Sie den MetroCluster-Node-Status:

```
metrocluster node show
```

8. Setzen Sie den Austausch des Controllers wieder ein:

```
system controller replace resume
```

9. Der Austausch des Controllers wird anhand der folgenden Meldung unterbrochen:

```
Cluster::*> system controller replace show
Node             Status                       Error-Action
---------------- -------------------------
-----------------------------------
Node1(now node3) Paused-for-intervention      Follow the instructions
given in
                                              Step Details
Node2                      None

Step Details:
--------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.

2 entries were displayed.
```

In diesem Verfahren wurde der Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node3_ umbenannt.

10. Wenn der Controller-Austausch im Status „Pause“ steht, fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, um die Netzwerkkonfiguration auf dem Node wiederherzustellen.

Stellen Sie die Netzwerkkonfiguration auf node3 wieder her

Nachdem Sie bestätigt haben, dass node3 sich im Quorum befindet und mit node2 kommunizieren kann, überprüfen Sie, ob node1 VLANs, Interface Groups und Broadcast-Domains auf node3 zu sehen sind. Überprüfen Sie außerdem, ob alle node3-Netzwerk-Ports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Verknüpfen mit *Network Management*.

> Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe "NetApp Bugs Online Fehler-ID 1570339" Und den Knowledge Base Artikel "CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE" Für eine Anleitung.

Schritte

1. Listen Sie alle physischen Ports auf, die auf einem aktualisierten Node1 (als node3 bezeichnet) stehen:

   ```
   network port show -node node3
   ```

   Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. In dieser Ausgabe sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um zu entscheiden, welche Ports als Ports für Schnittstellengruppen, VLAN-Basis-Ports oder eigenständige physische Ports zum Hosten von LIFs verwendet werden müssen.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Liste der Netzwerkanschlussfähigkeit aller Ports auf node3:

   ```
   network port reachability show
   ```

   Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
clusterA::*> reachability show -node node1_node3
(network port reachability show)
Node         Port       Expected Reachability   Reachability Status
-----------  ---------  ----------------------  ----------------------
node1_node3
             a0a        Default:Default         no-reachability
             a0a-822    Default:822             no-reachability
             a0a-823    Default:823             no-reachability
             e0M        Default:Mgmt            ok
             e0a        Cluster:Cluster         misconfigured-
reachability
             e0b        Cluster:Cluster         no-reachability
             e0c        Cluster:Cluster         no-reachability
             e0d        Cluster:Cluster         no-reachability
             e0e        Cluster:Cluster         ok
             e0e-822    -                       no-reachability
             e0e-823    -                       no-reachability
             e0f        Default:Default         no-reachability
             e0f-822    Default:822             no-reachability
             e0f-823    Default:823             no-reachability
             e0g        Default:Default         misconfigured-
reachability
             e0h        Default:Default         ok
             e0h-822    Default:822             ok
             e0h-823    Default:823             ok
18 entries were displayed.
```

Im vorherigen Beispiel wird node1_node3 kurz nach dem Austausch des Controllers gestartet. Einige Ports verfügen nicht über die Fähigkeit, ihre zu erwartenden Broadcast-Domänen zu erreichen und müssen repariert werden.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node3 mit einem anderen Status als der Erreichbarkeit `ok`. Führen Sie den folgenden Befehl aus, zuerst auf beliebigen physischen Ports, dann auf beliebigen VLAN-Ports, nacheinander:

   `network port reachability repair -node` *`node_name`* `-port` *`port_name`*

   Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node1_node3 -port e0h
```

```
Warning: Repairing port "node1_node3: e0h" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Wie oben dargestellt, wird eine Warnmeldung für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Wiederachbarkeit der Broadcast-Domain unterscheiden können, wo sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

```
network port reachability show
```

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Wenn die Konfiguration der Schnittstellengruppen nicht mit dem physischen Portlayout des neuen Controllers übereinstimmt, ändern Sie diese wie folgt.

   a. Sie müssen zunächst physische Ports entfernen, die als Ports für Schnittstellengruppen von ihrer Broadcast-Domain-Mitgliedschaft verwendet werden sollen. Dazu verwenden Sie den folgenden Befehl:

      ```
      network port broadcast-domain remove-ports -broadcast-domain broadcast-domain_name -ports node_name:port_name
      ```

   b. Hinzufügen eines Mitgliedports zu einer Schnittstellengruppe:

      ```
      network port ifgrp add-port -node node_name -ifgrp ifgrp -port port_name
      ```

   c. Die Schnittstellengruppe wird der Broadcast-Domäne automatisch ca. eine Minute nach dem Hinzufügen des ersten Mitgliedports hinzugefügt.

   d. Vergewissern Sie sich, dass die Schnittstellengruppe der entsprechenden Broadcast-Domäne hinzugefügt wurde:

      ```
      network port reachability show -node node_name -port ifgrp
      ```

      Wenn der Status der Erreichbarkeit der Schnittstellengruppe nicht lautet `ok`, Weisen Sie es der entsprechenden Broadcast-Domain zu:

```
network port broadcast-domain add-ports -broadcast-domain broadcast_domain_name -ports node:port
```

6. weisen Sie dem die entsprechenden physischen Ports zu `Cluster` Broadcast-Domäne in folgenden Schritten:

   a. Ermitteln Sie, welche Ports eine Reachability zum haben `Cluster` Broadcast-Domäne:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Reparieren Sie jeden Port mit Erreichbarkeit zum `Cluster` Broadcast-Domäne, wenn ihr Status der Erreichbarkeit nicht lautet `ok`:

      ```
      network port reachability repair -node node_name -port port_name
      ```

7. Verschieben Sie die verbleibenden physischen Ports in ihre korrekten Broadcast-Domänen, indem Sie einen der folgenden Befehle verwenden:

```
network port reachability repair -node node_name -port port_name

network port broadcast-domain remove-port

network port broadcast-domain add-port
```

Vergewissern Sie sich, dass keine unerreichbaren oder unerwarteten Ports vorhanden sind. Überprüfen Sie den Status der Erreichbarkeit aller physischen Ports mithilfe des folgenden Befehls und überprüfen Sie die Ausgabe, um sicherzustellen, dass der Status lautet `ok`:

```
network port reachability show -detail
```

8. Wiederherstellen aller VLANs, die möglicherweise verschoben wurden, durch die folgenden Schritte:

   a. Versetzte VLANs auflisten:

      ```
      cluster controller-replacement network displaced-vlans show
      ```

      Die Ausgabe sollte wie folgt angezeigt werden:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                Original
      Node      Base Port   VLANs
      --------  ----------  ----------------------------------------
      Node1       a0a       822, 823
                  e0e       822, 823
      2 entries were displayed.
      ```

   b. Stellen Sie VLANs wieder her, die von ihren früheren Basis-Ports verdrängt wurden:

      ```
      cluster controller-replacement network displaced-vlans restore
      ```

      Das folgende Beispiel zeigt die Wiederherstellung von VLANs, die aus der Schnittstellengruppe „a0a“ wieder in dieselbe Schnittstellengruppe verschoben wurden:

      ```
      Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
      -destination-port a0a
      ```

      Das folgende Beispiel zeigt die Wiederherstellung von verlagerten VLANs am Port „e0e“ an' e0h:

      ```
      Cluster::*> displaced-vlans restore -node node1_node3 -port e0e
      -destination-port e0h
      ```

      Wenn eine VLAN-Wiederherstellung erfolgreich ist, werden die verschobenen VLANs auf dem angegebenen Zielport erstellt. Die VLAN-Wiederherstellung schlägt fehl, wenn der Zielport Mitglied einer Schnittstellengruppe ist oder der Zielport nicht verfügbar ist.

Warten Sie etwa eine Minute, bis neu wiederhergestellte VLANs in ihren entsprechenden Broadcast-Domänen platziert werden.

a. Erstellen Sie bei Bedarf neue VLAN-Ports für VLAN-Ports, die nicht im enthalten sind `cluster controller-replacement network displaced-vlans show` Ausgabe sollte aber auf anderen physischen Ports konfiguriert werden.

9. Löschen Sie alle leeren Broadcast-Domänen, nachdem alle Port-Reparaturen abgeschlossen wurden:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
```

10. Überprüfung der Anschlussfähigkeit:

```
network port reachability show
```

Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn ein Port einen anderen Status als diese beiden meldet, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

11. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

```
network port show
```

12. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

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

13. Stellen Sie die LIF-Start-Ports wieder her und geben Sie ggf. den Vserver(s) und die Home Ports von LIFs an, die über folgende Schritte wiederhergestellt werden müssen:

a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

b. LIF-Home-Knoten und Home-Ports wiederherstellen:

```
cluster controller-replacement network displaced-interface restore-home-node
-node node_name -vserver vserver_name -lif-name LIF_name
```

14. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

```
network interface show -fields home-port, status-admin
```

Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3

Wenn Sie mithilfe von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Volumes auf dem System verschlüsseln, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht synchronisieren, können beim Verschieben der Node1-Aggregate mit ARL von node2 auf node3 Ausfälle auftreten, da node3 nicht über die

erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie den folgenden Befehl von node3 aus:

   ```
   security key-manager onboard sync
   ```

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node3 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

   ```
   ::> security key-manager key query -node node3 -fields restored -key
   -type SVM-KEK
   ```

   Beispiel

   ```
   ::> security key-manager key query -node node3 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node3    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3

Nachdem Sie die Netzwerkkonfiguration auf node3 und bevor Sie Aggregate von node2 auf node3 verschoben haben, müssen Sie überprüfen, ob die NAS-Daten-LIFs, die zu node1 gehören und sich derzeit auf node2 befinden, von node2 in node3 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Wenn Sie die Portgeschwindigkeit der T6-basierten Ethernet-Netzwerkkarten oder Motherboard-Ports ändern, können Sie nach der Geschwindigkeitskonvertierung fehlerhafte Pakete beobachten. Siehe "NetApp Bugs Online Fehler-ID 1570339" Und den Knowledge Base Artikel "CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE" Für eine Anleitung.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   `system controller replace resume`

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Wiederaufnahme des Betriebs der Versetzung:

   `system controller replace resume`

   Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen verschiebt das System die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf den neuen Controller, node3. Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

3. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

   Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

4. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

   `cluster controller-replacement network displaced-interface show`

   Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in Knoten 3 wieder her:

   `cluster controller-replacement network displaced-interface restore-home-node`

5. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

   `system controller replace resume`

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung
- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster
- Lautstärkerprüfung

Phase 4: Knoten2 verschieben und ausmustern

Phase-4-Übersicht

Während Phase 4 werden Aggregate und NAS-Daten-LIFs von Knoten 2 auf Knoten 3 verschoben. Sie zeichnen auch die erforderlichen node2-Informationen für die spätere Verwendung im Verfahren auf und ziehen dann node2 zurück.

Schritte

1. "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3"
2. "Node2 ausmustern"

Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3

Bevor Sie node2 durch node4 ersetzen, verschieben Sie die nicht-Root-Aggregate und NAS-Daten-LIFs, die im Besitz von node2 sind, auf node3.

Bevor Sie beginnen

Nach den Nachprüfungen aus der vorherigen Phase wird automatisch die Ressourcenfreigabe für node2 gestartet. Die Aggregate außerhalb des Root-Bereichs und LIFs für nicht-SAN-Daten werden von node2 auf node3 migriert.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich.

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. In dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in node3 migriert werden.

> Der Home-Inhaber für die Aggregate und LIFs werden nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind und ihren Status auf node3:

```
storage aggregate show -node node3 -state online -root false
```

Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

```
cluster::> storage aggregate show -node node3 state online -root false

Aggregate      Size         Available   Used%   State   #Vols  Nodes
RAID     Status
----------     ---------    ---------   ------  -----   -----  ------
-------  ------
aggr_1         744.9GB      744.8GB      0%     online  5      node2
raid_dp  normal
aggr_2         825.0GB      825.0GB      0%     online  1      node2
raid_dp  normal
2 entries were displayed.
```

Wenn die Aggregate offline sind oder in node3 offline sind, bringen Sie sie mit dem folgenden Befehl auf node3 online, einmal für jedes Aggregat:

`storage aggregate online -aggregate` *`aggr_name`*

2. Überprüfen Sie, ob alle Volumes auf node3 online sind, indem Sie den folgenden Befehl auf node3 verwenden und die Ausgabe überprüfen:

   `volume show -node` *`node3`* `-state offline`

   Wenn ein Volume auf node3 offline ist, schalten Sie sie online. Verwenden Sie dazu den folgenden Befehl auf node3, einmal für jedes Volume:

   `volume online -vserver` *`vserver_name`* `-volume` *`volume_name`*

   Der *`vserver_name`* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

3. Überprüfen Sie, ob die LIFs zu den richtigen Ports verschoben wurden und über den Status von verfügen `up`. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node_name`* `-status-admin up`

4. Wenn die Ports, die derzeit Daten-LIFs hosten, nicht auf der neuen Hardware vorhanden sind, entfernen Sie diese aus der Broadcast-Domäne:

   `network port broadcast-domain remove-ports`

5. Überprüfen Sie, ob auf node2 keine Daten-LIFs bleiben, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

   `network interface show -curr-node` *`node2`* `-role data`

Node2 ausmustern

Um node2 außer Betrieb zu nehmen, schalten Sie node2 zunächst ordnungsgemäß aus und entfernen Sie es aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

   Der Knoten wird automatisch angehalten.

Nachdem Sie fertig sind

Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5: installieren und booten sie node4

Phase-5-Übersicht

In Phase 5 installieren und booten Sie node4, überprüfen, ob die Cluster- und Node-Management-Ports von node2 auf node4 online geschaltet sind, und überprüfen Sie die Installation von node4. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Falls erforderlich, stellen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 ein. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind.

Schritte

1. "installieren und booten sie node4"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest"
3. "Überprüfen Sie die installation von node4"
4. "Wiederherstellen der Key-Manager-Konfiguration auf node4"
5. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4"

installieren und booten sie node4

Sie müssen node4 im Rack installieren, Verbindungen von node2 zu node4 übertragen, node4 booten und ONTAP installieren. Sie müssen dann eine der node2 Ersatzfestplatten, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die nicht zu node3 früher in diesem Prozess verschoben wurden, neu zuweisen, wie in diesem Abschnitt beschrieben.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Vorgang wird größtenteils automatisch durchgeführt. Der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen.

Sie müssen node4 als Netzboot ausführen, wenn es nicht die gleiche Version von ONTAP 9 hat, die auf node2 installiert ist. Nachdem sie node4 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Wichtig:

- Wenn Sie ein mit Storage-Arrays verbundenes V-Series System oder ein System mit FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Anforderungen unbedingt zu beachten Schritt 1 Bis Schritt 21, Dann verlassen Sie diesen Abschnitt und folgen Sie den Anweisungen zu "Konfigurieren Sie FC-Ports auf node4" Und nach "UTA/UTA2-Ports auf node4 prüfen und konfigurieren", Eingabe von Befehlen im Wartungsmodus. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 23.
- Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt ausfüllen und mit fortfahren "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt.

   Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

2. installieren sie node4 im Rack gemäß den Anweisungen in der Anleitung *Installation and Setup Instructions* für das Node-Modell.
3. Kabel node4, ziehen Sie die Verbindungen von node2 nach node4.

   Verkabeln Sie die folgenden Verbindungen mithilfe der Anleitung im *Installation and Setup Instructions* oder beim *FlexArray Installation Requirements and Reference* für die node4-Plattform, dem entsprechenden Platten-Shelf-Dokument und *High Availability Management*.

   Siehe "Quellen" Link zu den Installationsanforderungen für die FlexArray-Virtualisierung und „ Reference_“ und „ High Availability Management_“.

   - Konsole (Remote-Management-Port)
   - Cluster-Ports
   - Datenports
   - Cluster- und Node-Management-Ports
   - Storage
   - SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

   > Möglicherweise müssen Sie die Interconnect-Karte/FC-VI-Karte oder die Interconnect/FC-VI-Kabelverbindung von node2 auf node4 nicht verschieben, da die meisten Plattform-Modelle über einzigartige Interconnect-Kartenmodelle verfügen. Bei der MetroCluster Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node2 nach node4 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Schalten Sie node4 ein, und unterbrechen Sie den Bootvorgang, indem Sie am Konsolenterminal Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Wenn Sie node4 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
         because the battery is discharged but could be due to other
temporary
         conditions.
         When the battery is ready, the boot process will complete
         and services will be engaged. To override this delay, press 'c'
followed
         by 'Enter'
```

5. Wenn die Warnmeldung in Schritt 4 angezeigt wird, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.

Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der DNS-Domain-Name (optional). Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Ausführen eines Netzboots auf node4:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 1 im Abschnitt "Vorbereitungen für den Netzboot".

Unterbrechen Sie den Startvorgang nicht.

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.

Ignorieren Sie die folgende Meldung:

`This procedure is not supported for Non-Disruptive Upgrade on an HA pair`

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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

   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12. Vergewissern Sie sich, dass Controller und Chassis als HA konfiguriert sind:

    `ha-config show`

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn der Controller und das Chassis nicht als HA konfiguriert wurden, verwenden Sie zum Korrigieren der Konfiguration die folgenden Befehle:

    `ha-config modify controller ha`

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

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

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

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

14. Beenden des Wartungsmodus:

```
halt
```

Unterbrechen Sie DAS AUTOBOOT, indem Sie an der Eingabeaufforderung der Boot-Umgebung Strg-C drücken.

15. auf node3 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

```
date
```

16. Überprüfen Sie am node4 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

17. Legen Sie bei Bedarf das Datum auf node4 fest:

```
set date mm/dd/yyyy
```

18. Überprüfen Sie auf node4 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

19. Stellen Sie bei Bedarf die Uhrzeit auf node4 ein:

```
set time hh:mm:ss
```

20. Legen Sie im Boot-Loader die Partner-System-ID auf node4 fest:

```
setenv partner-sysid node3_sysid
```

Für node4, `partner-sysid` Muss das der Node3 sein.

Einstellungen speichern:

```
saveenv
```

21. [[Auto_install4_step21] Verify the `partner-sysid` für node4:

```
printenv partner-sysid
```

22. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Gehen Sie zu Schritt 23.
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Weiter mit Abschnitt "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Und vervollständigen Sie die Unterabschnitte in diesem Abschnitt. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 23. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

23. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

    Wenn Ihr System über ein Tape-SAN verfügt, müssen Sie das Zoning für die Initiatoren benötigen. Ändern Sie gegebenenfalls die integrierten Ports an den Initiator, indem Sie auf das verweisen "Konfigurieren Sie FC-Ports auf node4". Weitere Anweisungen zum Zoning finden Sie in der Dokumentation des Storage-Arrays und des Zoning.

24. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

25. Ändern Sie die WWPN-Werte (Worldwide Port Name) in den Host- oder Volume-Gruppen, die den Array-LUNs auf dem Speicher-Array zugeordnet sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

26. Wenn die Konfiguration das Switch-basierte Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.

27. Wenn Sie NSE-Laufwerke (NetApp Storage Encryption) installiert haben, führen Sie die folgenden Schritte aus.

    Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

    a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`.

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support **false**`

> FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Management der Storage-Verschlüsselung mit dem Onboard Key Manager".

28. Boot-Node im Startmenü:

```
boot_ontap menu
```

Wenn Sie keine FC- oder UTA/UTA2-Konfiguration haben, führen Sie sie aus "UTA/UTA2-Ports in node4, Schritt 15, prüfen und konfigurieren" Damit node4 die Platten von node2 erkennen kann.

29. für die MetroCluster Konfiguration, V-Series Systeme und Systeme mit FlexArray-Virtualisierungssoftware, die an Storage-Arrays angeschlossen ist, müssen Sie die FC- oder UTA/UTA2-Ports auf node4 einrichten und konfigurieren, um die mit dem Node verbundenen Festplatten zu erkennen. Um diese Aufgabe abzuschließen, gehen Sie zu Abschnitt "Legen Sie die FC- oder UTA/UT2-Konfiguration auf node4 fest".

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest

Wenn node4 über integrierte FC-Ports, integrierte Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte verfügt, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschnitt oder oder beide Abschnitte ausfüllen Konfigurieren Sie FC-Ports auf node4 UTA/UTA2-Ports auf node4 prüfen und konfigurieren .

> Wenn node4 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie weiter gehen "Überprüfen Sie die installation von node4". Wenn Sie jedoch ein V-Series System oder FlexArray-Virtualisierungssoftware haben und mit Storage-Arrays verbunden sind und node4 keine integrierten FC-Ports, Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie zum Abschnitt *Installation und Boot-Abschnitt node4* zurückkehren und wieder aufnehmen "Schritt 22". stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt. Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node4

- UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node4

Wenn node4 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in den Dienst stellen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node2 haben, die Sie im Abschnitt gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder einen UTA/UTA2-Adapter verfügt, konfigurieren Sie sie in UTA/UTA2-Ports auf node4 prüfen und konfigurieren.

> Wenn im System Storage-Festplatten vorhanden sind, müssen Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle eingeben. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware haben, die mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

2. Vergleichen Sie die FC-Einstellungen auf node4 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
3. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…

Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node4 nach Bedarf:
	• So programmieren Sie Zielanschlüsse:
	`ucadmin modify -m fc -t target adapter`
	• So programmieren Sie Initiator-Ports:
	`ucadmin modify -m fc -t initiator adapter`
	`-t` Ist der FC4-Typ: Target oder Initiator.

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node4 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

4. Beenden des Wartungsmodus:

   ```
   halt
   ```

5. Booten Sie das System über die LOADER-Eingabeaufforderung:

   ```
   boot_ontap menu
   ```

6. Nachdem Sie den Befehl eingegeben haben, warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
7. Wählen Sie die Option `5` Wählen Sie im Bootmenü für den Wartungsmodus aus.
8. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Überspringen Sie diesen Abschnitt und gehen Sie zu "Überprüfen Sie die installation von node4" Wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Gehen Sie zu UTA/UTA2-Ports auf node4 prüfen und konfigurieren Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt *UTA/UTA2-Ports auf node4* überprüfen und konfigurieren, wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat, zurück zum Abschnitt *Installation und Boot node4*, und wieder bei aufnehmen "Schritt 23".

UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Wenn node4 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie je nach Nutzung des aktualisierten Systems konfigurieren.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht es, gleichzeitig NIC- und FCoE-Datenverkehr die gleiche 10-GbE-SFP+-Schnittstelle zu nutzen und das FC-Ziel zu unterstützen.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

UTA2-Ports können an einem Adapter oder auf dem Controller mit den folgenden Konfigurationen verwendet werden:

- UTA-/UTA2-Karten, die gleichzeitig mit dem Controller bestellt wurden, werden vor dem Versand konfiguriert, um die von Ihnen angeforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden konfiguriert (vor dem Versand), um die von Ihnen angeforderte Persönlichkeit zu besitzen.

Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf node4 überprüfen und sie gegebenenfalls ändern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein MetroCluster FC-System, ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware verfügen, die mit Storage-Arrays verbunden ist, müssen Sie sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit mit einem der folgenden Befehle auf node4 konfiguriert werden:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node    Adapter Mode     Type       Mode      Type      Status
----    ------- ---      ---------  -------   --------  -------
f-a     0e      fc       initiator  -          -        online
f-a     0f      fc       initiator  -          -        online
f-a     0g      cna      target     -          -        online
f-a     0h      cna      target     -          -        online
f-a     0e      fc       initiator  -          -        online
f-a     0f      fc       initiator  -          -        online
f-a     0g      cna      target     -          -        online
f-a     0h      cna      target     -          -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Überprüfen Sie die Ausgabe des `ucadmin show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.
4. Führen Sie eine der folgenden Aktionen durch:

Wenn die CNA-Ports…	**Dann…**
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	**Dann…**
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

6. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

7. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

- `-m` Ist der Personality-Modus, FC oder 10GbE UTA.
- `-t` Ist der Typ FC4, `target` Oder `initiator`.

> Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

8. Überprüfen Sie die Einstellungen mit dem folgenden Befehl und prüfen Sie die Ausgabe:

```
ucadmin show
```

9. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`ucadmin show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
*> ucadmin show
Node  Adapter  Current Mode  Current Type  Pending Mode  Pending Type
Admin Status
----  -------  ------------  ------------  ------------  ------------
------------
f-a   1a       fc             initiator    -             -
online
f-a   1b       fc             target       -             initiator
online
f-a   2a       fc             target       cna           -
online
f-a   2b       fc             target       cna           -
online
4 entries were displayed.
*>
```

10. Platzieren Sie alle Ziel-Ports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`

Wenn das System…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config adapter_name up`

11. Verkabeln Sie den Port.
12. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Überprüfen Sie die installation von node4".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zum Abschnitt *Installieren und Starten von node4* zurück, und fahren Sie bei fort "Schritt 23".

13. Wartungsmodus beenden:

```
halt
```

14. Boot-Knoten in Boot-Menü:

```
boot_ontap menu.
```

Wenn Sie ein Upgrade auf eine A800 durchführen, gehen Sie zu Schritt 23

15. in node4 wechseln Sie zum Startmenü und wählen Sie unter 22/7 die ausgeblendete Option aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node2 ein, um die Festplatten von node2 node4 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7
(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
```

```
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to
restore the system configuration, or option (4) to initialize all
disks and setup a new system.
Normal Boot is prohibited.
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)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure
you want to continue?: yes
.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:
<nodename of the node being replaced>
Changing sysid of node node2 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
```

```
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote
    key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:
```

Im obigen Beispiel der Konsolenausgabe werden Sie von ONTAP aufgefordert, den Namen des Partner-Node anzugeben, wenn das System ADP-Festplatten (Advanced Disk Partitioning) verwendet.

16. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, Es zeigt an, dass das

System die FC- oder UTA/UTA2-Ports wieder in den Ziel-Modus zurückgesetzt hat und somit keine Disketten sehen kann. Um dies zu beheben, fahren Sie mit fort Schritt 17 Bis Schritt 22 Oder weiter mit Abschnitt "Überprüfen Sie die installation von node4".

17. Drücken Sie während des AUTOBOOTS Strg-C, um den Knoten an der Eingabeaufforderung LOADER> anzuhalten.
18. Wechseln Sie an der LOADER-Eingabeaufforderung in den Wartungsmodus:

    ```
    boot_ontap maint
    ```

19. Zeigen Sie im Wartungsmodus alle zuvor festgelegten Initiator-Ports an, die sich jetzt im Ziel-Modus befinden:

    ```
    ucadmin show
    ```

    Ändern Sie die Ports zurück in den Initiatormodus:

    ```
    ucadmin modify -m fc -t initiator -f adapter name
    ```

20. Vergewissern Sie sich, dass die Ports in den Initiatormodus geändert wurden:

    ```
    ucadmin show
    ```

21. Beenden des Wartungsmodus:

    ```
    halt
    ```

    > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das auch externe Festplatten unterstützt, gehen Sie zu Schritt 22.
    >
    > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten verwendet, zu einem System, das sowohl interne als auch externe Festplatten unterstützt, z. B. ein AFF A800 System, finden Sie unter Schritt 23.

22. Starten Sie an der LOADER-Eingabeaufforderung:

    ```
    boot_ontap menu
    ```

    Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

    Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her.

    > Dies gilt nur, wenn das Root-Volume NetApp-Volume-Verschlüsselung verwendet.

    a. Zurück zum speziellen Startmenü:

       ```
       LOADER> boot_ontap menu
       ```

```
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)? 10
```

a. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

b. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

d. Geben Sie bei Aufforderung die Backup-Daten ein.

> Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

e. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

> In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 22 Bis das System ordnungsgemäß gebootet wird.

23. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. AFF A800 Systeme), stellen Sie das node2-Aggregat als Root-Aggregat ein, um sicherzustellen, dass node4 aus dem Root-Aggregat von node2 startet. Zum Festlegen des Root-Aggregats rufen Sie das Boot-Menü auf und wählen dann Option `5` Um in den Wartungsmodus zu wechseln.

> **Die folgenden Teilschritte müssen in der angegebenen Reihenfolge ausgeführt werden; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.**

Mit dem folgenden Verfahren wird node4 vom Root-Aggregat von node2 gestartet:

a. Wechseln in den Wartungsmodus:

```
boot_ontap maint
```

b. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node2 Aggregat:

```
aggr status -r
```

c. Überprüfen Sie den Status des node2-Aggregats:

```
aggr status
```

d. Bei Bedarf das node2 Aggregat online bringen:

```
aggr_online root_aggr_from_node2
```

e. Verhindern Sie, dass das node4 aus dem ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node4
```

f. Legen Sie das node2-Root-Aggregat als das neue Root-Aggregat für node4 fest:

```
aggr options aggr_from_node2 root
```

g. Überprüfen Sie, ob das Root-Aggregat von node4 offline ist und das Root-Aggregat für die von node2 herübergebrachten Festplatten online ist und in den Root-Status eingestellt ist:

```
aggr status
```

> Wenn der vorherige Unterschritt nicht ausgeführt wird, kann node4 vom internen Root-Aggregat booten, oder es kann dazu führen, dass das System eine neue Cluster-Konfiguration übernimmt oder Sie aufgefordert werden, eine zu identifizieren.

Im Folgenden wird ein Beispiel für die Befehlsausgabe angezeigt:

```
------------------------------------------------------------------------
Aggr State                      Status              Options
aggr 0_nst_fas8080_15 online    raid_dp, aggr       root, nosnap=on
                                fast zeroed
                                64-bit
aggr0 offline                   raid_dp, aggr       diskroot
                                fast zeroed`
                                64-bit
------------------------------------------------------------------------
```

Überprüfen Sie die installation von node4

Sie müssen überprüfen, ob die physischen Ports von node2 den physischen Ports auf node4 korrekt zugeordnet sind. Dadurch kann node4 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu

erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Abhängig vom Modell der Nodes kann das physische Port-Layout variieren. Wenn der neue Node gestartet wird, versucht ONTAP, zu ermitteln, welche Ports die Cluster LIFs hosten sollten, damit es automatisch zu Quorum kommt.

Wenn die physischen Ports auf node2 nicht direkt den physischen Ports auf node4 zugeordnet werden, wird der folgende Abschnitt angezeigt Stellen Sie die Netzwerkkonfiguration auf node4 wieder her Muss zur Reparatur der Netzwerkverbindung verwendet werden.

Nachdem sie node4 installiert und gestartet haben, müssen Sie überprüfen, ob es ordnungsgemäß installiert wurde. sie müssen warten, bis node4 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen kann.

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node4 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node4 dem Quorum beigetreten ist:

   ```
   cluster show -node node4 -fields health
   ```

   Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node4 Teil desselben Clusters wie node3 ist und dass es sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Führen Sie abhängig von der ONTAP-Version auf dem zu aktualisierenden HA-Paar eine der folgenden Aktionen durch:

Lautet Ihre ONTAP Version…	Dann…
9.8 bis 9.11.1	Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören: `::> network connections listening show -vserver Cluster`
9.12.1 oder höher	Überspringen Sie diesen Schritt und gehen Sie zu Schritt 5.

   Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

4. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

   ```
   ::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
   int modify -vserver Cluster -lif cluster-lif -status-admin up
   ```

   Wiederholen Sie Schritt 3, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

5. Wechseln Sie in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

6. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand befindet, bevor node2 angehalten wurde, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

   ```
   system controller replace show

   system controller replace show-details
   ```

7. Wenn Sie auf einem MetroCluster System arbeiten, überprüfen Sie, ob der ersetzte Controller für die MetroCluster-Konfiguration ordnungsgemäß konfiguriert ist. Die MetroCluster-Konfiguration sollte sich in einem ordnungsgemäßen Zustand befinden. Siehe "Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration".

   Konfigurieren Sie die Intercluster-LIFs auf dem MetroCluster-Node node4 neu, und überprüfen Sie Cluster-Peering, um die Kommunikation zwischen den MetroCluster-Nodes wiederherzustellen, bevor Sie fortfahren mit Schritt 6.

   Überprüfen Sie den MetroCluster-Node-Status:

   ```
   metrocluster node show
   ```

8. Wiederaufnehmen des Controller-Austauschvorgangs:

   ```
   system controller replace resume
   ```

9. Der Austausch des Controllers wird anhand der folgenden Meldung unterbrochen:

```
Cluster::*> system controller replace show
Node             Status                        Error-Action
---------------- ------------------------
-----------------------------------
Node2(now node4) Paused-for-intervention      Follow the instructions
given in
                                               Step Details
Node2

Step Details:
-------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be
manually adjusted to match the new physical network configuration of the
hardware.
This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed
commands and instructions, refer to the "Re-creating VLANs, ifgrps, and
broadcast
domains" section of the upgrade controller hardware guide for the ONTAP
version
running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show"
to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement
network displaced-vlans restore" to restore the VLAN on the desired
port.
2 entries were displayed.
```

In diesem Verfahren wurde Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node4_ umbenannt.

10. Wenn der Controller-Austausch im Status „Pause“ steht, fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, um die Netzwerkkonfiguration auf dem Node wiederherzustellen.

Stellen Sie die Netzwerkkonfiguration auf node4 wieder her

Nachdem Sie bestätigt haben, dass node4 sich im Quorum befindet und mit node3 kommunizieren kann, überprüfen Sie, ob node2 VLANs, Interface Groups und Broadcast-Domains auf node4 zu sehen sind. Überprüfen Sie außerdem, ob alle node4-Netzwerkports in ihren richtigen Broadcast-Domänen konfiguriert sind.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Verknüpfen mit *Network Management*.

> Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe "NetApp Bugs Online Fehler-ID 1570339" Und den Knowledge Base Artikel "CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE" Für eine Anleitung.

Schritte

1. Listen Sie alle physischen Ports auf Upgrade-Knoten 2 (node4 genannt) auf:

   ```
   network port show -node node4
   ```

   Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. Von dieser Ausgabe aus sehen Sie alle physischen Ports, die in verschoben wurden `Cluster` Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um die Entscheidung zu erleichtern, welche Ports als Ports für Schnittstellengruppen, als VLAN-Basis-Ports oder als eigenständige physische Ports zum Hosten von LIFs verwendet werden sollten.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node4 auflisten:

   ```
   network port reachability show
   ```

   Die Ausgabe des Befehls sieht wie im folgenden Beispiel aus:

```
clusterA::*> reachability show -node node2_node4
  (network port reachability show)
Node         Port       Expected Reachability       Reachability Status
---------    --------  --------------------------
---------------------
node2_node4
             a0a        Default:Default            no-reachability
             a0a-822    Default:822                no-reachability
             a0a-823    Default:823                no-reachability
             e0M        Default:Mgmt               ok
             e0a        Cluster:Cluster            misconfigured-
reachability
             e0b        Cluster:Cluster            no-reachability
             e0c        Cluster:Cluster            no-reachability
             e0d        Cluster:Cluster            no-reachability
             e0e        Cluster:Cluster            ok
             e0e-822    -                          no-reachability
             e0e-823    -                          no-reachability
             e0f        Default:Default            no-reachability
             e0f-822    Default:822                no-reachability
             e0f-823    Default:823                no-reachability
             e0g        Default:Default            misconfigured-
reachability
             e0h        Default:Default            ok
             e0h-822    Default:822                ok
             e0h-823    Default:823                ok
18 entries were displayed.
```

Im obigen Beispiel wird node2_node4 erst nach dem Austausch des Controllers gestartet. Es verfügt über mehrere Ports, die keine Erreichbarkeit haben und eine Überprüfung der Erreichbarkeit ausstehen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node4 mit einem anderen Status als der Erreichbarkeit `ok`. Führen Sie den folgenden Befehl aus, zuerst auf beliebigen physischen Ports, dann auf beliebigen VLAN-Ports, nacheinander:

   `network port reachability repair -node` *`node_name`* `-port` *`port_name`*

   Die Ausgabe sieht wie das folgende Beispiel aus:

```
Cluster ::> reachability repair -node node2_node4 -port e0h
```

```
Warning: Repairing port "node2_node4: e0h" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Wie oben dargestellt, wird eine Warnmeldung für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Wiederachbarkeit der Broadcast-Domain unterscheiden können, wo sie sich derzeit befindet.

Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

```
network port reachability show
```

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Wenn die Konfiguration der Schnittstellengruppe nicht mit dem physischen Portlayout des neuen Controllers übereinstimmt, ändern Sie diese mit den folgenden Schritten.

   a. Sie müssen zunächst physische Ports entfernen, die als Ports für Schnittstellengruppen von ihrer Broadcast-Domain-Mitgliedschaft verwendet werden sollen. Dazu verwenden Sie den folgenden Befehl:

      ```
      network port broadcast-domain remove-ports -broadcast-domain
      broadcast_domain_name -ports node_name:port_name
      ```

   b. Hinzufügen eines Mitgliedports zu einer Schnittstellengruppe:

      ```
      network port ifgrp add-port -node node_name -ifgrp ifgrp -port port_name
      ```

   c. Die Schnittstellengruppe wird der Broadcast-Domäne automatisch ca. eine Minute nach dem Hinzufügen des ersten Mitgliedports hinzugefügt.

   d. Vergewissern Sie sich, dass die Schnittstellengruppe der entsprechenden Broadcast-Domäne hinzugefügt wurde:

      ```
      network port reachability show -node node_name -port ifgrp
      ```

      Wenn der Status der Erreichbarkeit der Schnittstellengruppe nicht lautet `ok`, Weisen Sie es der entsprechenden Broadcast-Domain zu:

```
network port broadcast-domain add-ports -broadcast-domain
broadcast_domain_name -ports node:port
```

6. Weisen Sie dem die entsprechenden physischen Ports zu `Cluster` Broadcast-Domäne:

   a. Ermitteln Sie, welche Ports eine Reachability zum haben `Cluster` Broadcast-Domäne:

      ```
      network port reachability show -reachable-broadcast-domains Cluster:Cluster
      ```

   b. Reparieren Sie jeden Port mit Erreichbarkeit zum `Cluster` Broadcast-Domäne, wenn ihr Status der Erreichbarkeit nicht lautet `ok`:

      ```
      network port reachability repair -node node_name -port port_name
      ```

7. Verschieben Sie die verbleibenden physischen Ports in ihre richtigen Broadcast-Domänen mithilfe eines der folgenden Befehle:

   `network port reachability repair -node node_name -port port_name`

   `network port broadcast-domain remove-port`

   `network port broadcast-domain add-port`

   Vergewissern Sie sich, dass keine unerreichbaren oder unerwarteten Ports vorhanden sind. Überprüfen Sie den Status der Erreichbarkeit aller physischen Ports mithilfe des folgenden Befehls und überprüfen Sie die Ausgabe, um sicherzustellen, dass der Status lautet `ok`:

   `network port reachability show -detail`

8. Stellen Sie alle VLANs wieder her, die möglicherweise verschoben wurden, indem Sie die folgenden Schritte ausführen:

   a. Versetzte VLANs auflisten:

      `cluster controller-replacement network displaced-vlans show`

      Die Ausgabe sollte wie folgt angezeigt werden:

      ```
      Cluster::*> displaced-vlans show
      (cluster controller-replacement network displaced-vlans show)
                  Original
      Node        Base Port     VLANs
      ---------   ---------
      ------------------------------------------------------
      Node1       a0a           822, 823
                  e0e           822, 823
      ```

   b. Stellen Sie VLANs wieder her, die von ihren früheren Basis-Ports verdrängt wurden:

      `cluster controller-replacement network displaced-vlans restore`

      Das folgende Beispiel zeigt die Wiederherstellung von VLANs, die aus der Schnittstellengruppe a0a wieder in dieselbe Schnittstellengruppe verschoben wurden:

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
      -destination-port a0a
      ```

      Das folgende Beispiel zeigt die Wiederherstellung von verlagerten VLANs am Port „e0e“ auf „e0h“:

      ```
      Cluster::*> displaced-vlans restore -node node2_node4 -port e0e
      -destination-port e0h
      ```

Wenn eine VLAN-Wiederherstellung erfolgreich ist, werden die verschobenen VLANs auf dem angegebenen Zielport erstellt. Die VLAN-Wiederherstellung schlägt fehl, wenn der Zielport Mitglied einer Schnittstellengruppe ist oder der Zielport nicht verfügbar ist.

Warten Sie etwa eine Minute, bis neu wiederhergestellte VLANs in ihren entsprechenden Broadcast-Domänen platziert werden.

a. Erstellen Sie bei Bedarf neue VLAN-Ports für VLAN-Ports, die nicht im enthalten sind `cluster controller-replacement network displaced-vlans show` Ausgabe sollte aber auf anderen physischen Ports konfiguriert werden.

9. Löschen Sie alle leeren Broadcast-Domänen, nachdem alle Port-Reparaturen abgeschlossen wurden:

   `network port broadcast-domain delete -broadcast-domain` *`broadcast_domain_name`*

10. Überprüfen der Port-Erreichbarkeit:

    `network port reachability show`

    Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn Ports einen anderen Status als diese beiden melden, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in Schritt 4.

11. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

    `network port show`

12. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

    `network port broadcast-domain show`

13. Stellen Sie die LIF-Start-Ports wieder her und geben Sie ggf. den Vserver(s) und die Home Ports der logischen Schnittstelle an, die wiederhergestellt werden müssen:

    a. Führen Sie alle vertriebenen LIFs auf:

       `displaced-interface show`

    b. LIF-Startports wiederherstellen:

       `displaced-interface restore-home-node -node` *`node_name`* `-vserver` *`vserver_name`* `-lif-name` *`LIF_name`*

14. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

    `network interface show -fields home-port, status-admin`

Wiederherstellen der Key-Manager-Konfiguration auf node4

Wenn Sie mithilfe von NetApp Volume Encryption (NVE) und NetApp Aggregate

Encryption (NAE) Volumes auf dem System verschlüsseln, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht synchronisieren, können beim Verschieben der Node2-Aggregate mit ARL Fehler auftreten, da node4 nicht über die erforderlichen Schlüssel verfügt, um verschlüsselte Volumes und Aggregate online zu bringen.

Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

Schritte

1. Führen Sie folgenden Befehl aus node4 aus:

   ```
   security key-manager onboard sync
   ```

2. Vergewissern Sie sich, dass der SVM-KEK-Schlüssel auf node4 als „true“ wiederhergestellt wurde, bevor Sie die Datenaggregate verschieben:

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK
   ```

   Beispiel

   ```
   ::> security key-manager key query -node node4 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node4    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4

Nachdem Sie die Netzwerkkonfiguration auf node4 überprüft und bevor Sie Aggregate von node3 auf node4 verschieben, müssen Sie überprüfen, ob die NAS-Daten-LIFs, die zu node2 gehören und sich derzeit auf node3 befinden, von node3 nach node4 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node4 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die

LIFs ordnungsgemäß sind und sich in den entsprechenden Ports befinden, nachdem Sie node4 in den Online-Modus versetzt haben.

> Wenn Sie die Portgeschwindigkeit der T6-basierten Ethernet-Netzwerkkarten oder Motherboard-Ports ändern, können Sie nach der Geschwindigkeitskonvertierung fehlerhafte Pakete beobachten. Siehe "NetApp Bugs Online Fehler-ID 1570339" Und den Knowledge Base Artikel "CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE" Für eine Anleitung.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   `system controller replace resume`

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Wiederaufnahme des Betriebs der Versetzung:

   `system controller replace resume`

   Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen werden die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, an den neuen Controller node4 verschoben. Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

3. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

   Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

4. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

   `cluster controller-replacement network displaced-interface show`

   Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in node4 wieder her:

   `cluster controller-replacement network displaced-interface restore-home-node`

5. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

```
system controller replace resume
```

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung
- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster
- Lautstärkerprüfung

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

MetroCluster FC-Konfiguration

In einer MetroCluster FC-Konfiguration müssen die Knoten für Disaster Recovery/Failover-Standort so schnell wie möglich ersetzt werden. Nicht übereinstimmende Controller-Modelle in einem MetroCluster wird nicht unterstützt, weil eine falsche Übereinstimmung des Controller-Modells dazu führen kann, dass Disaster Recovery-Spiegelung offline geht. Umgehen Sie MetroCluster-Überprüfungen mit dem `-skip -metrocluster-check true` Befehl, wenn Sie Nodes am zweiten Standort ersetzen.

Authentifizierungsmanagement mit KMIP-Servern

Mit ONTAP 9.8 oder höher können KMIP-Server (Key Management Interoperability Protocol) Authentifizierungsschlüssel managen.

Schritte

1. Hinzufügen eines neuen Controllers:

```
security key-manager external enable
```

2. Fügen Sie den Schlüsselmanager hinzu:

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um das korrekte Setup zu bestätigen, müssen Sie das HA-Paar aktivieren. Sie müssen außerdem überprüfen, dass Node3 und node4 auf den Storage der jeweils anderen Person zugreifen können und dass keine der logischen Datenschnittstellen zu anderen Nodes im Cluster vorhanden sind. Darüber hinaus müssen Sie bestätigen, dass Node3 zu Aggregaten node1 gehört und dass node4 die Aggregate von node2 besitzt und dass die Volumes für beide Nodes online sind.

Schritte

1. Nach den Tests nach der Prüfung von „node2“ werden das Storage Failover und das Cluster HA-Paar für den node2 Cluster aktiviert. Nach Abschluss des Vorgangs werden beide Nodes als abgeschlossen angezeigt, und das System führt einige Bereinigungsvorgänge aus.
2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   ```
   storage failover show
   ```

   Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

   ```
   cluster::> storage failover show
                       Takeover
   Node     Partner  Possible   State Description
   -------- -----    -------    ------------------
   node3    node4    true       Connected to node4
   node4    node3    true       Connected to node3
   ```

3. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

   ```
   cluster show
   ```

4. Stellen Sie sicher, dass node3 und node4 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

```
storage failover show -fields local-missing-disks, partner-missing-disks
```

5. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn keine der Knoten „Node3“ oder „node4“ Daten-LIFs besitzt, die sich im Besitz anderer Nodes im Cluster befinden, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

   ```
   network interface revert
   ```

6. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

   ```
   storage aggregate show -owner-name node3
   ```

   ```
   storage aggregate show -owner-name node4
   ```

7. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node node3 -state offline
   ```

   ```
   volume show -node node4 -state offline
   ```

8. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie im Abschnitt erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor", Und Online-Laufwerk eines der Offline-Volumes, nach Bedarf, durch Verwendung des folgenden Befehls, einmal für jedes Volume:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

9. Installieren Sie neue Lizenzen für die neuen Nodes mithilfe des folgenden Befehls für jeden Node:

   ```
   system license add -license-code license_code,license_code,license_code…
   ```

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

10. Entfernen Sie alle alten Lizenzen mithilfe eines der folgenden Befehle von den ursprünglichen Nodes:

    ```
    system license clean-up -unused -expired
    ```

    ```
    system license delete -serial-number node_serial_number -package
    licensable_package
    ```

    - Alle abgelaufenen Lizenzen löschen:

      ```
      system license clean-up -expired
      ```

    - Alle nicht verwendeten Lizenzen löschen:

      ```
      system license clean-up -unused
      ```

◦ Löschen Sie eine bestimmte Lizenz von einem Cluster mit den folgenden Befehlen auf den Nodes:

```
system license delete -serial-number node1_serial_number -package *

system license delete -serial-number node2_serial_number -package *
```

Die folgende Ausgabe wird angezeigt:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

Eingabe `y` Um alle Pakete zu entfernen.

11. Überprüfen Sie, ob die Lizenzen korrekt installiert sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

    ```
    system license show
    ```

    Sie können die Ausgabe mit der im Abschnitt erfassten Ausgabe vergleichen "Bereiten Sie die Knoten für ein Upgrade vor".

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie die eingestellt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel in "installieren und booten sie node4, Schritt 27"), Sie müssen die Einstellung der Variable aufheben:

    ```
    set diag; systemshell -node node_name -command sudo kenv -u -p
    kmip.init.maxwait
    ```

13. Konfigurieren Sie die SPs mit dem folgenden Befehl auf beiden Knoten:

    ```
    system service-processor network modify -node node_name
    ```

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen *ONTAP 9.8: Manual Page Reference* für detaillierte Informationen zum System `service-processor network modify` Befehl.

14. Informationen zum Einrichten eines Clusters ohne Switches auf den neuen Nodes finden Sie unter "Quellen" Um eine Verbindung zur NetApp Support Site_ zu erhalten, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node3 und node4 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von

Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore -node new_controller_name
   ```

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Onboard Key Manager

Konfigurieren Sie NVE oder NAE mit dem Onboard Key Manager.

Schritte

1. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager onboard sync
   ```

Externes Verschlüsselungsmanagement

Konfigurieren Sie NVE oder NAE mit externem Verschlüsselungsmanagement.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

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

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager external enable
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager external restore
   ```

   Für diesen Befehl ist die OKM-Passphrase erforderlich

Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder EKM-Server nicht erreicht werden konnten. Stellen Sie diese Volumes mithilfe der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "Überblick über das ARL Upgrade". Informationen über mögliche Ausfälle werden in der Phase des Verfahrens aufgelistet.

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   ```
   storage aggregate relocation show
   ```

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9.8: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 waren, gehören node4 nach Abschluss des Upgrades

Beim Abschluss des Upgrade-Verfahrens sollte die Knoten3 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node die Knoten1 hatten. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Unter den folgenden Umständen kann es nicht gelingen, Aggregate ordnungsgemäß zu verschieben und Node 1 als Home Node anstelle von Knoten3 zu verwenden:

- In Phase 3, wenn Aggregate von node2 auf node3 verschoben werden. Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann wird das Aggregat auf node2 zurückgelassen.
- Nach Stufe 4, wenn node2 durch node4 ersetzt wird. Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node4 als Home-Node statt node3 online.

Sie können das falsche Eigentümerproblem nach Phase 6 beheben, wenn ein Storage-Failover aktiviert wurde, indem Sie die folgenden Schritte durchführen:

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Liste der Aggregate zu erhalten:

   `storage aggregate show -nodes node4 -is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 mit der Ausgabe, die Sie für Knoten 1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links auf node4:

   `storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3`

   Verwenden Sie das nicht `-ndo-controller-upgrade` Parameter während dieser Verschiebung.

4. Vergewissern Sie sich, dass node3 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht über Node3 als Hausbesitzer verfügen, können mit dem gleichen Relocation-Befehl in auf node3 verschoben werden Schritt 3.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, in Panik geraten oder aus- und wieder eingeschaltet werden.

Die Lösung dieser Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikzugänge oder Energiezyklen während der Vorprüfphase

Node1 oder node2 stürzt vor der Pre-Check-Phase ab, während das HA-Paar noch aktiviert ist

Wenn node1 oder node2 vor der Pre-Check-Phase abstürzt, wurden noch keine Aggregate verschoben und die HA-Paar-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzugänge oder Energiezyklen während der ersten Ressourcenfreigabephase

Node1 stürzt während der ersten Resource-Release-Phase ab, während das HA-Paar noch aktiviert ist

Einige oder alle Aggregate wurden von node1 in node2 verschoben und das HA-Paar ist noch aktiviert. Node2 übernimmt das Root-Volume von node1 und alle nicht-Root-Aggregate, die nicht verschoben wurden.

Über diese Aufgabe

Eigentum an Aggregaten, die verschoben wurden, sehen genauso aus wie das Eigentum von nicht-Root-Aggregaten, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat.

Wenn node1 in den eintritt `waiting for giveback` Status, node2 gibt alle node1 nicht-Root-Aggregate zurück.

Schritte

1. Nachdem node1 gestartet wurde, sind alle nicht-Root-Aggregate von node1 zurück in node1 verschoben. Sie müssen eine manuelle Aggregatverschiebung der Aggregate von node1 nach node2 durchführen: `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während der ersten Ressourcen-Release-Phase ab, während das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 schlägt während der ersten Phase der Ressourcenfreigabe fehl, während das HA-Paar noch aktiviert ist

Node1 hat einige oder alle seine Aggregate in node2 verschoben. Das HA-Paar ist aktiviert.

Über diese Aufgabe

Node1 übernimmt alle node2 Aggregate sowie jedes seiner eigenen Aggregate, die auf node2 verschoben wurden. Beim Booten von node2 wird die Aggregatverschiebung automatisch abgeschlossen.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während der ersten Resource-Release-Phase ab und nachdem HA-Paar deaktiviert ist

Node1 übernimmt nicht.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem verbleibenden Upgrade des Node-Paars fort.

Startet während der ersten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node2 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

Node3 übernimmt nach einem Absturz nach einem node2 nicht, da das HA-Paar bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt in der ersten Verifizierungsphase ab, wobei das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der ersten Ressourcen-Wiederholen-Phase

Knoten 2 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Node2 hat einige oder alle seine Aggregate von node1 in node3 verschoben. Node3 stellt Daten von Aggregaten bereit, die verlagert wurden. Das HA-Paar ist deaktiviert und somit gibt es keine Übernahme.

Über diese Aufgabe

Es gibt einen Client-Ausfall für Aggregate, die nicht verschoben wurden. Beim Booten von node2 werden die Aggregate von node1 auf node3 verschoben.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während der ersten Phase zur Ressourcenrückgewinnung während der Aggregatverschiebung ab

Falls node3 abstürzt, während node2 Aggregate zu node3 verschoben wird, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Knoten 3 verlagert wurden, begegnen ein Client-Ausfall, während node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Führen Sie das Controller-Upgrade fort.

Neustarts, Panikspiele oder Energiezyklen während der Nachprüfphase

Node2 oder node3 stürzt während der Post-Check-Phase ab

Das HA-Paar ist deaktiviert, damit dies keine Übernahme ist. Es gibt einen Client-Ausfall für Aggregate, die zum neu gebooteten Node gehören.

Schritte

1. Bringen Sie den Node hoch.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der zweiten Ressourcenfreigabephase

Node3 stürzt während der zweiten Resource-Release-Phase ab

Wenn node3 abstürzt, während node2 Aggregate verschoben, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Node3 verlagert wurden, und Node3 eigene Aggregate stoßen auf Client-Ausfälle, während Node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Node2 stürzt während der zweiten Resource-Release-Phase ab

Wenn node2 während der Aggregatverschiebung abstürzt, wird node2 nicht übernommen.

Über diese Aufgabe

Node3 dient weiterhin den Aggregaten, die verschoben wurden, doch die Aggregate von node2 stoßen auf Client-Ausfälle.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Startet während der zweiten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node3 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node3 abstürzt, wird die Übernahme nicht ausgeführt, da das HA-Paar bereits

deaktiviert ist.

Über diese Aufgabe

Es gibt einen Client-Ausfall für alle Aggregate, bis node3 neu startet.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node4 stürzt während der zweiten Verifikationsphase ab

Wenn node4 während dieser Phase abstürzt, wird die Übernahme nicht durchgeführt. Node3 stellt Daten aus den Aggregaten bereit.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis node4 neu startet.

Schritte

1. bringen sie node4 auf.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------   --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder

Panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
--------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports lautet `down`.

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.

Inhalt	Beschreibung
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.

Inhalt	Beschreibung
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe", Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.

Verwenden Sie „System Controller replace“-Befehle, um ein Upgrade der Controller-Hardware mit ONTAP 9.5 auf 9.7 durchzuführen

Überblick

Dieses Verfahren beschreibt das Upgrade der Controller-Hardware mithilfe von Aggregate Relocation (ARL) für die folgenden Systemkonfigurationen:

Methode	ONTAP-Version	Unterstützte Systeme
Wird Verwendet `system controller replace` Befehle	9.5 bis 9.7	"Link zur unterstützten Systemmatrix"

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Außerdem migrieren Sie Daten-logische Schnittstellen (LIFs) und weisen Sie die Netzwerk-Ports auf dem neuen Controller den Schnittstellengruppen zu, während Sie fortfahren.

In diesen Informationen verwendete Terminologie

In dieser Information werden die ursprünglichen Knoten „node1“ und „node2“ genannt und die neuen Knoten „node3“ und „node4“ genannt. Während des beschriebenen Verfahrens wird "node1" durch "node3" ersetzt und "node2" durch "node4" ersetzt.

Die Begriffe "node1", "node2", "node3" und "node4" werden nur verwendet, um zwischen den ursprünglichen und den neuen Knoten zu unterscheiden. Wenn Sie das Verfahren befolgen, müssen Sie die richtigen Namen Ihrer ursprünglichen und neuen Knoten ersetzen. In der Realität ändern sich die Namen der Knoten jedoch nicht: „node3“ hat den gleichen Namen wie „node1“ und „node4“ hat nach dem Upgrade der Controller-Hardware den gleichen Namen wie „node2“.

Während dieser Informationen bezieht sich der Begriff „Systeme mit FlexArray-Virtualisierungssoftware“ auf Systeme, die zu diesen neuen Plattformen gehören. Der Begriff „V-Series System“ bezieht sich auf getrennte Hardwaresysteme, die an Storage Arrays angeschlossen werden können.

Wichtige Informationen:

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie müssen auch lesen und verstehen "Richtlinien für das Controller-Upgrade mit ARL" Und das "Überblick über das ARL Upgrade" Vor Beginn des Upgrades.
- Bei dieser Vorgehensweise wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht

verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn bereits die Ersatz-Controller-Hardware verwendet wurde, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP in 7-Mode ausgeführt wurde.

- Sie können dieses Verfahren zum Upgrade der Controller Hardware in Clustern mit mehr als zwei Nodes verwenden. Sie müssen jedoch die Verfahren für jedes HA-Paar im Cluster separat durchführen.
- Dieses Verfahren gilt für FAS Systeme, V-Series Systeme, AFF Systeme und Systeme mit FlexArray Virtualisierungssoftware. FAS Systeme, die nach ONTAP 9.5 freigegeben wurden, können an Speicher-Arrays angebunden werden, wenn die erforderliche Lizenz installiert ist. Die vorhandenen Systeme der V-Serie werden von ONTAP 9.5 unterstützt. Weitere Informationen zu den Modellen Storage Array und V-Series finden Sie unter "Quellen" Zu verlinken auf „Hardware Universe_“ und „V-Series Supportmatrix“.
- Ab ONTAP 9.6 gilt dieses Verfahren für Systeme mit MetroCluster-Konfiguration mit 4 Nodes oder höher. Da sich die MetroCluster-Konfigurationsstandorte an zwei physisch unterschiedlichen Standorten befinden können, muss das automatisierte Controller-Upgrade für ein HA-Paar individuell an jedem MetroCluster Standort durchgeführt werden.
- Wenn Sie ein Upgrade von einem AFF A320 System durchführen, können Sie das Upgrade der Controller-Hardware durch Volume-Verschiebung durchführen oder den technischen Support kontaktieren. Wenn Sie bereit sind, die Lautstärke zu verschieben, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Automatisierung des Controller-Upgrades

Während eines Controller-Upgrades wird der Controller durch einen anderen Controller ersetzt, auf dem eine neuere oder leistungsstärkere Plattform läuft.

In früheren Versionen dieses Inhalts enthielten Anweisungen für einen unterbrechungsfreien Controller-Update, der vollständig manuell ausgeführt wurde. Dieser Inhalt enthält die Schritte für das neue automatisierte Verfahren.

Der manuelle Prozess war langwierig und komplex, aber in diesem vereinfachten Verfahren können Sie ein Controller-Update mithilfe von Aggregatverschiebung implementieren, sodass effizientere, unterbrechungsfreie Upgrades für HA-Paare möglich sind. Vor allem in Bezug auf Validierung, Sammlung von Informationen und Nachprüfungen sind deutlich weniger manuelle Schritte erforderlich.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

In diesem Inhalt wird beschrieben, wie Sie die Storage Controller in einem HA-Paar mit neuen Controllern aktualisieren und dabei alle vorhandenen Daten und Festplatten beibehalten. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Verwenden Sie diese Inhalte unter folgenden Umständen:

- Sie aktualisieren gerade NetApp Controller mit ONTAP 9.5, 9.6 oder 9.7. Dieses Dokument gilt nicht für ein Upgrade auf ONTAP 9.8.
- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind in der Verwaltung von ONTAP erfahren und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.

- Wenn Sie eine MetroCluster Konfiguration aktualisieren, handelt es sich um eine FC-Konfiguration mit 4 oder mehr Nodes und auf allen Nodes wird ONTAP 9.6 oder 9.7 ausgeführt.

Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

die folgenden Tabellen zeigen die unterstützte Modellmatrix für das Controller-Upgrade.

Alter Controller	Ersatz-Controller
FAS8020, FAS8040, FAS8060, FAS8080	FAS8200, FAS8300, FAS8700, FAS9000
AFF8020, AFF8040, AFF8060, AFF8080	AFF A300, AFF A400, AFF A700[1], AFF A800[2]
FAS8200	FAS8700, FAS9000, FAS8300[4, 5]
AFF A300	AFF A700[1], AFF A800[2, 3], AFF A400[4, 5]

Wenn die Kombination aus dem Controller-Upgrade-Modell nicht in der oben stehenden Tabelle aufgeführt ist, wenden Sie sich an den technischen Support.

Das automatisierte Upgrade [1]ARL für das AFF A700 System wird von ONTAP 9.7P2 unterstützt.

[2]bei einem Update auf eine AFF A800 oder ein System, das interne und externe Festplatten unterstützt, müssen Sie spezifische Anweisungen für das Root-Aggregat auf internen NVMe-Festplatten befolgen. Siehe "UTA/UTA2-Ports in node3, Schritt 14, prüfen und konfigurieren" Und "UTA/UTA2-Ports in node4, Schritt 14, prüfen und konfigurieren".

Das automatisierte Upgrade [3]ARL von einer AFF A300 auf ein AFF A800 System wird von ONTAP 9.7P5 unterstützt.

Das automatisierte Upgrade [4]ARL von einer AFF A300 auf eine AFF A400 und eine FAS8200 zu einem FAS8300 System wird von ONTAP 9.7P8 unterstützt.

[5]Wenn Sie in einer 2-Node-Cluster-Konfiguration ein Upgrade von einer AFF A300 auf eine AFF A400 oder ein FAS8200 auf ein FAS8300 System durchführen, müssen Sie für das Controller-Upgrade temporäre Cluster-Ports auswählen. Die AFF A400- und FAS8300-Systeme sind in zwei Konfigurationen erhältlich – als Ethernet-Bundle, bei dem die Ports der Mezzanine-Karte Ethernet-Typ und als FC-Bundle enthalten sind. Dort befinden sich die Mezzanine-Ports vom FC-Typ.

- Bei einer AFF A400 oder einer FAS8300 mit Ethernet-Konfiguration können Sie jeden der beiden Mezzanine-Ports als temporäre Cluster-Ports verwenden.
- Bei einer AFF A400 oder einem FAS8300 mit FC-Typ-Konfiguration müssen Sie eine 10-GbE-Netzwerkschnittstellenkarte mit vier Ports (Teilenummer X1147A) hinzufügen, um temporäre Cluster Ports bereitstellen zu können.
- Nach Abschluss eines Controller-Upgrades mithilfe von temporären Cluster-Ports können Sie Cluster-LIFs unterbrechungsfrei zu e3a und e3b migrieren, 100-GbE-Ports auf einem AFF A400 System sowie e0c und e0d, 100-GbE-Ports auf einem FAS8300 System.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu

ONTAP 9 zugreifen können.

Die erforderlichen Tools und Dokumentationen

Sie müssen über spezielle Tools verfügen, um die neue Hardware zu installieren, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren.

Für die Durchführung des Upgrades benötigen Sie die folgenden Tools:

- Erdungsband
- #2 Kreuzschlitzschraubendreher

Wechseln Sie zum "Quellen" Abschnitt für den Zugriff auf die Liste der für dieses Upgrade erforderlichen Referenzdokumente und Referenzsites

Richtlinien für das Controller-Upgrade mit ARL

Um zu verstehen, ob Sie bei einem Controller-Upgrade von ONTAP 9.5 auf ONTAP 9.7 mit Aggregate Relocation (ARL) arbeiten können, hängt von der Plattform und der Konfiguration der ursprünglichen Controller sowie von dem Ersatz-Controller ab.

Unterstützte Upgrades für ARL

Wenn Sie ein Node-Paar mit diesem ARL-Verfahren für ONTAP 9.5 auf ONTAP 9.7 aktualisieren, müssen Sie sicherstellen, dass ARL an den Original- und Ersatz-Controllern ausgeführt werden kann.

Sie sollten die Größe aller definierten Aggregate und die Anzahl der Festplatten überprüfen, die vom ursprünglichen System unterstützt werden. Dann müssen Sie die Aggregatgröße und Anzahl der unterstützten Festplatten mit der Aggregatgröße und der Anzahl der vom neuen System unterstützten Festplatten vergleichen. Siehe "Quellen" Link zum *Hardware Universe*, wo diese Information verfügbar ist. Die Aggregatgröße und die Anzahl der vom neuen System unterstützten Festplatten müssen gleich oder größer sein als die Aggregatgröße und Anzahl der vom ursprünglichen System unterstützten Festplatten.

Sie sollten in den Cluster-Mischregeln validieren, ob neue Nodes zusammen mit den vorhandenen Nodes in das Cluster integriert werden können, wenn der ursprüngliche Controller ersetzt wird. Weitere Informationen zu Regeln für die Kombination von Clustern finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

Bevor Sie ein AFF-Systemupgrade durchführen, müssen Sie ONTAP auf Version 9.5P1 oder neuer aktualisieren. Diese Versionsebenen sind für ein erfolgreiches Upgrade erforderlich.

Informationen zum Upgrade eines Systems, das interne Laufwerke unterstützt (z. B. eine FAS2700 oder AFF A250), aber KEINE internen Laufwerke enthält, finden Sie unter "Quellen" Und verwenden Sie das Verfahren in der *Aggregate Relocation, um den für Ihre Version von ONTAP korrekten Controller-Hardware*-Inhalt manuell zu aktualisieren.

Wenn Sie ONTAP 9.6P11, 9.7P8 oder neuere Versionen verwenden, wird empfohlen, die Aktivierung von Connectivity, Lebendigkeit und Availability Monitor (CLAM)-Übernahme zu aktivieren, um das Cluster bei bestimmten Node-Ausfällen in Quorum zurückzugeben. Der `kernel-service` Für Befehl ist der erweiterte Zugriff auf die Berechtigungsebene erforderlich. Weitere Informationen finden Sie unter: "NetApp KB-Artikel SU436: DIE CLAM-Übernahme hat sich die Standardkonfiguration geändert".

Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise undSnapLock Compliance Volumes konfiguriert sind.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren.

Upgrades werden für ARL nicht unterstützt

Sie können die folgenden Aktualisierungen nicht ausführen:

- Zum Austausch von Controllern, die die mit den ursprünglichen Controllern verbundenen Platten-Shelfs nicht unterstützen

  Siehe "Quellen" Um Informationen zur Hardware Universe Festplattenunterstützung zu erhalten.

- Um Controller der Einstiegsklasse mit internen Laufwerken zu erhalten, beispielsweise eine FAS 2500.

  Informationen zum Upgrade von Controllern der Einstiegsklasse mit internen Laufwerken finden Sie unter "Quellen" Link zu *Upgrade durch Verschiebung von Volumes oder Storage* und Vorgang *Upgrade eines Node-Paares, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.

Fehlerbehebung

Falls beim Upgrade der Controller Probleme auftreten, finden Sie weitere Informationen im "Fehlerbehebung" Abschnitt am Ende des Verfahrens für weitere Informationen und mögliche Lösungen.

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Bevor Sie ein Upgrade auf einer Fabric-MetroCluster-Konfiguration starten, müssen Sie den Zustand der MetroCluster-Konfiguration überprüfen, um den ordnungsgemäßen Betrieb sicherzustellen.

Schritte

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

   `metrocluster check run`

   ```
   dpgqa-mcc-funct-8040-0403_siteA::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

2. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ergebnisse anzeigen:

   `metrocluster check show`

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
metrocluster_siteA::*> metrocluster check show
Last Checked On: 4/7/2019 21:15:05
Component            Result
---------------      -------
nodes                ok
lifs                 ok
config-replication   ok
aggregates           warning
clusters             ok
connections          not-applicable
volumes              ok
7 entries were displayed.
```

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

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

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

   ```
   system health alert show
   ```

Prüfen Sie auf MetroCluster-Konfigurationsfehler

Sie können das Active IQ Config Advisor Tool auf der NetApp Support-Website verwenden, um häufige Konfigurationsfehler zu überprüfen.

Wenn Sie keine MetroCluster-Konfiguration haben, können Sie diesen Abschnitt überspringen.

Über diese Aufgabe

Active IQ 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.

1. Laden Sie die herunter "Active IQ Config Advisor" Werkzeug.
2. Führen Sie Active IQ Config Advisor aus, überprüfen Sie die Ausgabe und folgen Sie seinen Empfehlungen, um eventuelle Probleme zu beheben.

Überprüfung von UmschalttaFunktionen, Healing und Switchback

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

Siehe "Quellen" Verbinden mit Inhalten für *MetroCluster Management and Disaster Recovery* und Verwenden der genannten Verfahren für ausgehandelte Umschaltung, Heilung und Umschalten.

Überblick über das ARL Upgrade

Bevor Sie die Nodes mit ARL aktualisieren, sollten Sie unbedingt verstehen, wie das Verfahren funktioniert. In diesem Inhalt wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und dann für die ursprünglichen und die neuen Nodes eine Reihe von Schritten ausführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Schritte
"Stufe 1: Bereiten Sie sich auf das Upgrade vor"	In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Sie müssen bestimmte Informationen aufzeichnen, wenn Sie Storage-Verschlüsselung mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate. • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate.
"Stufe 2: Knoten1 verschieben und ausmustern"	Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie müssen die erforderlichen Node1-Informationen für die spätere Verwendung im Verfahren notieren und dann Node1 ausmustern. Sie können sich auch später beim Verfahren auf den Netzboot node3 und node4 vorbereiten. Gesamteigentum am Ende von Phase 2: • Node2 ist der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.

Stufe	Schritte
"Phase 3: Installieren und booten Sie node3"	In Phase 3 installieren und booten Sie node3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu und überprüfen die Installation node3. Wenn erforderlich, legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest und bestätigen, dass node3 Quorum beigetreten ist. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind. Gesamteigentum am Ende von Stufe 3: • Node3 ist der Hausbesitzer und der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 4: Knoten2 verschieben und ausmustern"	Während Phase 4 werden node2-Aggregate ohne Root-Root-Fehler und logische Daten-LIFs außerhalb des SAN in Knoten 3 verschoben. Sie notieren auch die notwendigen node2 Informationen und setzen dann node2 in den Ruhestand. Gesamteigentum am Ende von Stufe 4: • Node3 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehörten. • Node2 ist der Hausbesitzer von node2 Aggregaten. • Node3 ist der aktuelle Besitzer von node2 Aggregaten.
"Phase 5: installieren und booten sie node4"	In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 nach node4 zu und überprüfen die Installation von node4. Wenn erforderlich, legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest und bestätigen, dass node4 Quorum beigetreten ist. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind. Gesamteigentum am Ende von Stufe 5: • Node3 ist der Hausbesitzer und aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Node4 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Phase 6: Schließen Sie das Upgrade ab"	In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 führen Sie Vorabprüfungen durch und korrigieren, falls erforderlich, die Eigentümerschaft für die Aggregate. Außerdem zeichnen Sie bestimmte Informationen

auf, wenn Sie Storage-Verschlüsselung mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten.

Schritte

1. "Bereiten Sie die Knoten für ein Upgrade vor"
2. "Management der Storage-Verschlüsselung mit dem Onboard Key Manager"

Bereiten Sie die Knoten für ein Upgrade vor

Der Prozess des Controller-Austauschs beginnt mit einer Reihe von Vorabprüfungen. Sie sammeln auch Informationen über die ursprünglichen Nodes, die Sie später verwenden können. Falls erforderlich, ermitteln Sie den Typ der verwendeten Self-Encrypting Drives.

Schritte

1. Starten Sie den Controller-Ersatzprozess, indem Sie den folgenden Befehl in die ONTAP-Befehlszeile eingeben:

   `system controller replace start -nodes node_names`

   Dieser Befehl kann nur auf der erweiterten Berechtigungsebene ausgeführt werden: `set -privilege advanced`

   Sie sehen die folgende Ausgabe:

   ```
   Warning:
   1. Current ONTAP version is 9.x
   Before starting controller replacement operation, ensure that the new
   controllers are running the version 9.x

   2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
   and charge them if they are not. You need to physically check the new
   nodes to see if the NVMEM or NVRAM  batteries are charged. You can check
   the battery status either by connecting to a serial console or using
   SSH, logging into the Service Processor (SP) or Baseboard Management
   Controller (BMC) for your system, and use the system sensors to see if
   the battery has a sufficient charge.

   Attention: Do not try to clear the NVRAM contents. If there is a need to
   clear the contents of NVRAM, contact NetApp technical support.

   3. If a controller was previously part of a different cluster, run
   wipeconfig before using it as the replacement controller.

   Do you want to continue? {y|n}: y
   ```

2. Drücken Sie `y`, Sie sehen die folgende Ausgabe:

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

Das System führt die folgenden Vorabprüfungen durch. Notieren Sie die Ausgabe jeder Vorabprüfung zur Verwendung im weiteren Verlauf des Verfahrens:

Pre-Check	Beschreibung
Cluster-Integritätsprüfung	Überprüft alle Nodes im Cluster, um sicherzustellen, dass sie sich in einem ordnungsgemäßen Zustand befinden.
MCC Cluster Check	Überprüft, ob es sich bei dem System um eine MetroCluster-Konfiguration handelt. Der Vorgang erkennt automatisch, ob es sich um eine MetroCluster Konfiguration handelt oder nicht, und führt die spezifischen Vorabprüfungen und Verifizierungsüberprüfungen durch. Es wird nur eine MetroCluster FC-Konfiguration mit 4 Nodes unterstützt. Bei 2-Node-MetroCluster-Konfiguration und 4-Node-MetroCluster IP-Konfiguration schlägt die Prüfung fehl. Wenn die MetroCluster-Konfiguration im Umschaltzustand ist, schlägt die Prüfung fehl.
Statusprüfung Der Aggregatverschiebung	Überprüft, ob eine Aggregatverschiebung bereits erfolgt. Wenn eine weitere Aggregatverschiebung erfolgt, schlägt die Prüfung fehl.
Modellname Prüfen	Überprüft, ob die Controller-Modelle bei diesem Verfahren unterstützt werden. Wenn die Modelle nicht unterstützt werden, schlägt die Aufgabe fehl.
Cluster-Quorum-Prüfung	Überprüft, ob die zu ersetzenden Nodes sich in Quorum befinden. Wenn sich die Knoten nicht im Quorum befinden, schlägt die Aufgabe fehl.
Überprüfung Der Bildversion	Überprüft, ob die zu ersetzenden Nodes dieselbe Version von ONTAP ausführen. Wenn sich die ONTAP-Image-Versionen unterscheiden, schlägt die Aufgabe fehl. Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version von ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation als Netzboot einsetzen. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.
HA-Statusüberprüfung	Überprüft, ob beide Nodes, die ersetzt werden, in einer HA-Paar-Konfiguration mit Hochverfügbarkeit vorhanden sind. Wenn das Speicher-Failover für die Controller nicht aktiviert ist, schlägt die Aufgabe fehl.
Aggregatstatus-Prüfung	Wenn die Nodes ersetzt werden, eigene Aggregate, für die sie nicht der Home-Inhaber sind, schlägt die Aufgabe fehl. Die Nodes sollten nicht im Besitz von nicht lokalen Aggregaten sein.
Überprüfung Des Festplattenstatus	Wenn zu ersetzende Knoten keine oder fehlerhafte Festplatten haben, schlägt die Aufgabe fehl. Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.

Pre-Check	Beschreibung
LIF-Statusüberprüfung von Daten	Überprüft, ob für einen der zu ersetzenden Nodes keine lokalen Daten-LIFs vorhanden sind. Die Nodes sollten keine Daten-LIFs enthalten, für die sie nicht der Home-Inhaber sind. Wenn einer der Nodes nicht-lokale Daten-LIFs enthält, schlägt die Aufgabe fehl.
LIF-Status des Clusters	Überprüft, ob die Cluster-LIFs für beide Nodes aktiv sind. Wenn die Cluster-LIFs ausgefallen sind, schlägt die Aufgabe fehl.
ASUP-Statusprüfung	Wenn ASUP Benachrichtigungen nicht konfiguriert sind, schlägt die Aufgabe fehl. Sie müssen AutoSupport aktivieren, bevor Sie mit dem Austausch des Controllers beginnen.
CPU-Auslastungs-Prüfung	Überprüft, ob die CPU-Auslastung bei allen zu ersetzenden Nodes mehr als 50 % beträgt. Wenn die CPU-Nutzung über einen erheblichen Zeitraum mehr als 50 % beträgt, schlägt die Aufgabe fehl.
Aggregatrekonstruktion	Überprüft, ob bei beliebigen Datenaggregaten eine Rekonstruktion durchgeführt wird. Wenn die Aggregatrekonstruktion ausgeführt wird, schlägt die Aufgabe fehl.
Knoten Affinität Job Überprüfung	Überprüft, ob Jobs mit Knotenorientierung ausgeführt werden. Wenn Knotenaffinitätsjobs ausgeführt werden, schlägt die Prüfung fehl.

3. Wenn der Controller-Ersatzvorgang gestartet und die Vorabprüfungen abgeschlossen sind, hält der Vorgang die Aktivierung ein, damit Sie die Ausgabeinformationen, die Sie später bei der Konfiguration von node3 benötigen könnten, sammeln können.
4. Führen Sie den folgenden Befehlssatz aus, wie durch das Verfahren zum Austausch des Controllers auf der Systemkonsole gesteuert.

   Führen Sie von dem seriellen Port aus, der mit jedem Node verbunden ist, und speichern Sie die Ausgabe der folgenden Befehle einzeln:

   - `vserver services name-service dns show`
   - `network interface show -curr-node local -role cluster,intercluster,node-mgmt,clustermgmt, data`
   - `network port show -node local -type physical`
   - `service-processor show -node local -instance`
   - `network fcp adapter show -node local`
   - `network port ifgrp show -node local`
   - `network port vlan show`
   - `system node show -instance -node local`
   - `run -node local sysconfig`
   - `storage aggregate show -node local`
   - `volume show -node local`
   - `network interface failover-groups show`

- `storage array config show -switch switch_name`
- `system license show -owner local`
- `storage encryption disk show`

> Wenn NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) mit Onboard Key Manager verwendet wird, halten Sie die Schlüsselmanager-Passphrase bereit, um die Resynchronisierung des Schlüsselmanagers später im Verfahren durchzuführen.

5. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:
   - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
   - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

   > FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
   >
   > SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

   "Weitere Informationen zu unterstützten Self-Encrypting Drives".

Korrigieren Sie die Aggregateigentümer bei Ausfall einer ARL-Vorabprüfung

Wenn die aggregierte Statusprüfung fehlschlägt, müssen Sie Aggregate des Partner-Node an den Node „Home-Owner“ zurückgeben und den Vorabprüfvorgang erneut initiieren.

Schritte

1. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

   ```
   storage aggregate relocation start -node source_node -destination destination-node -aggregate-list *
   ```

2. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   ```
   storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state
   ```

   Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields
owner-name,home-name,state
aggregate   home-name  owner-name  state
---------   ---------  ----------  ------
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Nachdem Sie fertig sind

Sie müssen den Controller-Ersatzprozess neu starten:

`system controller replace start -nodes node_names`

Lizenz

Einige Funktionen erfordern Lizenzen, die als *Packages* ausgegeben werden, die eine oder mehrere Funktionen enthalten. Jeder Node im Cluster muss über seinen eigenen Schlüssel für jede Funktion im Cluster verfügen.

Wenn Sie keine neuen Lizenzschlüssel haben, stehen dem neuen Controller derzeit lizenzierte Funktionen im Cluster zur Verfügung. Durch die Verwendung nicht lizenzierter Funktionen auf dem Controller können Sie jedoch möglicherweise die Einhaltung Ihrer Lizenzvereinbarung verschließen. Sie sollten daher nach Abschluss des Upgrades den neuen Lizenzschlüssel oder die neuen Schlüssel für den neuen Controller installieren.

Siehe "Quellen" Link zur *NetApp-Support-Website*, auf der Sie neue 28-stellige Lizenzschlüssel für ONTAP erhalten können. Die Schlüssel sind im Abschnitt „*My Support*“ unter „*Software licenses*“ verfügbar. Wenn auf der Website nicht die erforderlichen Lizenzschlüssel vorhanden sind, können Sie sich an Ihren NetApp Ansprechpartner wenden.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Management der Storage-Verschlüsselung mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung der Schlüssel verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager`

`onboard show-backup` Befehl.

Stilllegen der SnapMirror Beziehungen (optional)

Bevor Sie mit dem Verfahren fortfahren, müssen Sie bestätigen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   Wenn der Status „Übertragen“ lautet, müssen Sie diese Transfers abbrechen: `snapmirror abort -destination-vserver vserver_name`

   Der Abbruch schlägt fehl, wenn sich die SnapMirror-Beziehung nicht im Zustand „Übertragen“ befindet.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Stufe 2: Knoten1 verschieben und ausmustern

Phase-2-Übersicht

Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie zeichnen auch die erforderlichen node1-Informationen auf, nehmen Node1 außer Betrieb und bereiten den Netzboot node3 und node4 später im Verfahren vor.

Schritte

1. "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2"
2. "Verschiebung ausgefallener oder Vetos von Aggregaten"
3. "Node1 ausmustern"
4. "Vorbereitungen für den Netzboot"

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2

Bevor Sie node1 durch Node3 ersetzen können, müssen Sie die nicht-Root-Aggregate und NAS-Daten-LIFs von node1 auf node2 verschieben, bevor Sie die Ressourcen von node1 schließlich in node3 verschieben.

Bevor Sie beginnen

Der Vorgang muss bereits angehalten werden, wenn Sie mit der Aufgabe beginnen. Sie müssen den Vorgang

manuell fortsetzen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. Sie müssen überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Der Home-Inhaber für die Aggregate und LIFs wird nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Wiederaufnahme der Vorgänge für die Aggregatverschiebung und die LIF-Verschiebung von NAS-Daten:

   `system controller replace resume`

   Alle Aggregate ohne Root-Root-Root-Root-Daten und LIFs werden von node1 auf node2 migriert.

   Der Vorgang angehalten, damit Sie überprüfen können, ob alle node1-Aggregate und LIFs für nicht-SAN-Daten in node2 migriert wurden.

2. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

3. Wenn der Vorgang noch angehalten wird, vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind, damit ihr Status bei node2 lautet:

   `storage aggregate show -node node2 -state online -root false`

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

   ```
   cluster::> storage aggregate show -node node2 state online -root false

   Aggregate  Size     Available  Used%  State  #Vols  Nodes  RAID Status
   ---------  -------  ---------  -----  ------ -----  ------
   --------------
   aggr_1     744.9GB  744.8GB    0%     online     5  node2
   raid_dp,normal
   aggr_2     825.0GB  825.0GB    0%     online     1  node2
   raid_dp,normal
   2 entries were displayed.
   ```

   Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

   `storage aggregate online -aggregate aggr_name`

4. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 verwenden und seine Ausgabe überprüfen:

```
volume show -node node2 -state offline
```

Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

```
volume online -vserver vserver_name -volume volume_name
```

Der *vserver_name* Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

5. Wenn die Ports, die derzeit Daten-LIFs hosten, nicht auf der neuen Hardware vorhanden sind, entfernen Sie sie aus der Broadcast-Domäne:

```
network port broadcast-domain remove-ports
```

6. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif LIF_name-home-node
nodename -status-admin up
```

7. Wenn Schnittstellengruppen oder VLANs konfiguriert sind, führen Sie die folgenden Teilschritte aus:

   a. Wenn Sie sie noch nicht gespeichert haben, notieren Sie die VLAN- und Schnittstellengruppen-Informationen, damit Sie die VLANs und Schnittstellengruppen auf node3 neu erstellen können, nachdem node3 gestartet wurde.

   b. Entfernen Sie die VLANs aus den Schnittstellengruppen:

```
network port vlan delete -node nodename -port ifgrp -vlan-id VLAN_ID
```

      Befolgen Sie die Korrekturmaßnahme, um alle Fehler zu beheben, die vom befehl vlan delete vorgeschlagen werden.

   c. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu sehen, ob Schnittstellengruppen auf dem Node konfiguriert sind:

```
network port ifgrp show -node nodename -ifgrp ifgrp_name -instance
```

      Das System zeigt Schnittstellengruppeninformationen für den Node an, wie im folgenden Beispiel gezeigt:

```
cluster::> network port ifgrp show -node node1 -ifgrp a0a -instance
                  Node: node1
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Wenn Schnittstellengruppen auf dem Node konfiguriert sind, notieren Sie die Namen dieser Gruppen und der ihnen zugewiesenen Ports. Löschen Sie dann die Ports, indem Sie den folgenden Befehl eingeben, und zwar einmal für jeden Port:

   `network port ifgrp remove-port -node nodename -ifgrp ifgrp_name -port netport`

Verschiebung ausgefallener oder Vetos von Aggregaten

Falls Aggregate nicht verschoben oder ein Vetoo eingesetzt werden kann, müssen sie die Aggregate manuell verschieben oder – falls erforderlich – entweder die Vetos oder Zielprüfungen überschreiben.

Über diese Aufgabe

Der Umzugsvorgang wird aufgrund des Fehlers angehalten.

Schritte

1. Überprüfen Sie die EMS-Protokolle, um festzustellen, warum das Aggregat nicht verschoben oder ein Veto eingelegt hat.
2. Verschiebung ausgefallener oder Vetos von Aggregaten:

   `storage aggregate relocation start -node node1 -destination node2 aggregate-list * -ndocontroller-upgrade true`

3. Geben Sie bei der entsprechenden Aufforderung ein `y`.
4. Sie können die Verschiebung mit einer der folgenden Methoden erzwingen:

Option	Beschreibung
Veto-Prüfungen werden überschrieben	Geben Sie Folgendes ein: `storage aggregate relocation start -override -vetoes * -ndocontroller-upgrade true`
Zielprüfungen überschreiben	Geben Sie Folgendes ein: `storage aggregate relocation start -overridedestination-checks * -ndo -controllerupgrade true`

Node1 ausmustern

Um „node1“ außer Betrieb zu nehmen, setzen Sie den automatischen Vorgang fort, um das HA-Paar mit node2 zu deaktivieren und node1 ordnungsgemäß herunterzufahren. Später im Verfahren entfernen Sie Knoten 1 aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

2. Vergewissern Sie sich, dass node1 angehalten wurde:

   ```
   system controller replace show-details
   ```

Nachdem Sie fertig sind

Sie können Node1 nach Abschluss des Upgrades außer Betrieb nehmen. Siehe "Ausmustern des alten Systems".

Vorbereitungen für den Netzboot

Nachdem Sie später noch Node3 und node4 physisch gerast haben, müssen Sie sie eventuell als Netzboot Netboot eingesetzt werden. Der Begriff „Netzboot“ bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf den Netzboot legen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver, auf den das System zugreifen kann.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Siehe "Quellen" Um eine Verknüpfung zur NetApp Support-Website zu erhalten und die erforderlichen Systemdateien für Ihre Plattform und die richtige Version von ONTAP herunterzuladen.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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.

Sie müssen die Controller jedoch nicht per Netzboot fahren, wenn auf den Original-Controllern die gleiche Version von ONTAP 9 installiert ist. Wenn ja, können Sie diesen Abschnitt überspringen und mit fortfahren "Stufe 3 Installieren und Booten von Knoten3"

Schritte

1. Rufen Sie die NetApp Support Site auf, um die Dateien zum Netzboot des Systems herunterzuladen.
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. 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 FAS/AFF8000 Serie	Extrahieren Sie den Inhalt des `<ontap_version>_image.tgz` Datei zum Zielverzeichnis:
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz` Sie müssen den Inhalt des nicht extrahieren `<ontap_version>_image.tgz` Datei:

Sie verwenden die Informationen in den Verzeichnissen in "Phase 3".

Phase 3: Installieren und booten Sie node3

Phase-3-Übersicht

In Phase 3 installieren und booten Sie node3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu und überprüfen die Installation node3. Wenn erforderlich, legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest und bestätigen, dass node3 Quorum beigetreten ist. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Schritte

1. "Installieren und booten Sie node3"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest"
3. "Ports von node1 nach node3 zuordnen"
4. "Beitritt zum Quorum, wenn ein Knoten über einen anderen Satz von Netzwerkports verfügt"
5. "Überprüfen Sie die Installation von node3"
6. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3"

Installieren und booten Sie node3

Sie müssen node3 im Rack installieren, Verbindungen von node1 zu node3, Boot node3 übertragen und ONTAP installieren. Sie müssen dann eine der freien Festplatten von

node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die zuvor nicht in node2 verschoben wurden, wie in diesem Abschnitt beschrieben neu zuweisen.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Außerdem müssen Sie überprüfen, ob die SAN-LIFs erfolgreich in Knoten 3 verschoben wurden.

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Wichtig:

- Wenn Sie ein mit Storage Arrays verbundenes V-Series System oder ein System über FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Upgrades erforderlich Schritt 1 Bis Schritt 21, Dann verlassen Sie diesen Abschnitt und folgen Sie den Anweisungen im "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Abschnitte nach Bedarf, geben Sie Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 23.
- Wenn Sie ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und anschließend mit den fortfahren "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Geben Sie Abschnitte ein, und geben Sie Befehle an der Cluster-Eingabeaufforderung ein.

Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

   Wenn sich Node1 und Node2 in einem separaten Chassis befanden, können Sie Node3 in denselben Rack-Standort wie node1 platzieren. Wenn sich Node1 jedoch im selben Chassis mit node2 befand, müssen Sie den Node3 in seinen eigenen Regalbereich legen, vorzugsweise in der Nähe der Position von node1.

2. Installieren Sie node3 im Rack und befolgen Sie die Anweisungen *Installation und Setup* für Ihr Node-Modell.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im selben Chassis durchführen, installieren sie node4 sowohl im Chassis als auch in node3. Wenn Sie dies nicht tun, verhält sich der Node, wenn Sie node3 booten, wie in einer Dual-Chassis-Konfiguration. Und wenn Sie node4 booten, wird der Interconnect zwischen den Nodes nicht gestartet.

3. Kabelnode3, Verschieben der Verbindungen von node1 nach node3.

   Verkabeln Sie die folgenden Verbindungen mithilfe des *Installations- und Setup-Leitfadens* oder der *Installationsanforderungen für die FlexArray-Virtualisierung und Referenz* für die node3-Plattform, des entsprechenden Festplatten-Shelf-Dokuments und „ High Availability Management_“.

   Siehe "Quellen" Link zu den Installationsanforderungen für die FlexArray-Virtualisierung und „ Reference_“ und „ High Availability Management_“.

   - Konsole (Remote-Management-Port)

- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Möglicherweise müssen Sie die Interconnect-Karte oder die Cluster Interconnect-Kabelverbindung von node1 zu node3 nicht verschieben, da die meisten Plattform-Modelle über ein einzigartiges Interconnect-Kartenmodell verfügen. Für die MetroCluster Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node1 auf node3 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Einschalten Sie den Netzstrom auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im gleichen Chassis durchführen, wird node4 auch neu gebootet. Allerdings kann man den node4-Stiefel bis später ignorieren.

   > Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

   ```
   WARNING: The battery is unfit to retain data during a power outage. This
   is likely because the battery is discharged but could be due to other
   temporary conditions.
   When the battery is ready, the boot process will complete and services
   will be engaged.
   To override this delay, press 'c' followed by 'Enter'
   ```

5. Wenn die Warnmeldung in angezeigt wird Schritt 4, Nehmen Sie die folgenden Aktionen:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

   > **Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.**

   > Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

   > Sie müssen 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 DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Storage-System. (Pflichtfeld). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Netzboot auf Node3 durchführen:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` Im Abschnitt "Vorbereitungen für den Netzboot".

Unterbrechen Sie den Startvorgang nicht.

8. im Startmenü Option wählen `(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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

> 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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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. Vervollständigen Sie die folgenden Teilschritte, um das Controller-Modul neu zu starten:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie den Wartungsmodus aus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12.] Überprüfen Sie, ob Controller und Chassis als ha konfiguriert sind:

    ```
    ha-config show
    ```

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    > Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn Controller und Chassis nicht als ha konfiguriert sind, verwenden Sie zum Korrigieren der Konfiguration die folgenden Befehle:

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

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

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

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

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

14. Wartungsmodus beenden:

```
halt
```

Unterbrechen Sie DAS AUTOBOOT, indem Sie an der Eingabeaufforderung der Boot-Umgebung Strg-C drücken.

15. auf node2 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

```
date
```

16. prüfen Sie das Datum in node3 mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

17. Geben Sie bei Bedarf das Datum auf node3 ein:

```
set date mm/dd/yyyy
```

18. auf node3 überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

19. Ggf. Die Zeit auf node3 einstellen:

```
set time hh:mm:ss
```

20. legen Sie im Boot-Loader die Partner-System-ID auf node3 fest:

```
setenv partner-sysid node2_sysid
```

Für Knoten 3, `partner-sysid` Muss der von node2 sein.

a. Einstellungen speichern:

```
saveenv
```

21. Überprüfen Sie den `partner-sysid` Für Knoten 3:

```
printenv partner-sysid
```

22. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Beschreibung
Verfügt über Festplatten und keinen Back-End-Speicher	Gehen Sie zu Schritt 23
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Weiter mit Abschnitt "Einstellen der FC- oder UTA/UTA2-Konfiguration auf node3" Und vervollständigen Sie die Unterabschnitte in diesem Abschnitt. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 23. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

23. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

    Wenn Ihr System über ein Tape-SAN verfügt, müssen Sie das Zoning für die Initiatoren benötigen. Ändern Sie gegebenenfalls die integrierten Ports an den Initiator, indem Sie auf das verweisen "Konfigurieren von FC-Ports auf node3". Weitere Anweisungen zum Zoning finden Sie in der Dokumentation des Storage-Arrays und des Zoning.

24. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

25. Ändern Sie die WWPN-Werte (Worldwide Port Name) in den Host- oder Volume-Gruppen, die mit Array-LUNs auf dem Speicher-Array verknüpft sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

26. Wenn Ihre Konfiguration ein Switch-basiertes Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
27. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.

    Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

    a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Wenden Sie sich an den NetApp Support, um Hilfe beim Wiederherstellen der integrierten Schlüsselmanagementinformationen zu erhalten.

28. Boot-Node im Startmenü:

```
boot_ontap menu
```

Wenn Sie nicht über eine FC- oder UTA/UTA2-Konfiguration verfügen, führen Sie die entsprechenden Aufgaben aus "UTA/UTA2-Ports in node4, Schritt 15, prüfen und konfigurieren" Damit node4 die Festplatten von node2 erkennen kann.

29.] für eine MetroCluster-Konfiguration finden Sie V-Series Systeme und Systeme mit FlexArray-Virtualisierungssoftware, die mit Storage-Arrays verbunden ist, unter "UTA/UTA2-Ports in node3, Schritt 15, prüfen und konfigurieren".

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest

Wenn node3 integrierte FC-Ports, Onboard Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschnitt ausfüllen Konfigurieren Sie FC-Ports auf node3, Der Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren, Oder beide Abschnitte.

Unter Umständen bezieht sich bei den Marketingmaterialien von NetApp der Begriff UTA2 auf Adapter und Ports des konvergierten Netzwerkadapters (CNA). Allerdings verwendet die CLI den Begriff CNA.

- Wenn node3 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie zur springen "Ports von node1 nach node3 zuordnen" Abschnitt.
- Wenn Sie jedoch ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware mit Storage-Arrays haben und node3 keine integrierten FC-Ports, Onboard UTA/UTA-Ports oder eine UTA/UTA2-Karte hat, kehren Sie zum Abschnitt *Installation und Boot-node3* zurück und fahren Sie fort "Schritt 23".

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node3
- UTA/UTA2-Ports in node3 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node3

Wenn node3 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in Betrieb nehmen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node1 haben, die Sie im Abschnitt gespeichert haben

"Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder eine UTA/UTA2-Karte verfügt, konfigurieren Sie sie in UTA/UTA2-Ports in node3 prüfen und konfigurieren.

Wenn Ihr System über Speicherfestplatten verfügt, geben Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle ein. Wenn Sie über ein „V-Series System“ oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus die entsprechenden Befehle ein.

1. Vergleichen Sie die FC-Einstellungen auf node3 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
2. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…

Festplatten sind vorhanden	Ändern Sie im Wartungsmodus (Option 5 im Startmenü) die FC-Ports auf node3 nach Bedarf:
	• So programmieren Sie Zielanschlüsse:
	`ucadmin modify -m fc -t target adapter`
	• So programmieren Sie Initiator-Ports:
	`ucadmin modify -m fc -t initiator adapter`
	`-t` Ist der FC4-Typ: Target oder Initiator.

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie im Wartungsmodus (Option 5 im Startmenü) die FC-Ports auf node3 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

3. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen mit dem folgenden Befehl und überprüfen Sie die Ausgabe: `ucadmin show`

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen mit dem folgenden Befehl und überprüfen Sie die Ausgabe: `ucadmin show`

4. Wartungsmodus beenden:

```
halt
```

5. Booten Sie das System über die LOADER-Eingabeaufforderung:

```
boot_ontap menu
```

6. nach Eingabe des Befehls warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
7. Wählen Sie die Option `5` Wählen Sie im Bootmenü für den Wartungsmodus aus.
8. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, fahren Sie mit dem Abschnitt fort UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen Sie den Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren. Und gehen Sie zum Abschnitt "Ports von node1 nach node3 zuordnen".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, fahren Sie mit dem Abschnitt fort UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen Sie den Abschnitt UTA/UTA2-Ports in node3 prüfen und konfigurieren Und zurück zum Abschnitt *Installieren und Starten von node3* beim Wiederaufnehmen bei "Schritt 23".

UTA/UTA2-Ports in node3 prüfen und konfigurieren

Wenn node3 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie möglicherweise neu konfigurieren, je nachdem, wie Sie das aktualisierte System verwenden möchten.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

Wenn Sie einen Unified Target Adapter (UTA/UTA2)-Port für FC verwenden möchten, müssen Sie zuerst überprüfen, wie der Port konfiguriert ist.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

Sie können das verwenden `ucadmin show` Befehl zum Überprüfen der aktuellen Portkonfiguration:

```
*> ucadmin show
         Current  Current    Pending   Pending      Admin
Adapter  Mode     Type       Mode      Type         Status
-------  -------  -------    --------  ----------   --------
0e       fc       target     -         initiator    offline
0f       fc       target     -         initiator    offline
0g       fc       target     -         initiator    offline
0h       fc       target     -         initiator    offline
1a       fc       target     -         -            online
1b       fc       target     -         -            online
6 entries were displayed.
```

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht gleichzeitige NIC- und FCoE-Traffic über die gleiche 10-GbE-SFP+-Schnittstelle und unterstützt FC-Ziele.

UTA/UTA2-Ports befinden sich möglicherweise auf einem Adapter oder auf dem Controller und verfügen über die folgenden Konfigurationen. Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf der node3 überprüfen und gegebenenfalls ändern:

- UTA-/UTA2-Karten, die bestellt werden, werden vor dem Versand konfiguriert, um die von Ihnen geforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden vor dem Versand konfiguriert, um die Persönlichkeit zu erhalten, die Sie anfordern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein V-Series System verfügen oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt an der Eingabeaufforderung im Wartungsmodus Befehle ein. Sie müssen sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit konfiguriert sind, indem Sie auf node3 den folgenden Befehl eingeben:

Wenn das System…	Dann…
Festplatten sind vorhanden	Keine Aktion erforderlich.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
          Current  Current     Pending   Pending    Admin
Adapter   Mode     Type        Mode      Type       Status
-------   -------  ---------   -------   --------   ---------
0e        fc       initiator   -         -          online
0f        fc       initiator   -         -          online
0g        cna      target      -         -          online
0h        cna      target      -         -          online
0e        fc       initiator   -         -          online
0f        fc       initiator   -         -          online
0g        cna      target      -         -          online
0h        cna      target      -         -          online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Untersuchung der Ausgabe des `ucadmin show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.
4. Nehmen Sie eine der folgenden Aktionen:

Wenn die UTA/UTA2-Ports…	Dann…
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. [[Auto_check3_schritt 5]]Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

6. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

7. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` Ist der Persönlichkeitsmodus, `fc` Oder `cna`.
   - `-t` Ist der Typ FC4, `target` Oder `initiator`.

   > Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

8. Überprüfen Sie die Einstellungen:

   `ucadmin show`

9. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`ucadmin show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
*> ucadmin show
         Current    Current     Pending  Pending     Admin
Adapter  Mode       Type        Mode     Type        Status
-------  --------   ----------  -------  --------    --------
1a       fc         initiator   -        -           online
1b       fc         target      -        initiator   online
2a       fc         target      cna      -           online
2b       fc         target      cna      -           online
*>
```

10. Platzieren Sie alle Zielports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

11. Anschluss verkabeln.
12. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Ports von node1 nach node3 zuordnen"
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zu *Install and Boot node3* zurück und setzen Sie den Abschnitt unter fort "Schritt 23".

1. Wartungsmodus beenden:

   `halt`

2. Boot-Knoten in Boot-Menü durch Ausführen `boot_ontap menu`. Wenn Sie ein Upgrade auf eine A800 durchführen, gehen Sie zu Schritt 23.
3. in node3 gehen Sie zum Startmenü und wählen Sie die verborgene Option mit 22/7 aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node1 ein, um die Festplatten von node1 zu node3 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
.
.
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.
Selection (1-9)? 22/7
.
.
(boot_after_controller_replacement)   Boot after controller upgrade
(9a)                                  Unpartition all disks and
remove their ownership information.
(9b)                                  Clean configuration and
initialize node with partitioned disks.
(9c)                                  Clean configuration and
initialize node with whole disks.
(9d)                                  Reboot the node.
(9e)                                  Return to main boot menu.

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.
Selection (1-9)? boot_after_controller_replacement
```

```
.
This will replace all flash-based configuration with the last backup
to
disks. Are you sure you want to continue?: yes
.
.
Controller Replacement: Provide name of the node you would like to
replace: <name of the node being replaced>
.
.
Changing sysid of node <node being replaced> disks.
Fetched sanown old_owner_sysid = 536953334 and calculated old sys id
= 536953334
Partner sysid = 4294967295, owner sysid = 536953334
.
.
.
Terminated
<node reboots>
.
.
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
.
.
System rebooting...
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
Login:
...
```

4. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, Das liegt daran, dass es die Ports wieder in den Zielmodus zurückgesetzt hat und somit keine Disketten sehen kann. Weiter mit Schritt 17 Bis Schritt 22 Um dies zu beheben.
5. Drücken Sie während des AUTOBOOTS Strg-C, um den Knoten an der Eingabeaufforderung LOADER> anzuhalten.
6. wechseln Sie an der LOADER-Eingabeaufforderung in den Wartungsmodus:

```
boot_ontap maint
```

7.] im Wartungsmodus werden alle zuvor festgelegten Initiator-Ports angezeigt, die sich jetzt im Zielmodus befinden:

   ```
   ucadmin show
   ```

   Ändern Sie die Ports zurück in den Initiatormodus:

   ```
   ucadmin modify -m fc -t initiator -f adapter name
   ```

8. Überprüfen Sie, ob die Ports in den Initiatormodus geändert wurden:

   ```
   ucadmin show
   ```

9. Wartungsmodus beenden:

   ```
   halt
   ```

   > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das auch externe Festplatten unterstützt, gehen Sie zu Schritt 22.
   >
   > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das sowohl interne als auch externe Festplatten, wie z. B. ein AFF A800 System, unterstützt, finden Sie unter Schritt 23.

10. Starten Sie an der LOADER-Eingabeaufforderung:

    ```
    boot_ontap menu
    ```

    Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

    Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her:

    a. Zurück zum speziellen Startmenü:

       ```
       LOADER> boot_ontap menu
       ```

```
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)? 10
```

a. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

b. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

d. Geben Sie bei Aufforderung die Backup-Daten ein.

> Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

e. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

> In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 22 Bis das System ordnungsgemäß gebootet wird.

11. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. AFF A800 Systeme), setzen Sie das node1-Aggregat als Root-Aggregat ein, um zu bestätigen, dass node3 aus dem Root-Aggregat von node1 bootet. Zum Festlegen des Root-Aggregats rufen Sie das Boot-Menü auf und wählen dann Option `5` Um in den Wartungsmodus zu wechseln.

> **Die folgenden Teilschritte müssen in der angegebenen Reihenfolge ausgeführt werden; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.**

Im folgenden Verfahren wird node3 vom Root-Aggregat von node1 gestartet:

a. Wechseln in den Wartungsmodus:

```
boot_ontap maint
```

b. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node1 Aggregat:

```
aggr status -r
```

c. Überprüfen Sie den Status des node1-Aggregats:

```
aggr status
```

d. Bei Bedarf das node1 Aggregat online bringen:

```
aggr_online root_aggr_from_node1
```

e. Verhindern Sie, dass das node3 vom ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node3
```

f. Legen Sie das node1-Root-Aggregat als das neue Root-Aggregat für node3 fest:

```
aggr options aggr_from_node1 root
```

g. Überprüfen Sie, ob das Root-Aggregat von node3 offline ist und das Root-Aggregat für die von node1 hergebrachten Festplatten online ist und in den Root-Status eingestellt ist:

```
aggr status
```

> Wenn der vorherige Unterschritt nicht ausgeführt wird, kann node3 vom internen Root-Aggregat booten, oder es kann dazu führen, dass das System eine neue Cluster-Konfiguration übernimmt oder Sie aufgefordert werden, eine zu identifizieren.

Im Folgenden wird ein Beispiel für die Befehlsausgabe angezeigt:

```
------------------------------------------------------------------
Aggr                  State    Status             Options

aggr0_nst_fas8080_15 online   raid_dp, aggr      root, nosnap=on
                              fast zeroed
                              64-bit

aggr0                 offline  raid_dp, aggr      diskroot
                              fast zeroed
                              64-bit
------------------------------------------------------------------
```

Ports von node1 nach node3 zuordnen

Sie müssen überprüfen, ob die physischen Ports auf node1 den physischen Ports auf node3 korrekt zugeordnet sind. Dadurch kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Die Port-Einstellungen können je nach Modell der Nodes variieren. Sie müssen die Port- und LIF-Konfiguration auf dem ursprünglichen Node mit der geplanten Verwendung und Konfiguration des neuen Node kompatibel machen. Dies liegt daran, dass der neue Node beim Booten der gleichen Konfiguration wiedergibt. Dies bedeutet, dass ONTAP beim Booten von node3 versuchen wird, LIFs auf den gleichen Ports zu hosten, die in node1 verwendet wurden.

Wenn also die physischen Ports auf node1 nicht direkt den physischen Ports auf node3 zugeordnet werden, sind daher Änderungen der Software-Konfiguration erforderlich, um nach dem Booten die Cluster-, Management- und Netzwerkkonnektivität wiederherzustellen. Wenn die Cluster-Ports auf node1 nicht direkt den Cluster-Ports auf node3 zugeordnet werden, wird node3 möglicherweise nicht automatisch dem Quorum beitreten, wenn er neu gestartet wird, bis Sie die Software-Konfiguration ändern, um die Cluster-LIFs auf den richtigen physischen Ports zu hosten.

Schritte

1. Notieren Sie in der Tabelle alle Kabelinformationen für node1, die Ports, Broadcast-Domänen und IPspaces:

LIF	Anzahl an Knoten1-Ports	Node1-IPspaces	Broadcast-Domänen der Nr. 1	Node3-Ports	Node3-IPspaces	Node3 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						

2. Zeichnen Sie alle Kabelinformationen für node3, die Ports, Broadcast-Domänen und IPspaces in der Tabelle auf.
3. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob es sich bei dem Setup um ein 2-Node-Cluster ohne Switches handelt:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
cluster::> set -privilege advanced
```

b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
cluster::> network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

+
Der Wert dieser Befehlsausgabe muss dem physischen Status des Systems entsprechen.

a. Zurück zur Administratorberechtigungsebene:

```
cluster::*> set -privilege admin

cluster::>
```

4. Gehen Sie folgendermaßen vor, um Node3 in Quorum zu platzieren:

a. Boot-Knoten 3. Siehe "Installieren und booten Sie node3" Um den Node zu booten, wenn Sie dies noch nicht getan haben.

b. Vergewissern Sie sich, dass sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden:

```
network port show -node node -port port -fields broadcast-domain
```

Das folgende Beispiel zeigt, dass Port „e0a“ sich in der Cluster-Domäne auf node3 befindet:

```
 cluster::> network port show -node _node3_ -port e0a -fields
broadcast-domain

 node       port broadcast-domain
 ---------- ---- ----------------
 node3      e0a  Cluster
```

c. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domäne befinden, fügen Sie sie mit dem folgenden Befehl hinzu:

```
broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports
node:port
```

Dieses Beispiel fügt Cluster-Port „e1b“ auf Knoten3 hinzu:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

d. Fügen Sie die korrekten Ports zur Cluster Broadcast-Domäne hinzu:

```
network port modify -node -port -ipspace Cluster -mtu 9000
```

Dieses Beispiel fügt Cluster-Port „e1b“ auf node4 hinzu:

```
network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000
```

e. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

```
network interface migrate -vserver Cluster -lif lif_name -source-node node3
-destination-node node3 -destination-port port_name
```

f. Ändern Sie den Startport der Cluster-LIFs:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

g. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne:

```
network port broadcast-domain remove-ports
```

Mit dem folgenden Befehl wird der Port „e0d“ auf node3 entfernt:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain
Cluster -ports node3:e0d
```

a. Vergewissern Sie sich, dass node3 erneut dem Quorum beigetreten ist:

```
cluster show -node node3 -fields health
```

5. Anpassen der Broadcast-Domänen, die Ihre Cluster-LIFs hosten, sowie Node-Management/clustermanagement-LIFs. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie die LIFs möglicherweise wie folgt migrieren und ändern müssen:

a. Zeigen Sie den Startport einer logischen Schnittstelle an:

```
network interface show -fields home-node,home-port
```

b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:

```
network port broadcast-domain add-ports
```

```
network port broadcast-domain remove-ports
```

a. Ändern Sie den Home-Port eines LIF:

```
network interface modify -vserver vserver -lif lif_name –home-port port_name
```

6. Passen Sie die Broadcast-Domänenmitgliedschaft der Netzwerkports an, die für Intercluster LIFs verwendet werden, mit denselben Befehlen an, wie in dargestellt Schritt 5.
7. Passen Sie alle anderen Broadcast-Domänen an und migrieren Sie die Daten-LIFs, falls erforderlich, mit denselben Befehlen in Schritt 5.
8. Wenn auf node1 keine Ports mehr vorhanden waren, löschen Sie sie mit den folgenden Schritten:
   a. Zugriff auf die erweiterte Berechtigungsebene auf beiden Nodes:

      ```
      set -privilege advanced
      ```

   b. So löschen Sie die Ports:

      ```
      network port delete -node node_name -port port_name
      ```

   c. Zurück zur Administratorebene:

      ```
      set -privilege admin
      ```

9. Passen Sie alle LIF Failover-Gruppen an:

   ```
   network interface modify -failover-group failover_group -failover-policy
   failover_policy
   ```

   Mit dem folgenden Befehl wird die Failover-Richtlinie auf festgelegt `broadcast-domain-wide` Und verwendet die Ports in der Failover-Gruppe „fg1“ als Failover-Ziele für LIF „data1“ auf node3:

   ```
   network interface modify -vserver node3 -lif data1 failover-policy broadcast-
   domainwide -failover-group fg1
   ```

   Siehe "Quellen" Link zu *Netzwerkverwaltung* oder den Befehlen *ONTAP 9: Manual Page Reference* für weitere Informationen.

10. Überprüfen Sie die Änderungen auf node3:

    ```
    network port show -node node3
    ```

11. Jedes Cluster-LIF muss an Port 7700 zuhören. Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören:

    ```
    ::> network connections listening show -vserver Cluster
    ```

    Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

    ```
    ::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
    int modify -vserver Cluster -lif cluster-lif -status-admin up
    ```

    Wiederholen Sie Schritt 11, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

Fügen Sie dem Quorum bei, wenn ein Node über einen anderen Satz an Netzwerkports verfügt

Der Node mit dem neuen Controller bootet und versucht zuerst, dem Cluster automatisch beizutreten. Wenn der neue Node jedoch einen anderen Satz an Netzwerkports aufweist, müssen Sie die folgenden Schritte durchführen, um zu bestätigen, dass der Node dem Quorum erfolgreich hinzugefügt wurde.

Über diese Aufgabe

Sie können diese Anweisungen für alle relevanten Knoten verwenden. Node3 wird in der folgenden Probe verwendet.

Schritte

1. Überprüfen Sie, ob sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

   ```
   network port show -node node -port port -fields broadcast-domain
   ```

   Das folgende Beispiel zeigt, dass sich der Port „e1a“ in der Cluster-Domäne auf node3 befindet:

   ```
   cluster::> network port show -node node3 -port e1a -fields broadcast-
   domain
   node   port broadcast-domain
   ------ ---- ----------------
   node3  e1a  Cluster
   ```

2. Fügen Sie die korrekten Ports der Cluster Broadcast-Domäne hinzu, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network port modify -node -port -ipspace Cluster -mtu 9000
```

Dieses Beispiel fügt Cluster-Port „e1b“ auf Knoten3 hinzu:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

3. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF, und verwenden Sie den folgenden Befehl:

   ```
   network interface migrate -vserver Cluster -lif lif_name -source-node node3 -
   destination-node node3 -destination-port port_name
   ```

4. Ändern Sie den Startport der Cluster-LIFs:

   ```
   network interface modify -vserver Cluster -lif lif_name –home-port port_name
   ```

5. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domäne befinden, fügen Sie sie mit folgendem Befehl hinzu:

   ```
   network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain
   Cluster - ports node:port
   ```

6. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne. Sie können für jeden relevanten Knoten verwenden. Mit dem folgenden Befehl wird der Port „e0d“ auf node3 entfernt:

   ```
   network port broadcast-domain remove-ports network port broadcast-domain
   remove-ports ipspace Cluster -broadcast-domain Cluster -ports node3:e0d
   ```

7. Vergewissern Sie sich, dass der Node erneut dem Quorum beigetreten ist:

   ```
   cluster show -node node3 -fields health
   ```

8. Passen Sie die Broadcast-Domänen an, die Ihre Cluster-LIFs und LIFs für das Node-Management/Cluster-Management hosten. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie die LIFs möglicherweise wie folgt migrieren und ändern müssen:

   a. Zeigen Sie den Startport einer logischen Schnittstelle an:

      ```
      network interface show -fields home-node,home-port
      ```

   b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

      ```
      network port broadcast-domain show -ports node_name:port_name
      ```

   c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:
      `network port broadcast-domain add-ports network port broadcast-domain remove-port`

   d. Ändern eines Startports einer LIF:
      `network interface modify -vserver vserver -lif lif_name –home-port port_name`
      Passen Sie die Intercluster-Broadcast-Domänen an und migrieren Sie gegebenenfalls die Intercluster LIFs. Die Daten-LIFs bleiben unverändert.

Überprüfen Sie die Installation von node3

Nach der Installation und dem Booten von node3 müssen Sie überprüfen, ob die Installation korrekt ist. Sie müssen warten, bis Knoten 3 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen.

Über diese Aufgabe

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node3 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node3 dem Quorum beigetreten ist:

   ```
   cluster show -node node3 -fields health
   ```

2. Vergewissern Sie sich, dass node3 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Überprüfen Sie den Status des Vorgangs, und überprüfen Sie, ob die Konfigurationsinformationen für node3 identisch sind mit node1:

   ```
   system controller replace show-details
   ```

   Wenn sich die Konfiguration für node3 unterscheidet, kann zu einem späteren Zeitpunkt eine Systemunterbrechung auftreten.

4. Überprüfen Sie, ob der ersetzte Controller für die MetroCluster-Konfiguration ordnungsgemäß konfiguriert ist, die MetroCluster-Konfiguration sollte sich im ordnungsgemäßen Zustand befinden und nicht im Switchover-Modus. Siehe "Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration".

Erneutes Erstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen auf Knoten3

Nachdem Sie bestätigt haben, dass node3 sich im Quorum befindet und mit node2 kommunizieren kann, müssen Sie die VLANs, Schnittstellengruppen und Broadcast-Domänen von node1 auf node3 neu erstellen. Sie müssen auch die node3-Ports zu den neu erstellten Broadcast-Domänen hinzufügen.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Und Link zu *Network Management*.

Schritte

1. Erstellen Sie die VLANs auf Node3 anhand der Node1-Informationen, die im aufgezeichnet wurden, erneut "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2" Abschnitt:

   ```
   network port vlan create -node node_name -vlan vlan-names
   ```

2. Erstellen Sie die Schnittstellengruppen auf node3 mit den node1-Informationen, die im aufgezeichnet wurden, erneut "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2" Abschnitt:

   ```
   network port ifgrp create -node node_name -ifgrp port_ifgrp_names-distr-func
   ```

3. Erstellen Sie die Broadcast-Domänen auf node3 mithilfe der node1-Informationen, die im aufgezeichnet wurden, erneut "Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf Knoten 2" Abschnitt:

   ```
   network port broadcast-domain create -ipspace Default -broadcast-domain
   broadcast_domain_names -mtu mtu_size -ports
   node_name:port_name,node_name:port_name
   ```

4. Fügen Sie die node3-Ports zu den neu erstellten Broadcast-Domänen hinzu:

   ```
   network port broadcast-domain add-ports -broadcast-domain
   broadcast_domain_names -ports node_name:port_name,node_name:port_name
   ```

Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3

Wenn Sie NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) zur Verschlüsselung von Volumes auf dem System verwenden, das Sie aktualisieren, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht wiederherstellen, werden beim Verschieben der Node1-Aggregate mit ARL von node2 auf Knoten 3 verschlüsselte Volumes offline geschaltet.

Schritte

1. Führen Sie zum Synchronisieren der Verschlüsselungskonfiguration für Onboard Key Manager den folgenden Befehl an der Cluster-Eingabeaufforderung aus:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 oder 9.7	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

2. Geben Sie die Cluster-weite Passphrase für das Onboard Key Manager ein.

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3

Nachdem Sie die Installation node3 überprüft haben und bevor Sie Aggregate von node2 auf node3 verschieben, müssen Sie die NAS-Daten-LIFs von node1 verschieben, die sich derzeit in node2 von node2 auf node3 befinden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

Das System führt die folgenden Aufgaben aus:

- Cluster-Quorum-Prüfung
- System-ID-Prüfung
- Prüfung der Bildversion
- Überprüfung der Zielplattform
- Prüfung der Netzwerkanachabilität

Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Überprüfen Sie manuell, ob das Netzwerk und alle VLANs, Schnittstellengruppen und Broadcast-Domänen korrekt konfiguriert wurden.
3. Wiederaufnahme des Betriebs der Versetzung:

   `system controller replace resume`

   ```
   To complete the "Network Reachability" phase, ONTAP network
   configuration must
   be manually adjusted to match the new physical network configuration of
   the
   hardware. This includes assigning network ports to the correct broadcast
   domains, creating any required ifgrps and VLANs, and modifying the home-
   port
   parameter of network interfaces to the appropriate ports. Refer to the
   "Using
   aggregate relocation to upgrade controller hardware on a pair of nodes
   running
   ONTAP 9.x" documentation, Stages 3 and 5. Have all of these steps been
   manually
   completed? [y/n]
   ```

4. Eingabe `y` Um fortzufahren.
5. Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen verschiebt das System die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf den neuen Controller, node3. Das System hält an, sobald die Ressourcenverlagerung abgeschlossen ist.

6. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   `system controller replace show-details`

7. Überprüfen Sie, ob die nicht-Root-Aggregate und NAS-Daten-LIFs erfolgreich in node3 verschoben wurden.

Falls Aggregate nicht verschoben oder ein Vetoo eingesetzt werden kann, müssen sie die Aggregate manuell verschieben oder – falls erforderlich – entweder die Vetos oder die Zielprüfungen außer Kraft setzen. Siehe "Verschiebung ausgefallener oder Vetos von Aggregaten" Finden Sie weitere Informationen.

8. Überprüfen Sie, ob sich die SAN-LIFs auf den richtigen Ports auf node3 befinden, indem Sie die folgenden Teilschritte ausführen:

   a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

      `network interface show -data-protocol iscsi|fcp -home-node node3`

      Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3

        Logical   Status     Network           Current  Current Is
Vserver Interface Admin/Oper Address/Mask      Node     Port    Home
------- --------- ---------- ----------------- -------- ------- ----
vs0
        a0a       up/down     10.63.0.53/24     node3   a0a     true
        data1     up/up       10.63.0.50/18     node3   e0c     true
        rads1     up/up       10.63.0.51/18     node3   e1a     true
        rads2     up/down     10.63.0.52/24     node3   e1b     true
vs1
        lif1      up/up       172.17.176.120/24 node3   e0c     true
        lif2      up/up       172.17.176.121/24 node3   e1a     true
```

   b. Wenn node3 irgendwelche SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der nicht in node1 vorhanden war oder einem anderen Port zugeordnet werden muss, verschieben Sie sie zu einem geeigneten Port auf node3, indem Sie die folgenden Teilschritte ausführen:

      i. Setzen Sie den LIF-Status auf „down“:

         `network interface modify -vserver Vserver_name -lif LIF_name -status -admin down`

      ii. Entfernen Sie das LIF aus dem Portsatz:

         `portset remove -vserver Vserver_name -portset portset_name -port-name port_name`

      iii. Geben Sie einen der folgenden Befehle ein:

         - Verschieben eines einzelnen LIF:

           `network interface modify -vserver Vserver_name -lif LIF_name -home -port new_home_port`

         - Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen neuen Port:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver Vserver_name -portset portset_name -port-name
port_name
```

Sie müssen bestätigen, dass Sie SAN-LIFs zu einem Port mit der gleichen Verbindungsgeschwindigkeit wie der ursprüngliche Port verschoben haben.

a. Ändern Sie den Status aller LIFs auf „up“, damit die LIFs den Datenverkehr auf dem Node akzeptieren und senden können:

```
network interface modify -home-port port_name -home-node node3 -lif data
-status admin up
```

b. Geben Sie an jedem Node den folgenden Befehl ein, und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von aufweisen `up`:

```
network interface show -home-node node3 -role data
```

c. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif lif_name -status-admin
up
```

9. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

```
system controller replace resume
```

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung
- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster

Phase 4: Knoten2 verschieben und ausmustern

Phase-4-Übersicht

Während Phase 4 werden Aggregate und NAS-Daten-LIFs von Knoten 2 auf Knoten 3 verschoben. Sie müssen die nötigen node2-Informationen notieren und dann node2 stilllegen.

Schritte

1. "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3"
2. "Node2 ausmustern"

Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3

Bevor Sie node2 durch node4 ersetzen, verschieben Sie die nicht-Root-Aggregate und NAS-Daten-LIFs, die im Besitz von node2 sind, auf node3.

Bevor Sie beginnen

Nach den Nachprüfungen aus der vorherigen Phase wird automatisch die Ressourcenfreigabe für node2 gestartet. Die Aggregate außerhalb des Root-Bereichs und LIFs für nicht-SAN-Daten werden von node2 auf node3 migriert.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich.

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. In dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in node3 migriert werden.

Der Home-Inhaber für die Aggregate und LIFs werden nicht geändert, nur der aktuelle Besitzer wird geändert.

Schritte

1. Vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind und ihren Status auf node3:

   `storage aggregate show -node node3 -state online -root false`

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

   ```
   cluster::> storage aggregate show -node node3 state online -root false

   Aggregate      Size         Available   Used%   State   #Vols  Nodes
   RAID     Status
   ----------     ---------    ---------   ------  -----   -----  ------
   -------  ------
   aggr_1         744.9GB      744.8GB      0%     online  5      node2
   raid_dp  normal
   aggr_2         825.0GB      825.0GB      0%     online  1      node2
   raid_dp  normal
   2 entries were displayed.
   ```

   Wenn die Aggregate offline sind oder in node3 offline sind, bringen Sie sie mit dem folgenden Befehl auf node3 online, einmal für jedes Aggregat:

   `storage aggregate online -aggregate aggr_name`

2. Überprüfen Sie, ob alle Volumes auf node3 online sind, indem Sie den folgenden Befehl auf node3 verwenden und die Ausgabe überprüfen:

   `volume show -node node3 -state offline`

   Wenn ein Volume auf node3 offline ist, schalten Sie sie online. Verwenden Sie dazu den folgenden Befehl auf node3, einmal für jedes Volume:

   `volume online -vserver vserver_name -volume volume_name`

   Der `vserver_name` Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

3. Überprüfen Sie, ob die LIFs zu den richtigen Ports verschoben wurden und über den Status von verfügen `up`. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

   `network interface modify -vserver vserver_name -lif LIF_name -home-node node_name -status-admin up`

4. Wenn die Ports, die derzeit Daten-LIFs hosten, nicht auf der neuen Hardware vorhanden sind, entfernen Sie diese aus der Broadcast-Domäne:

   `network port broadcast-domain remove-ports`

5. Überprüfen Sie, ob auf node2 keine Daten-LIFs bleiben, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

   `network interface show -curr-node node2 -role data`

6. Wenn Schnittstellengruppen oder VLANs konfiguriert sind, führen Sie die folgenden Teilschritte aus:

   a. Notieren Sie VLAN- und Schnittstellengruppeninformationen, damit Sie die VLANs und Schnittstellengruppen auf node3 neu erstellen können, nachdem node3 gestartet wurde.

   b. Entfernen Sie die VLANs aus den Schnittstellengruppen:

      `network port vlan delete -node nodename -port ifgrp -vlan-id VLAN_ID`

   c. Überprüfen Sie, ob auf dem Node Schnittstellengruppen konfiguriert sind, indem Sie den folgenden Befehl eingeben und seine Ausgabe überprüfen:

      `network port ifgrp show -node node2 -ifgrp ifgrp_name -instance`

      Das System zeigt Schnittstellengruppeninformationen für den Node an, wie im folgenden Beispiel gezeigt:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node3
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Wenn Schnittstellengruppen auf dem Node konfiguriert sind, notieren Sie die Namen dieser Gruppen und der ihnen zugewiesenen Ports. Löschen Sie dann die Ports, indem Sie den folgenden Befehl eingeben, und zwar einmal für jeden Port:

   `network port ifgrp remove-port -node nodename -ifgrp ifgrp_name -port netport`

Node2 ausmustern

Um node2 außer Betrieb zu nehmen, schalten Sie node2 zunächst ordnungsgemäß aus und entfernen Sie es aus dem Rack oder Gehäuse.

Schritte

1. Vorgang fortsetzen:

   `system controller replace resume`

   Der Knoten wird automatisch angehalten.

Nachdem Sie fertig sind

Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5: installieren und booten sie node4

Phase-5-Übersicht

In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 nach node4 zu und überprüfen die Installation von node4. Wenn erforderlich, legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest und bestätigen, dass node4 Quorum beigetreten ist. Außerdem werden Knoten2-NAS-Daten-LIFs und nicht-Root-Aggregate von node3 auf node4 verschoben und überprüft, ob die SAN-LIFs auf node4 vorhanden sind.

Schritte

1. "installieren und booten sie node4"

2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest"
3. "Weisen Sie Ports von node2 nach node4 zu"
4. "Fügen Sie dem Quorum bei, wenn ein Node über einen anderen Satz an Netzwerkports verfügt"
5. "Überprüfen Sie die installation von node4"
6. "Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4"

installieren und booten sie node4

Sie müssen node4 im Rack installieren, die node2-Verbindungen nach node4 übertragen, node4 booten und ONTAP installieren. Sie müssen dann freie Festplatten in node2 neu zuweisen, sämtliche Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die zuvor nicht in node3 verschoben wurden, wie in diesem Abschnitt beschrieben.

Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Vorgang wird größtenteils automatisch durchgeführt. Der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Außerdem müssen Sie überprüfen, ob die NAS-Daten-LIFs erfolgreich in node4 verschoben wurden.

Sie müssen node4 als Netzboot ausführen, wenn es nicht die gleiche Version von ONTAP 9 hat, die auf node2 installiert ist. Nachdem sie node4 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen "Vorbereitungen für den Netzboot".

Wichtig:

- Wenn Sie ein mit Storage-Arrays verbundenes V-Series System oder ein System mit FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Anforderungen unbedingt zu beachten Schritt 1 Bis Schritt 21, Dann verlassen Sie diesen Abschnitt und folgen Sie den Anweisungen zu "Konfigurieren Sie FC-Ports auf node4" Und nach "UTA/UTA2-Ports auf node4 prüfen und konfigurieren", Eingabe von Befehlen im Wartungsmodus. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 23.
- Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt ausfüllen und mit fortfahren "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt.

   Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

2. installieren sie node4 im Rack gemäß den Anweisungen in der Anleitung *Installation and Setup Instructions* für das Node-Modell.
3. Kabel node4, ziehen Sie die Verbindungen von node2 nach node4.

   Verkabeln Sie die folgenden Verbindungen mithilfe der Anleitung im *Installation and Setup Instructions*

oder beim *FlexArray Installation Requirements and Reference* für die node4-Plattform, dem entsprechenden Platten-Shelf-Dokument und *High Availability Management*.

Siehe "Quellen" Link zu den Installationsanforderungen für die FlexArray-Virtualisierung und „ Reference_“ und „ High Availability Management_“.

- Konsole (Remote-Management-Port)
- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Möglicherweise müssen Sie die Interconnect-Karte/FC-VI-Karte oder die Interconnect/FC-VI-Kabelverbindung von node2 auf node4 nicht verschieben, da die meisten Plattform-Modelle über einzigartige Interconnect-Kartenmodelle verfügen. Bei der MetroCluster Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node2 nach node4 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Schalten Sie node4 ein, und unterbrechen Sie den Bootvorgang, indem Sie am Konsolenterminal Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

   Wenn Sie node4 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
         because the battery is discharged but could be due to other
temporary
         conditions.
         When the battery is ready, the boot process will complete
         and services will be engaged. To override this delay, press 'c'
followed
         by 'Enter'
```

5. Wenn die Warnmeldung in Schritt 4 angezeigt wird, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

      Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.

   Siehe "Vorbereitungen für den Netzboot".

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie müssen 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 DHCP (Dynamic Host Configuration Protocol) lautet…	**Dann…**
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. HINWEIS: Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

7. Ausführen eines Netzboots auf node4:

Für…	**Dann…**
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_web-accessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 1 im Abschnitt "Vorbereitungen für den Netzboot".

> Unterbrechen Sie den Startvorgang nicht.

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.

Ignorieren Sie die folgende Meldung:

`This procedure is not supported for Non-Disruptive Upgrade on an HA pair`

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

> 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. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

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

   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

11. Wählen Sie Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12. Vergewissern Sie sich, dass Controller und Chassis als HA konfiguriert sind:

    `ha-config show`

    Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

    ```
    Chassis HA configuration: ha
    Controller HA configuration: ha
    ```

    > Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn der Controller und das Chassis nicht als HA konfiguriert wurden, verwenden Sie zum Korrigieren der Konfiguration die folgenden Befehle:

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

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

    Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

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

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

14. Beenden des Wartungsmodus:

    ```
    halt
    ```

    Unterbrechen Sie DAS AUTOBOOT, indem Sie an der Eingabeaufforderung der Boot-Umgebung Strg-C drücken.

15. auf node3 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

    ```
    date
    ```

16. Überprüfen Sie am node4 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show date
    ```

17. Legen Sie bei Bedarf das Datum auf node4 fest:

    ```
    set date mm/dd/yyyy
    ```

18. Überprüfen Sie auf node4 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show time
    ```

19. Stellen Sie bei Bedarf die Uhrzeit auf node4 ein:

    ```
    set time hh:mm:ss
    ```

20. Legen Sie im Boot-Loader die Partner-System-ID auf node4 fest:

    ```
    setenv partner-sysid node3_sysid
    ```

    Für node4, `partner-sysid` Muss das der Node3 sein.

    Einstellungen speichern:

    ```
    saveenv
    ```

21. [[Auto_install4_step21] Verify the `partner-sysid` für node4:

```
printenv partner-sysid
```

22. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Gehen Sie zu Schritt 23.
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Weiter mit Abschnitt "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Und vervollständigen Sie die Unterabschnitte in diesem Abschnitt. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 23. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

23. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

    Ändern Sie gegebenenfalls die integrierten Ports an den Initiator, indem Sie auf das verweisen "Konfigurieren Sie FC-Ports auf node4". Weitere Anweisungen zum Zoning finden Sie in der Dokumentation des Storage-Arrays und des Zoning.

24. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

25. Ändern Sie die WWPN-Werte (Worldwide Port Name) in den Host- oder Volume-Gruppen, die den Array-LUNs auf dem Speicher-Array zugeordnet sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

26. Wenn die Konfiguration das Switch-basierte Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.

27. Wenn Sie NSE-Laufwerke (NetApp Storage Encryption) installiert haben, führen Sie die folgenden Schritte aus.

    Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

    a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support **true**`
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support **false**`

> FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Wenden Sie sich an den NetApp Support, um Hilfe beim Wiederherstellen der integrierten Schlüsselmanagementinformationen zu erhalten.

28. Boot-Node im Startmenü:

```
boot_ontap menu
```

Wenn Sie nicht über eine FC- oder UTA/UTA2-Konfiguration verfügen, führen Sie die entsprechenden Aufgaben aus "UTA/UTA2-Ports in node4, Schritt 15, prüfen und konfigurieren" Damit node4 die Festplatten von node2 erkennen kann.

29. für MetroCluster Konfigurationen, V-Series Systeme und Systeme mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist, finden Sie den Link:set_fc_or_uta_uta2_config_node4.HTML#Auto_Check_4_step15[UTA/UTA2-Ports auf node4 prüfen und konfigurieren, Schritt 15].

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest

Wenn node4 über integrierte FC-Ports, integrierte Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte verfügt, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschnitt oder oder beide Abschnitte ausfüllen Konfigurieren Sie FC-Ports auf node4 UTA/UTA2-Ports auf node4 prüfen und konfigurieren .

> Wenn node4 keine integrierten FC-Ports, Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie zur springen "Weisen Sie Ports von node2 nach node4 zu" Abschnitt. Wenn Sie jedoch ein V-Series System oder FlexArray-Virtualisierungssoftware haben und mit Storage-Arrays verbunden sind und node4 keine integrierten FC-Ports, Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie zurück in den Abschnitt *Installation und Boot-node4* und wieder aufnehmen "Schritt 22". stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt. Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node4
- UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node4

Wenn node4 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in den Dienst stellen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node2 haben, die Sie im Abschnitt gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder einen UTA/UTA2-Adapter verfügt, konfigurieren Sie sie in UTA/UTA2-Ports auf node4 prüfen und konfigurieren.

> Wenn im System Storage-Festplatten vorhanden sind, müssen Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle eingeben. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware haben, die mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

2. Vergleichen Sie die FC-Einstellungen auf node4 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
3. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…

Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node4 nach Bedarf:
	• So programmieren Sie Zielanschlüsse:
	`ucadmin modify -m fc -t target adapter`
	• So programmieren Sie Initiator-Ports:
	`ucadmin modify -m fc -t initiator adapter`
	`-t` Ist der FC4-Typ: Target oder Initiator.

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node4 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

4. Beenden des Wartungsmodus:

   ```
   halt
   ```

5. Booten Sie das System über die LOADER-Eingabeaufforderung:

   ```
   boot_ontap menu
   ```

6. Nachdem Sie den Befehl eingegeben haben, warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
7. Wählen Sie die Option `5` Wählen Sie im Bootmenü für den Wartungsmodus aus.
8. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Überspringen Sie diesen Abschnitt und gehen Sie zu "Weisen Sie Ports von node2 nach node4 zu" Wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Gehen Sie zu "UTA/UTA2-Ports auf node4 prüfen und konfigurieren" Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt *UTA/UTA2-Ports auf node4* überprüfen und konfigurieren, wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat, zurück zum Abschnitt *Installation und Boot node4*, und wieder bei aufnehmen "Schritt 23".

UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Wenn node4 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie je nach Nutzung des aktualisierten Systems konfigurieren.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht es, gleichzeitig NIC- und FCoE-Datenverkehr die gleiche 10-GbE-SFP+-Schnittstelle zu nutzen und das FC-Ziel zu unterstützen.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

UTA2-Ports können an einem Adapter oder auf dem Controller mit den folgenden Konfigurationen verwendet werden:

- UTA-/UTA2-Karten, die gleichzeitig mit dem Controller bestellt wurden, werden vor dem Versand konfiguriert, um die von Ihnen angeforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden konfiguriert (vor dem Versand), um die von Ihnen angeforderte Persönlichkeit zu besitzen.

Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf node4 überprüfen und sie gegebenenfalls ändern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein MetroCluster FC-System, ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware verfügen, die mit Storage-Arrays verbunden ist, müssen Sie sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit mit einem der folgenden Befehle auf node4 konfiguriert werden:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node    Adapter Mode     Type       Mode      Type      Status
----    ------- ---      ---------  -------   --------  -------
f-a     0e      fc       initiator  -          -        online
f-a     0f      fc       initiator  -          -        online
f-a     0g      cna      target     -          -        online
f-a     0h      cna      target     -          -        online
f-a     0e      fc       initiator  -          -        online
f-a     0f      fc       initiator  -          -        online
f-a     0g      cna      target     -          -        online
f-a     0h      cna      target     -          -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Überprüfen Sie die Ausgabe des `ucadmin show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.
4. Führen Sie eine der folgenden Aktionen durch:

Wenn die CNA-Ports…	**Dann…**
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	**Dann…**
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

6. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

7. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

- `-m` Ist der Personality-Modus, FC oder 10GbE UTA.
- `-t` Ist der Typ FC4, `target` Oder `initiator`.

> Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

8. Überprüfen Sie die Einstellungen mit dem folgenden Befehl und prüfen Sie die Ausgabe:

```
ucadmin show
```

9. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`ucadmin show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
*> ucadmin show
Node  Adapter  Current Mode  Current Type  Pending Mode  Pending Type
Admin Status
----  -------  ------------  ------------  ------------  ------------
------------
f-a   1a       fc             initiator    -             -
online
f-a   1b       fc             target       -             initiator
online
f-a   2a       fc             target       cna           -
online
f-a   2b       fc             target       cna           -
online
4 entries were displayed.
*>
```

10. Platzieren Sie alle Ziel-Ports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`

Wenn das System…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config adapter_name up`

11. Verkabeln Sie den Port.
12. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Wechseln Sie zum Abschnitt "Weisen Sie Ports von node2 nach node4 zu".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zum Abschnitt *Installieren und Starten von node4* zurück, und fahren Sie bei fort "Schritt 23".

13. Wartungsmodus beenden:

```
halt
```

14. Boot-Knoten in Boot-Menü:

```
boot_ontap menu
```

Wenn Sie ein Upgrade auf eine A800 durchführen, gehen Sie zu Schritt 23.

15. in node4 wechseln Sie zum Startmenü und wählen Sie unter 22/7 die ausgeblendete Option aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node2 ein, um die Festplatten von node2 node4 wie im folgenden Beispiel neu zuzuweisen.

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu ...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
.
.
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.
Selection (1-9)? 22/7
.
.
(boot_after_controller_replacement) Boot after controller upgrade
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.

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.
Selection (1-9)? boot_after_controller_replacement
```

```
.
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes
.
.
Controller Replacement: Provide name of the node you would like to
replace: <name of the node being replaced>
.
.
Changing sysid of node <node being replaced> disks.
Fetched sanown old_owner_sysid = 536953334 and calculated old sys id
= 536953334
Partner sysid = 4294967295, owner sysid = 536953334
.
.
.
Terminated
<node reboots>
.
.
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
.
.
System rebooting...
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
Login: ...
```

16. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, Das liegt daran, dass es die Ports wieder in den Zielmodus zurückgesetzt hat und somit keine Disketten sehen kann. Weiter mit Schritt 17 Bis Schritt 22 Um dies zu beheben.
17. Drücken Sie während des AUTOBOOTS Strg-C, um den Knoten an der Eingabeaufforderung LOADER> anzuhalten.
18. Wechseln Sie an der LOADER-Eingabeaufforderung in den Wartungsmodus:

    ```
    boot_ontap maint
    ```

19. Zeigen Sie im Wartungsmodus alle zuvor festgelegten Initiator-Ports an, die sich jetzt im Ziel-Modus befinden:

    ```
    ucadmin show
    ```

    Ändern Sie die Ports zurück in den Initiatormodus:

    ```
    ucadmin modify -m fc -t initiator -f adapter name
    ```

20. Vergewissern Sie sich, dass die Ports in den Initiatormodus geändert wurden:

    ```
    ucadmin show
    ```

21. Beenden des Wartungsmodus:

    ```
    halt
    ```

    > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten unterstützt, auf ein System, das auch externe Festplatten unterstützt, gehen Sie zu Schritt 22.
    >
    > Wenn Sie ein Upgrade von einem System durchführen, das externe Festplatten verwendet, zu einem System, das sowohl interne als auch externe Festplatten unterstützt, z. B. ein AFF A800 System, finden Sie unter Schritt 23.

22. Starten Sie an der LOADER-Eingabeaufforderung:

    ```
    boot_ontap menu
    ```

    Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

    Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her:

    a. Zurück zum speziellen Startmenü:

       ```
       LOADER> boot_ontap menu
       ```

```
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)? 10
```

a. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

b. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

c. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

d. Geben Sie bei Aufforderung die Backup-Daten ein.

> Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Abschnitt dieses Verfahrens.

e. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus

> In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in Schritt 22 Bis das System ordnungsgemäß gebootet wird.

23. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. AFF A800 Systeme), setzen Sie das node2-Aggregat als Root-Aggregat ein, um zu bestätigen, dass node4 aus dem Root-Aggregat von node2 startet. Zum Festlegen des Root-Aggregats rufen Sie das Boot-Menü auf und wählen dann Option `5` Um in den Wartungsmodus zu wechseln.

> **Die folgenden Teilschritte müssen in der angegebenen Reihenfolge ausgeführt werden; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.**

Mit dem folgenden Verfahren wird node4 vom Root-Aggregat von node2 gestartet:

a. Wechseln in den Wartungsmodus:

```
boot_ontap maint
```

b. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node2 Aggregat:

```
aggr status -r
```

c. Überprüfen Sie den Status des node2-Aggregats:

```
aggr status
```

d. Bei Bedarf das node2 Aggregat online bringen:

```
aggr_online root_aggr_from_node2
```

e. Verhindern Sie, dass das node4 aus dem ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node4
```

f. Legen Sie das node2-Root-Aggregat als das neue Root-Aggregat für node4 fest:

```
aggr options aggr_from_node2 root
```

Weisen Sie Ports von node2 nach node4 zu

Sie müssen überprüfen, ob die physischen Ports auf node2 den physischen Ports auf node4 korrekt zugeordnet sind. Dadurch kann node4 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Über diese Aufgabe

Siehe "Quellen" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

die Softwarekonfiguration von node4 muss mit der physischen Konnektivität von node4 übereinstimmen und die IP-Konnektivität muss wiederhergestellt werden, bevor Sie das Upgrade fortsetzen.

Die Port-Einstellungen können je nach Modell der Nodes variieren. Sie müssen den Port des ursprünglichen Node und die LIF-Konfiguration mit dem kompatibel machen, was Sie planen, die Konfiguration des neuen Node zu verwenden. Dies liegt daran, dass der neue Node beim Booten die gleiche Konfiguration wiedergibt. Dies bedeutet, wenn Sie node4 booten, wird Data ONTAP versuchen, LIFs auf den gleichen Ports zu hosten, die in node2 verwendet wurden.

Wenn die physischen Ports auf node2 also nicht direkt den physischen Ports auf node4 zugeordnet werden, sind daher Änderungen der Software-Konfiguration erforderlich, um nach dem Booten die Cluster-, Management- und Netzwerkkonnektivität wiederherzustellen. Wenn die Cluster-Ports auf node2 zudem nicht direkt den Cluster-Ports auf node4 zugeordnet werden, wird node4 beim Neustart möglicherweise nicht automatisch dem Quorum beitreten, bis die Software-Konfiguration geändert wird, um die Cluster LIFs auf den korrekten physischen Ports zu hosten.

Schritte

1. Notieren Sie alle node2-Verkabelungsinformationen für node2, die Ports, Broadcast-Domänen und IPspaces in der Tabelle:

LIF	Anzahl an Knoten2-Ports	Node2-IPspaces	Node2 Broadcast-Domänen	Node4-Ports	Node4 IPspaces	Node4 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						

2. Zeichnen Sie alle Kabelinformationen für node4, die Ports, Broadcast-Domänen und IPspaces in der Tabelle auf.
3. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob es sich bei dem Setup um ein 2-Node-Cluster ohne Switches handelt:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      ```
      cluster::> set -privilege advanced
      ```

   b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

      ```
      cluster::> network options switchless-cluster show
      ```

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

+
Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

   a. Zurück zur Administratorberechtigungsebene:

```
cluster::*> set -privilege admin
cluster::>
```

4. Gehen Sie folgendermaßen vor, um node4 in Quorum zu platzieren:

   a. Boot node4. Siehe "installieren und booten sie node4" Um den Node zu booten, wenn Sie dies noch nicht getan haben.

   b. Vergewissern Sie sich, dass sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden:

      `network port show -node node -port port -fields broadcast-domain`

      Das folgende Beispiel zeigt, dass Port „e0a“ in der Cluster-Domäne auf node4 ist:

      ```
      cluster::> network port show -node node4 -port e0a -fields broadcast-
      domain
      node       port broadcast-domain
      ---------- ---- ---------------
      node4      e0a  Cluster
      ```

   c. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domäne befinden, fügen Sie sie mit dem folgenden Befehl hinzu:

      `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports node:port`

   d. Fügen Sie die korrekten Ports zur Cluster Broadcast-Domäne hinzu:

      `network port modify -node -port -ipspace Cluster -mtu 9000`

      Dieses Beispiel fügt Cluster-Port „e1b“ auf node4 hinzu:

      `network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000`

   e. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

      `network interface migrate -vserver Cluster -lif lif_name -source-node node4 destination-node node4 -destination-port port_name`

   f. Ändern Sie den Startport der Cluster-LIFs:

      `network interface modify -vserver Cluster -lif lif_name –home-port port_name`

   g. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne:

      `network port broadcast-domain remove-ports`

      Dieser Befehl entfernt Port „e0d“ auf node4:

`network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain Cluster -ports node4:e0d`

   a. Vergewissern Sie sich, dass node4 Quorum erneut verbunden hat:

      `cluster show -node node4 -fields health`

5. Anpassen der Broadcast-Domänen, die Ihre Cluster-LIFs hosten, sowie Node-Management/clustermanagement-LIFs. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie möglicherweise die LIFs migrieren und ändern müssen, wie in den folgenden Schritten dargestellt:

   a. Zeigen Sie den Startport einer logischen Schnittstelle an:

      ```
      network interface show -fields home-node,home-port
      ```

   b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

      ```
      network port broadcast-domain show -ports node_name:port_name
      ```

   c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:

      ```
      network port broadcast-domain add-ports
      network port broadcast-domain remove-ports
      ```

   d. Ändern Sie den Home-Port eines LIF:

      ```
      network interface modify -vserver vserver -lif lif_name –home-port port_name
      ```

6. Passen Sie die Intercluster-Broadcast-Domänen an und migrieren Sie gegebenenfalls die Intercluster LIFs mithilfe derselben Befehle, die in dargestellt sind Schritt 5.
7. Passen Sie alle anderen Broadcast-Domänen an und migrieren Sie die Daten-LIFs, falls erforderlich, mit denselben Befehlen in Schritt 5.
8. Wenn in node4 keine Ports mehr vorhanden sind, löschen Sie diese wie folgt:

   a. Zugriff auf die erweiterte Berechtigungsebene auf beiden Nodes:

      ```
      set -privilege advanced
      ```

   b. So löschen Sie die Ports:

      ```
      network port delete -node node_name -port port_name
      ```

   c. Zurück zur Administratorebene:

      ```
      set -privilege admin
      ```

9. Passen Sie alle LIF Failover-Gruppen an:

   ```
   network interface modify -failover-group failover_group -failover-policy
   failover_policy
   ```

   Mit dem folgenden Befehl wird die Failover-Richtlinie auf festgelegt `broadcast-domain-wide` Und verwendet die Ports in Failover-Gruppe `fg1` Als Failover-Ziele für LIF `data1` Ein `node4`:

   ```
   network interface modify -vserver node4 -lif data1 failover-policy broadcast-
   domainwide –failover-group fg1
   ```

   Siehe "Quellen" Weitere Informationen finden Sie unter *Netzwerkverwaltung* oder den Befehlen *ONTAP 9: Manual Page Reference* unter *Failover-Einstellungen auf LIF konfigurieren*.

10. Überprüfen Sie die Änderungen auf node4:

    ```
    network port show -node node4
    ```

11. Jedes Cluster-LIF muss an Port 7700 zuhören. Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören:

    ```
    ::> network connections listening show -vserver Cluster
    ```

    Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

    ```
    Cluster::> network connections listening show -vserver Cluster
    Vserver Name     Interface Name:Local Port     Protocol/Service
    ---------------- ----------------------------  -------------------
    Node: NodeA
    Cluster          NodeA_clus1:7700               TCP/ctlopcp
    Cluster          NodeA_clus2:7700               TCP/ctlopcp
    Node: NodeB
    Cluster          NodeB_clus1:7700               TCP/ctlopcp
    Cluster          NodeB_clus2:7700               TCP/ctlopcp
    4 entries were displayed.
    ```

12. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

    ```
    ::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
    int modify -vserver Cluster -lif cluster-lif -status-admin up
    ```

    Wiederholen Sie Schritt 11, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

Fügen Sie dem Quorum bei, wenn ein Node über einen anderen Satz an Netzwerkports verfügt

Der Node mit dem neuen Controller bootet und versucht zuerst, dem Cluster automatisch beizutreten. Wenn der neue Node jedoch einen anderen Satz an Netzwerkports aufweist, müssen Sie die folgenden Schritte durchführen, um zu bestätigen, dass der Node dem Quorum erfolgreich hinzugefügt wurde.

Über diese Aufgabe

Sie können diese Anweisungen für alle relevanten Knoten verwenden. Node3 wird in der folgenden Probe verwendet.

Schritte

1. Überprüfen Sie, ob sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

    ```
    network port show -node node -port port -fields broadcast-domain
    ```

    Das folgende Beispiel zeigt, dass sich der Port „e1a“ in der Cluster-Domäne auf node3 befindet:

```
cluster::> network port show -node node3 -port e1a -fields broadcast-
domain
node    port  broadcast-domain
------  ----  ---------------
node3   e1a   Cluster
```

2. Fügen Sie die korrekten Ports zur Cluster Broadcast-Domäne hinzu, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

   ```
   network port modify -node -port -ipspace Cluster -mtu 9000
   ```

   Dieses Beispiel fügt Cluster-Port „e1b“ auf Knoten3 hinzu:

   ```
   network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
   ```

3. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF, und verwenden Sie den folgenden Befehl:

   ```
   network interface migrate -vserver Cluster -lif lif_name -source-node node3
   destination-node node3 -destination-port port_name
   ```

4. Ändern Sie den Home-Port der Cluster-LIFs wie folgt:

   ```
   network interface modify -vserver Cluster -lif lif_name –home-port port_name
   ```

5. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domäne befinden, fügen Sie sie mit dem folgenden Befehl hinzu:

   ```
   network port broadcast-domain add-ports -ipspace Cluster -broadcastdomain
   Cluster ports node:port
   ```

6. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne. Sie können für jeden relevanten Knoten verwenden. Mit dem folgenden Befehl wird der Port „e0d“ auf node3 entfernt:

   ```
   network port broadcast-domain remove-ports network port broadcast-domain
   remove-ports ipspace Cluster -broadcast-domain Cluster -ports node3:e0d
   ```

7. Vergewissern Sie sich, dass sich der Node erneut dem Quorum angeschlossen hat:

   ```
   cluster show -node node3 -fields health
   ```

8. Passen Sie die Broadcast-Domänen an, die Ihre Cluster-LIFs und LIFs für das Node-Management/Cluster-Management hosten. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie die LIFs möglicherweise wie folgt migrieren und ändern müssen:

   a. Zeigen Sie den Startport einer logischen Schnittstelle an:

      ```
      network interface show -fields home-node,home-port
      ```

b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:

```
network port broadcast-domain add-ports network port broadcast-domain
remove-port
```

d. Ändern eines Startports einer LIF:

```
network interface modify -vserver vserver-name -lif lif_name –home-port
port_name
```

Passen Sie die Intercluster-Broadcast-Domänen an und migrieren Sie gegebenenfalls die Intercluster LIFs. Die Daten-LIFs bleiben unverändert.

Überprüfen Sie die installation von node4

Nach der Installation und dem Booten von node4 müssen Sie überprüfen, ob node4 korrekt installiert ist, dass er Teil des Clusters ist und mit node3 kommunizieren kann.

Über diese Aufgabe

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node4 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node4 dem Quorum beigetreten ist:

   ```
   cluster show -node node4 -fields health
   ```

2. Vergewissern Sie sich, dass node4 Teil desselben Clusters wie node3 und des entsprechenden Clusters ist, indem Sie den folgenden Befehl eingeben:

   ```
   cluster show
   ```

3. Überprüfen Sie den Status des Vorgangs, und überprüfen Sie, ob die Konfigurationsinformationen für node4 identisch sind mit node2:

   ```
   system controller replace show-details
   ```

   Wenn sich die Konfiguration für node4 unterscheidet, kann es zu einem späteren Zeitpunkt zu einer Systemunterbrechung kommen.

4. Überprüfen Sie, ob der ersetzte Controller für MetroCluster-Konfiguration und nicht im Switch-Over-Modus korrekt konfiguriert ist.

   Achtung: in dieser Phase befindet sich die MetroCluster-Konfiguration nicht im normalen Zustand, und es können Fehler auftreten, die behoben werden können. Siehe "Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration".

VLANs, Schnittstellengruppen und Broadcast-Domänen auf node4 neu erstellen

Nachdem Sie bestätigt haben, dass node4 sich im Quorum befindet und mit node3 kommunizieren kann, müssen Sie die VLANs, Schnittstellengruppen und Broadcast-Domänen von node2 auf node4 neu erstellen. Sie müssen auch die node3-Ports zu den neu erstellten Broadcast-Domänen hinzufügen.

Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "Quellen" Und Link zu *Network Management*.

Schritte

1. Erstellen Sie die VLANs auf node4 mithilfe der node2-Informationen, die im aufgezeichnet wurden, neu "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3" Abschnitt:

   `network port vlan create -node node4 -vlan vlan-names`

2. Erstellen Sie die Schnittstellengruppen auf node4 mithilfe der node2-Informationen, die im aufgezeichnet wurden, neu "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3" Abschnitt:

   `network port ifgrp create -node node4 -ifgrp port_ifgrp_names-distr-func`

3. Erstellen Sie die Broadcast-Domänen auf node4 mithilfe der node2-Informationen, die im aufgezeichnet wurden, erneut "Verschieben von Aggregaten und NAS-Daten-LIFs ohne Root-Wurzeln von Knoten 2 auf Knoten 3" Abschnitt:

   `network port broadcast-domain create -ipspace Default -broadcast-domain broadcast_domain_names -mtu mtu_size -ports node_name:port_name,node_name:port_name`

4. Fügen Sie die node4-Ports zu den neu erstellten Broadcast-Domänen hinzu:

   `network port broadcast-domain add-ports -broadcast-domain broadcast_domain_names -ports node_name:port_name,node_name:port_name`

Wiederherstellen der Key-Manager-Konfiguration auf node4

Wenn Sie NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) zur Verschlüsselung von Volumes auf dem System verwenden, das Sie aktualisieren, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht wiederherstellen, werden beim Verschieben der Node2-Aggregate mit ARL von node3 auf node4 verschlüsselte Volumes offline geschaltet.

Schritte

1. Führen Sie zum Synchronisieren der Verschlüsselungskonfiguration für Onboard Key Manager den folgenden Befehl an der Cluster-Eingabeaufforderung aus:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 oder 9.7	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

2. Geben Sie die Cluster-weite Passphrase für das Onboard Key Manager ein.

Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, von node3 auf node4

Nachdem Sie die node4-Installation überprüft haben und bevor Sie Aggregate von node3 auf node4 verschieben, müssen Sie die NAS-Daten-LIFs von node2 verschieben, die sich derzeit in node3 von node3 nach node4 befinden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node4 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs ordnungsgemäß sind und sich in den entsprechenden Ports befinden, nachdem Sie node4 in den Online-Modus versetzt haben.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

   - Cluster-Quorum-Prüfung
   - System-ID-Prüfung
   - Prüfung der Bildversion
   - Überprüfung der Zielplattform
   - Prüfung der Netzwerkanachabilität

   Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

2. Überprüfen Sie manuell, ob das Netzwerk und alle VLANs, Schnittstellengruppen und Broadcast-Domänen korrekt konfiguriert wurden.
3. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   ```
   To complete the "Network Reachability" phase, ONTAP network
   configuration must be manually adjusted to match the new physical
   network configuration of the hardware. This includes assigning network
   ports to the correct broadcast domains,creating any required ifgrps and
   VLANs, and modifying the home-port parameter of network interfaces to
   the appropriate ports.Refer to the "Using aggregate relocation to
   upgrade controller hardware on a pair of nodes running ONTAP 9.x"
   documentation, Stages 3 and 5. Have all of these steps been manually
   completed? [y/n]
   ```

4. Eingabe `y` Um fortzufahren.
5. Das System führt folgende Prüfungen durch:
   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Prüfungen werden die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node2 befinden, an den neuen Controller node4 verschoben. Das System hält an, sobald die Ressourcenverlagerung abgeschlossen ist.
6. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

   ```
   system controller replace show-details
   ```
7. Überprüfen Sie manuell, ob die nicht-Root-Aggregate und NAS-Daten-LIFs erfolgreich in node4 verschoben wurden.

   Falls Aggregate nicht verschoben oder ein Vetoo eingesetzt werden kann, müssen sie die Aggregate manuell verschieben oder – falls erforderlich – entweder die Vetos oder Zielprüfungen überschreiben. Siehe Abschnitt "Verschiebung ausgefallener oder Vetos von Aggregaten" Finden Sie weitere Informationen.
8. Vergewissern Sie sich, dass sich die SAN-LIFs auf den richtigen Ports auf node4 befinden, indem Sie die folgenden Teilschritte ausführen:
   a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

      ```
      network interface show -data-protocol iscsi|fcp -home-node node4
      ```

      Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

      ```
      cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical    Status     Network            Current Current Is
      Vserver Interface  Admin/Oper Address/Mask      Node    Port    Home
      ------- ---------- ---------- ----------------- ------- ------- ---
      vs0
              a0a        up/down    10.63.0.53/24     node3   a0a     true
              data1      up/up      10.63.0.50/18     node3   e0c     true
              rads1      up/up      10.63.0.51/18     node3   e1a     true
              rads2      up/down    10.63.0.52/24     node3   e1b     true
      vs1
              lif1       up/up      172.17.176.120/24 node3   e0c     true
              lif2       up/up      172.17.176.121/24 node3   e1a     true
      ```
   b. Wenn node4 eine SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der nicht in node2 vorhanden war oder einem anderen Port zugeordnet werden muss, verschieben Sie sie in einen entsprechenden Port auf node4, indem Sie die folgenden Teilschritte ausführen:
      i. Stellen Sie den LIF-Status auf „down“ ein, indem Sie den folgenden Befehl eingeben:

         ```
         network interface modify -vserver vserver_name -lif lif_name -status
         ```

```
-admin down
```

ii. Entfernen Sie das LIF aus dem Portsatz:

```
portset remove -vserver vserver_name -portset portset_name -port-name
port_name
```

iii. Geben Sie einen der folgenden Befehle ein:

- Verschieben Sie ein einzelnes LIF durch Eingabe des folgenden Befehls:

```
network interface modify -vserver vserver_name -lif lif_name -home
-port new_home_port
```

- Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen neuen Port, indem Sie den folgenden Befehl eingeben:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

Sie müssen bestätigen, dass Sie SAN LIFs zu einem Port mit der gleichen Verbindungsgeschwindigkeit wie der ursprüngliche Port verschieben.

a. Ändern Sie den Status aller LIFs in `up` Damit die LIFs Datenverkehr auf dem Node akzeptieren und senden können, indem Sie den folgenden Befehl eingeben:

```
network interface modify -home-port port_name -home-node node4 -lif data
-statusadmin up
```

b. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von aufweisen `up` Wenn Sie auf einem der beiden Nodes den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network interface show -home-node <node4> -role data
```

c. Wenn irgendwelche LIFs ausgefallen sind, setzen Sie den Administratorstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif lif_name -status-admin
up
```

9. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

```
system controller replace resume
```

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung

- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

MetroCluster FC-Konfiguration

In einer MetroCluster FC-Konfiguration müssen die Knoten für Disaster Recovery/Failover-Standort so schnell wie möglich ersetzt werden. Nicht übereinstimmende Controller-Modelle in einem MetroCluster wird nicht unterstützt, weil eine falsche Übereinstimmung des Controller-Modells dazu führen kann, dass Disaster Recovery-Spiegelung offline geht. Umgehen Sie MetroCluster-Überprüfungen mit dem `-skip -metrocluster-check true` Befehl, wenn Sie Nodes am zweiten Standort ersetzen.

Authentifizierungsmanagement mit KMIP-Servern

Von ONTAP 9.5 bis 9.7 können KMIP-Server (Key Management Interoperability Protocol) Authentifizierungsschlüssel managen.

Schritte

1. Hinzufügen eines neuen Controllers:

   ```
   security key-manager setup -node new_controller_name
   ```

2. Fügen Sie den Schlüsselmanager hinzu:

   ```
   security key-manager -add key_management_server_ip_address
   ```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

```
security key-manager restore -node new_controller_name
```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um das korrekte Setup zu bestätigen, müssen Sie das HA-Paar aktivieren. Sie müssen außerdem überprüfen, dass Node3 und node4 auf den Storage der jeweils anderen Person zugreifen können und dass keine der logischen Datenschnittstellen zu anderen Nodes im Cluster vorhanden sind. Darüber hinaus müssen Sie bestätigen, dass Node3 zu Aggregaten node1 gehört und dass node4 die Aggregate von node2 besitzt und dass die Volumes für beide Nodes online sind.

Schritte

1. Nach den Tests nach der Prüfung von „node2“ werden das Storage Failover und das Cluster HA-Paar für den node2 Cluster aktiviert. Nach Abschluss des Vorgangs werden beide Nodes als abgeschlossen angezeigt, und das System führt einige Bereinigungsvorgänge aus.
2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

```
storage failover show
```

Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

```
cluster::> storage failover show
                    Takeover
Node     Partner  Possible   State Description
-------- -----    -------    ------------------
node3    node4    true       Connected to node4
node4    node3    true       Connected to node3
```

3. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

```
cluster show
```

4. Stellen Sie sicher, dass node3 und node4 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

```
storage failover show -fields local-missing-disks, partner-missing-disks
```

5. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

```
network interface show
```

Wenn keine der Knoten „Node3“ oder „node4“ Daten-LIFs besitzt, die sich im Besitz anderer Nodes im

Cluster befinden, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

```
network interface revert
```

6. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

   ```
   storage aggregate show -owner-name node3
   ```

   ```
   storage aggregate show -owner-name node4
   ```

7. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node node3 -state offline
   ```

   ```
   volume show -node node4 -state offline
   ```

8. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie im Abschnitt erfasst haben "Bereiten Sie die Knoten für ein Upgrade vor", Und Online-Laufwerk eines der Offline-Volumes, nach Bedarf, durch Verwendung des folgenden Befehls, einmal für jedes Volume:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

9. Installieren Sie neue Lizenzen für die neuen Nodes mithilfe des folgenden Befehls für jeden Node:

   ```
   system license add -license-code license_code,license_code,license_code…
   ```

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

10. Entfernen Sie alle alten Lizenzen mithilfe eines der folgenden Befehle von den ursprünglichen Nodes:

    ```
    system license clean-up -unused -expired
    ```

    ```
    system license delete -serial-number node_serial_number -package
    licensable_package
    ```

    - Alle abgelaufenen Lizenzen löschen:

      ```
      system license clean-up -expired
      ```

    - Alle nicht verwendeten Lizenzen löschen:

      ```
      system license clean-up -unused
      ```

    - Löschen Sie eine bestimmte Lizenz von einem Cluster mit den folgenden Befehlen auf den Nodes:

      ```
      system license delete -serial-number node1_serial_number -package *
      ```

      ```
      system license delete -serial-number node2_serial_number -package *
      ```

    Die folgende Ausgabe wird angezeigt:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

Eingabe `y` Um alle Pakete zu entfernen.

11. Überprüfen Sie, ob die Lizenzen korrekt installiert sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

    `system license show`

    Sie können die Ausgabe mit der im Abschnitt erfassten Ausgabe vergleichen "Bereiten Sie die Knoten für ein Upgrade vor".

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie die eingestellt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel in "installieren und booten sie node4, Schritt 27"), Sie müssen die Einstellung der Variable aufheben:

    `set diag; systemshell -node node_name -command sudo kenv -u -p kmip.init.maxwait`

13. Konfigurieren Sie die SPs mit dem folgenden Befehl auf beiden Knoten:

    `system service-processor network modify -node node_name`

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen *ONTAP 9: Manual Page Reference* für detaillierte Informationen zum System `service-processor network modify` Befehl.

14. Informationen zum Einrichten eines Clusters ohne Switches auf den neuen Nodes finden Sie unter "Quellen" Um eine Verbindung zur NetApp Support Site_ zu erhalten, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node3 und node4 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager show -status

   security key-manager query
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.
   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.
   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.
4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager restore -node new_controller_name
   ```

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

ONTAP 9.6 und 9.7

Konfigurieren Sie NVE oder NAE auf Controllern mit ONTAP 9.6 oder 9.7

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server.

      Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her.

   - Authentifizierung für externen Schlüsselmanager wiederherstellen:

     ```
     security key-manager external restore
     ```

     Für diesen Befehl ist die OKM-Passphrase (Onboard Key Manager) erforderlich.

   Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

   - Authentifizierung für den OKM wiederherstellen:

     ```
     security key-manager onboard sync
     ```

ONTAP 9.5

NVE oder NAE auf Controllern mit ONTAP 9.5 konfigurieren

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server.

      Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her.

   - Authentifizierung für externen Schlüsselmanager wiederherstellen:

     ```
     security key-manager external restore
     ```

     Für diesen Befehl ist die OKM-Passphrase (Onboard Key Manager) erforderlich.

   Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

   - Restore-Authentifizierung für OKM:

     ```
     security key-manager setup -node node_name
     ```

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder externe Schlüsselverwaltungsserver nicht erreicht werden konnten. Stellen Sie diese Volumes mit der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht

migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "Überblick über das ARL Upgrade". Informationen über mögliche Ausfälle werden in der Phase des Verfahrens aufgelistet.

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   ```
   storage aggregate relocation show
   ```

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 waren, gehören node4 nach Abschluss des Upgrades

Beim Abschluss des Upgrade-Verfahrens sollte die Knoten3 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node die Knoten1 hatten. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Unter den folgenden Umständen kann es nicht gelingen, Aggregate ordnungsgemäß zu verschieben und Node 1 als Home Node anstelle von Knoten3 zu verwenden:

- In Phase 3, wenn Aggregate von node2 auf node3 verschoben werden. Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann wird das Aggregat auf node2 zurückgelassen.
- Nach Stufe 4, wenn node2 durch node4 ersetzt wird. Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node4 als Home-Node statt node3 online.

Sie können das falsche Eigentümerproblem nach Phase 6 beheben, wenn ein Storage-Failover aktiviert wurde, indem Sie die folgenden Schritte durchführen:

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Liste der Aggregate zu erhalten:

   `storage aggregate show -nodes node4 -is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 mit der Ausgabe, die Sie für Knoten 1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links auf node4:

   `storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3`

   Verwenden Sie das nicht `-ndo-controller-upgrade` Parameter während dieser Verschiebung.

4. Vergewissern Sie sich, dass node3 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht über Node3 als Hausbesitzer verfügen, können mit dem gleichen Relocation-Befehl in auf node3 verschoben werden Schritt 3.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, in Panik geraten oder aus- und wieder eingeschaltet werden.

Die Lösung dieser Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikzugänge oder Energiezyklen während der Vorprüfphase

Node1 oder node2 stürzt vor der Pre-Check-Phase ab, während das HA-Paar noch aktiviert ist

Wenn node1 oder node2 vor der Pre-Check-Phase abstürzt, wurden noch keine Aggregate verschoben und die HA-Paar-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während der ersten Resource-Release-Phase ab, während das HA-Paar noch aktiviert ist

Einige oder alle Aggregate wurden von node1 in node2 verschoben und das HA-Paar ist noch aktiviert. Node2 übernimmt das Root-Volume von node1 und alle nicht-Root-Aggregate, die nicht verschoben wurden.

Über diese Aufgabe

Eigentum an Aggregaten, die verschoben wurden, sehen genauso aus wie das Eigentum von nicht-Root-Aggregaten, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat.

Wenn node1 in den eintritt `waiting for giveback` Status, node2 gibt alle node1 nicht-Root-Aggregate zurück.

Schritte

1. Nachdem node1 gestartet wurde, sind alle nicht-Root-Aggregate von node1 zurück in node1 verschoben. Sie müssen eine manuelle Aggregatverschiebung der Aggregate von node1 nach node2 durchführen: `storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true`
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während der ersten Ressourcen-Release-Phase ab, während das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 schlägt während der ersten Phase der Ressourcenfreigabe fehl, während das HA-Paar noch aktiviert ist

Node1 hat einige oder alle seine Aggregate in node2 verschoben. Das HA-Paar ist aktiviert.

Über diese Aufgabe

Node1 übernimmt alle node2 Aggregate sowie jedes seiner eigenen Aggregate, die auf node2 verschoben wurden. Beim Booten von node2 wird die Aggregatverschiebung automatisch abgeschlossen.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während der ersten Resource-Release-Phase ab und nachdem HA-Paar deaktiviert ist

Node1 übernimmt nicht.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem verbleibenden Upgrade des Node-Paars fort.

Startet während der ersten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node2 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

Node3 übernimmt nach einem Absturz nach einem node2 nicht, da das HA-Paar bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall tritt für alle Aggregate auf, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt in der ersten Verifizierungsphase ab, wobei das HA-Paar deaktiviert ist

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der ersten Ressourcen-Wiederholen-Phase

Knoten 2 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Node2 hat einige oder alle seine Aggregate von node1 in node3 verschoben. Node3 stellt Daten von Aggregaten bereit, die verlagert wurden. Das HA-Paar ist deaktiviert und somit gibt es keine Übernahme.

Über diese Aufgabe

Es gibt einen Client-Ausfall für Aggregate, die nicht verschoben wurden. Beim Booten von node2 werden die Aggregate von node1 auf node3 verschoben.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während der ersten Phase zur Ressourcenrückgewinnung während der Aggregatverschiebung ab

Falls node3 abstürzt, während node2 Aggregate zu node3 verschoben wird, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Knoten 3 verlagert wurden, begegnen ein Client-Ausfall, während node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Führen Sie das Controller-Upgrade fort.

Neustarts, Panikspiele oder Energiezyklen während der Nachprüfphase

Node2 oder node3 stürzt während der Post-Check-Phase ab

Das HA-Paar ist deaktiviert, damit dies keine Übernahme ist. Es gibt einen Client-Ausfall für Aggregate, die zum neu gebooteten Node gehören.

Schritte

1. Bringen Sie den Node hoch.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikzucken oder Energiezyklen während der zweiten Ressourcenfreigabephase

Node3 stürzt während der zweiten Resource-Release-Phase ab

Wenn node3 abstürzt, während node2 Aggregate verschoben, wird die Aufgabe nach dem Booten von node3 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Node3 verlagert wurden, und Node3 eigene Aggregate stoßen auf Client-Ausfälle, während Node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Node2 stürzt während der zweiten Resource-Release-Phase ab

Wenn node2 während der Aggregatverschiebung abstürzt, wird node2 nicht übernommen.

Über diese Aufgabe

Node3 dient weiterhin den Aggregaten, die verschoben wurden, doch die Aggregate von node2 stoßen auf Client-Ausfälle.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Controller-Upgrade fort.

Startet während der zweiten Verifikationsphase neu, erzeugt eine Panik oder schaltet die Stromversorgung aus

Node3 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node3 abstürzt, wird die Übernahme nicht durchgeführt, da HA bereits deaktiviert ist.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis nach einem Neustart von Knoten3.

Schritte

1. Knoten 3 aufbring.

Ein Client-Ausfall tritt für alle Aggregate auf, während Node3 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node4 stürzt während der zweiten Verifikationsphase ab

Wenn node4 während dieser Phase abstürzt, wird die Übernahme nicht durchgeführt. Node3 stellt Daten aus den Aggregaten bereit.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis node4 neu startet.

Schritte

1. bringen sie node4 auf.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------   --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder Panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
--------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports lautet `down`.

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.

Inhalt	Beschreibung
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.

Inhalt	Beschreibung
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe",

Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.

Führen Sie ein manuelles Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durch

Überblick

Dieses Verfahren beschreibt das Upgrade der Controller-Hardware mithilfe von Aggregate Relocation (ARL) für die folgenden Systemkonfigurationen:

Methode	ONTAP-Version	Unterstützte Systeme
Manuelles Upgrade mit ARL	9.8 oder höher	• FAS System zu FAS System • FAS System auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System • AFF System zu AFF System • System mit FlexArray Virtualisierungssoftware oder einem V-Series System auf einem FAS System, vorausgesetzt, dass das System mit FlexArray Virtualisierungssoftware oder V-Series System keine Array-LUNs besitzt. • V-Series Systeme auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Außerdem migrieren Sie Daten-logische Schnittstellen (LIFs) und weisen Sie die Netzwerk-Ports auf dem neuen Controller den Schnittstellengruppen zu, während Sie fortfahren.

In diesem Dokument werden die ursprünglichen Knoten *node1* und *node2* genannt, und die neuen Knoten werden *node3* und *node4* genannt. Während des beschriebenen Verfahrens wird node1 durch node3 ersetzt und node2 durch node4 ersetzt. Die Begriffe *node1*, *node2*, *node3* und *node4* werden nur verwendet, um zwischen den ursprünglichen und neuen Knoten zu unterscheiden. Wenn Sie das Verfahren befolgen, müssen Sie die richtigen Namen Ihrer ursprünglichen und neuen Knoten ersetzen. In der Realität ändern sich jedoch die Namen der Nodes nicht: node3 hat den Namen node1 und node4 hat nach dem Upgrade der Controller-Hardware den Namen node2. In diesem Dokument wird der Begriff „ Systems with FlexArray Virtualization Software_“ verwendet, um sich auf Systeme zu beziehen, die zu diesen neuen Plattformen gehören. Dabei wird der Begriff *V-Series System* verwendet, um sich auf die separaten Hardware-Systeme zu beziehen, die an Storage-Arrays angeschlossen werden können

Wichtige Informationen:

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-

Administrationsfähigkeiten verfügen. Sie müssen auch lesen und verstehen, die "Richtlinien für das Controller-Upgrade mit ARL" Und das "ARL Upgrade-Workflow" Abschnitte vor Beginn der Aktualisierung.

- Bei dieser Vorgehensweise wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn bereits die Ersatz-Controller-Hardware verwendet wurde, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP in 7-Mode ausgeführt wurde.
- Mit diesem Verfahren können Sie die Controller-Hardware in Clustern mit mehr als zwei Nodes aktualisieren. Sie müssen jedoch für jedes Hochverfügbarkeitspaar (HA) im Cluster separat vorgehen.
- Dieses Verfahren gilt für FAS Systeme, V-Series Systeme, AFF Systeme und Systeme mit FlexArray Virtualisierungssoftware. FAS Systeme, die nach ONTAP 9 freigegeben wurden, können an Speicher-Arrays angebunden werden, wenn die erforderliche Lizenz installiert ist. Die vorhandenen Systeme der V-Serie werden von ONTAP 9 unterstützt. Informationen zu den Modellen Storage Array und V-Series finden Sie unter "Quellen" Um zu *Hardware Universe* zu verlinken und eine Support-Matrix zur *V-Serie* zu erhalten.
- Neben Konfigurationen, die nicht von MetroCluster stammen, gilt dieses Verfahren für Fabric MetroCluster Konfigurationen mit vier und acht Nodes mit ONTAP 9.8 und höher.
  - Weitere Informationen zu MetroCluster Konfigurationen mit ONTAP 9.7 und früher finden Sie unter "Quellen" Verbinden mit *Aggregat-Verlagerung verwenden, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder früher* durchzuführen.
  - Weitere Upgrade-Optionen für MetroCluster IP-Konfigurationen und zusätzliche Upgrade-Optionen für Fabric-MetroCluster-Konfigurationen finden Sie unter "Quellen" Zum Verlinken auf den Inhalt *MetroCluster Upgrade und Expansion*.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

In diesem Inhalt wird beschrieben, wie Sie die Storage Controller in einem HA-Paar mit neuen Controllern aktualisieren und dabei alle vorhandenen Daten und Festplatten beibehalten. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Verwenden Sie diese Inhalte unter folgenden Umständen:

- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind in der Verwaltung von ONTAP erfahren und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.
- Sie verfügen über ein System, bei dem Fabric MetroCluster Konfigurationen mit 4 und 8 Nodes und ONTAP 9.8 oder höher zum Einsatz kommen.
- Sie nutzen Hybrid-Aggregate auf Ihrem System.

> Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu

ONTAP 9 zugreifen können.

ARL Upgrade-Workflow

Bevor Sie die Nodes mit ARL aktualisieren, müssen Sie zunächst verstehen, wie das Verfahren funktioniert. In diesem Dokument wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

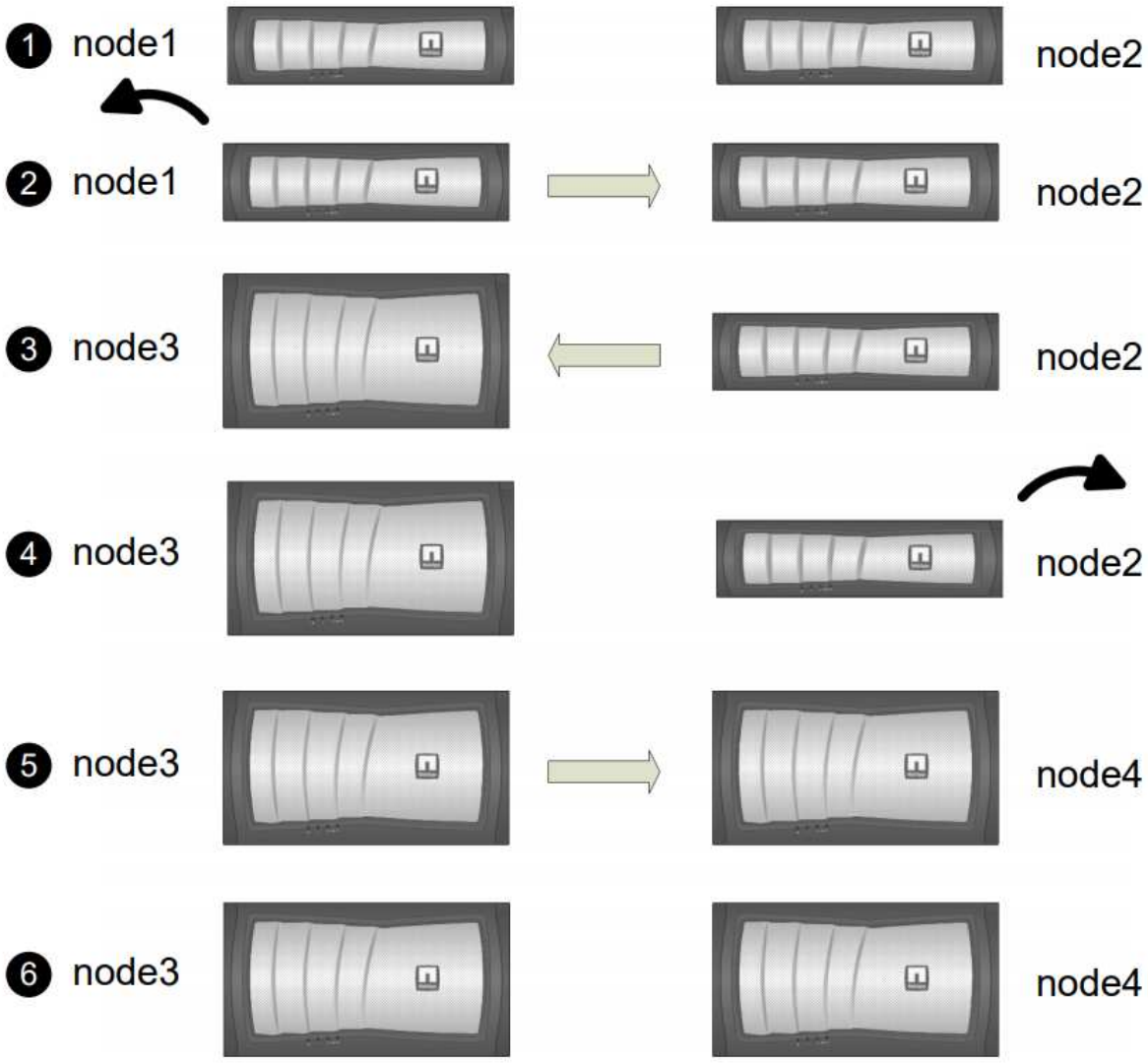
Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und anschließend eine Reihe von Schritten sowohl auf den ursprünglichen als auch auf den neuen Nodes durchführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Abbildung zeigt die Phasen des Verfahrens. Die dicken, hellgrauen Pfeile stehen für die Verschiebung der Aggregate und die Verschiebung der LIFs. Die dünneren schwarzen Pfeile stellen die Entfernung der ursprünglichen Nodes dar. Die kleineren Controller Images stellen die ursprünglichen Nodes dar und die größeren Controller Images repräsentieren die neuen Nodes.



Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Schritte
"Phase 1: Upgrade vorbereiten"	In Phase 1 bestätigen Sie, dass interne Festplatten keine Root-Aggregate oder Datenaggregate enthalten, die Nodes für das Upgrade vorbereiten und mehrere Vorabprüfungen durchführen. Gegebenenfalls können Sie Festplatten für die Storage-Verschlüsselung neu verschlüsseln und die neuen Controller in Vorbereitung nehmen. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate. • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate.
"Stufe 2: Node1 ausmustern"	Während Phase 2 verschieben Sie Aggregate ohne Root-Root-Fehler von Knoten1 auf Knoten2 und verschieben Daten-LIFs, die nicht-SAN-Daten-LIFs gehören, die sich im Besitz von node1 befinden, auf Knoten 2, einschließlich fehlgeschlagener oder Vetos. Sie notieren auch die nötigen Node1-Informationen, die Sie später im Verfahren verwenden können, und setzen node1 aus. Gesamteigentum am Ende von Phase 2: • Node1 ist der Hausbesitzer von node1 Aggregaten. • Node2 ist der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 3: Installieren und booten node3"	In Phase 3 installieren und booten Sie Knoten3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu und verschieben Daten-LIFs und SAN-LIFs, die zu node1 gehören, von node2 auf node3. Außerdem werden alle Aggregate von node2 auf node3 verschoben und die Daten-LIFs und SAN-LIFs von node2 auf node3 verschoben. Gesamteigentum am Ende von Stufe 3: • Node2 ist der Hausbesitzer von node2 Aggregate, aber nicht der aktuelle Eigentümer. • Node3 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehören. • Node2 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die zu node2 gehören, aber nicht der Hausbesitzer.
"Stufe 4: Außer Dienst 2"	Während Phase 4 notieren Sie die nötigen Node2-Informationen, die später im Verfahren verwendet werden sollen, und nehmen dann die Node2-Daten in den Ruhestand. Es findet keine Änderungen am Aggregateigentum statt.

Stufe	Schritte
"Phase 5: Installieren und booten node4"	In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 bis node4 zu und verschieben Daten-LIFs und SAN-LIFs, die zu node2 von node3 nach node4 gehören. Außerdem werden node2-Aggregate von node3 nach node4 verschoben und die Daten-LIFs und SAN-LIFs von node2 auf node3 verschoben. Gesamteigentum am Ende von Stufe 5: • Node3 ist der Hausbesitzer und aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Node4 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Phase 6: Das Upgrade abschließen"	In Phase 6 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden und Storage Encryption oder NetApp Volume Encryption einrichten, wenn die neuen Nodes verschlüsselt sind. Zudem sollten die alten Nodes außer Betrieb gesetzt werden, um den SnapMirror Betrieb fortzusetzen. ⓘ Die Disaster-Recovery-Updates für Storage Virtual Machine (SVM) werden nicht gemäß den zugewiesenen Zeitplänen unterbrochen. Es findet keine Änderungen am Aggregateigentum statt.

Richtlinien für das Controller-Upgrade mit ARL

Um zu verstehen, ob Sie mithilfe von Aggregate Relocation (ARL) ein Upgrade eines Controller-Paars mit ONTAP 9.8 durchführen können, hängt von der Plattform und der Konfiguration des ursprünglichen Controllers sowie des Ersatz-Controllers ab.

Unterstützte Upgrades für ARL

Unter den folgenden Umständen können Sie ein Upgrade eines Node-Paars mit ARL durchführen:

- Auf den ursprünglichen Controllern und den Ersatz-Controllern muss vor dem Upgrade dieselbe Version von ONTAP 9.8 ausgeführt werden.
- Die Ersatz-Controller müssen die gleiche oder eine höhere Kapazität aufweisen als die ursprünglichen Controller. Bei gleicher oder höherer Kapazität werden Attribute bezeichnet, beispielsweise die Maximalanzahl für NVRAM, Volume, LUN oder Aggregate. Er bezieht sich auch auf die maximale Volume- oder Aggregatgröße der neuen Nodes.
- Sie können die folgenden Systemtypen aktualisieren:
  - Einem FAS System auf ein FAS System.
  - Ein FAS System auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System.
  - Einem AFF System auf ein AFF System.

    - Ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System auf einem FAS System, vorausgesetzt, dass das System mit FlexArray Virtualisierungssoftware oder V-Series System keine Array-LUNs besitzt.
    - Eines V-Series Systems auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System
- Bei einigen Upgrades des ARL-Controllers können Sie für das Upgrade temporäre Cluster-Ports auf dem Ersatz-Controller verwenden. Wenn Sie beispielsweise je nach Konfiguration der AFF A400 ein Upgrade von einem AFF A300 auf ein AFF A400 System durchführen, können Sie einen der beiden Mezzanine-Ports verwenden oder eine 10-GbE-Netzwerkschnittstellenkarte mit vier Ports für temporäre Cluster-Ports hinzufügen. Nachdem Sie ein Controller-Upgrade über temporäre Cluster-Ports abgeschlossen haben, können Sie Cluster unterbrechungsfrei zu 100-GbE-Ports auf dem Ersatz-Controller migrieren.
- Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise und SnapLock Compliance Volumes konfiguriert sind.

Sie müssen überprüfen, ob der ARL-Vorgang auf den Original- und Ersatz-Controllern ausgeführt werden kann. Sie müssen die Größe aller definierten Aggregate und die Anzahl der Festplatten überprüfen, die vom ursprünglichen System unterstützt werden. Vergleichen Sie dann die aggregierte Größe und Anzahl der vom neuen System unterstützten Festplatten. Informationen zum Zugriff auf diese Informationen finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*. Die Aggregatgröße und die Anzahl der vom neuen System unterstützten Festplatten müssen gleich oder größer sein als die Aggregatgröße und Anzahl der vom ursprünglichen System unterstützten Festplatten.

Sie müssen in den Cluster-Mischregeln validieren, ob neue Nodes zusammen mit den vorhandenen Nodes Teil des Clusters werden können, wenn der ursprüngliche Controller ersetzt wird. Weitere Informationen zu Regeln für die Kombination von Clustern finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

> Beide Systeme sind entweder hochverfügbarkeits- (HA) oder kein HA-System. Beide Nodes müssen entweder die Persönlichkeit aktiviert oder deaktiviert sein. Sie können einen Node nicht mit der All-Flash-optimierten Persönlichkeit kombinieren, die bei einem Node aktiviert ist, der nicht im gleichen HA-Paar die Persönlichkeit aktiviert hat. Wenn sich die Persönlichkeiten unterscheiden, wenden Sie sich an den technischen Support.

> Wenn das neue System weniger Steckplätze als das ursprüngliche System besitzt oder weniger oder unterschiedliche Ports vorhanden sind, müssen Sie dem neuen System möglicherweise einen Adapter hinzufügen. Siehe "Quellen" Link zum *Hardware Universe* auf der NetApp Support-Website, um Informationen zu bestimmten Plattformen zu erhalten.

Wenn Sie ein System mit mehr als zwei Cluster-Ports pro Node, wie z. B. einem FAS8080 oder AFF8080 System, haben Sie vor dem Upgrade die Cluster-LIFs zu zwei Cluster-Ports pro Node zu migrieren und neu zu starten. Wenn Sie das Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node durchführen, fehlen möglicherweise nach dem Upgrade Cluster-LIFs auf dem neuen Controller.

Upgrades werden für ARL nicht unterstützt

Sie können die folgenden Aktualisierungen nicht ausführen:

- Zu oder von Controllern, die ONTAP 9.8 oder höher nicht ausführen können.
- Zum Austausch von Controllern, die die mit den ursprünglichen Controllern verbundenen Platten-Shelfs nicht unterstützen.

  Informationen zur Unterstützung von Festplatten finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

- Von Controllern mit Root-Aggregaten oder Datenaggregaten auf internen Laufwerken.

  Wenn Sie Controller mit Root-Aggregaten oder Datenaggregaten auf internen Festplattenlaufwerken aktualisieren möchten, lesen Sie "Quellen" Link zu *Upgrade durch Verschiebung von Volumes oder Storage* und Vorgang *Upgrade eines Node-Paares, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.

  Wenn Sie ONTAP auf Nodes in einem Cluster aktualisieren möchten, lesen Sie "Quellen" Link zu *Upgrade ONTAP*.

Annahmen und Terminologie

Dieses Dokument wird an folgende Annahmen geschrieben:

- Die Ersatz-Controller-Hardware ist neu und wurde nicht verwendet.

  Achtung: Da dieses Verfahren davon ausgeht, dass die Hardware des Ersatzcontrollers neu ist und nicht verwendet wurde, werden die erforderlichen Schritte zur Vorbereitung gebrauchter Controller mit dem ausgeführt `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn bereits die Ersatz-Controller-Hardware verwendet wurde, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP in 7-Mode ausgeführt wurde.

- Die Richtlinien zum Upgrade des Knotenpaars werden gelesen und verstanden.

  Achtung: Versuchen Sie nicht, den NVRAM-Inhalt zu löschen. Wenn Sie den Inhalt des NVRAM löschen müssen, wenden Sie sich an den technischen Support von NetApp.

- Sie führen den entsprechenden Befehl vor und nach dem aus `modify` Und die Ausgabe von beiden vergleichen `show` Befehle, um zu überprüfen, dass das `modify` Befehl erfolgreich.
- Wenn Sie über eine SAN-Konfiguration verfügen, stehen Ihnen auf dem HA-Paar lokale LIFs und Partner-LIFs für jede Storage Virtual Machine (SVM) zur Verfügung. Wenn Sie keine lokalen LIFs für jede SVM haben und keine Partner-LIFs haben, sollten Sie vor dem Upgrade die SAN-Daten-LIF auf dem Remote- und lokalen Node für diese SVM hinzufügen.
- Wenn Sie in einer SAN-Konfiguration Port-Sets haben, müssen Sie überprüfen, dass jeder gebundene Port-Satz mindestens eine LIF von jedem Node im HA-Paar enthält.

Bei diesem Verfahren wird der Begriff „*Boot Environment prompt*“ verwendet, um die Eingabeaufforderung auf einem Node, von dem Sie bestimmte Aufgaben ausführen können, zu lesen, z. B. beim Neubooten des Knotens und beim Drucken oder Festlegen von Umgebungsvariablen. Die Eingabeaufforderung wird manchmal informell als *Boot-Loader Prompt* bezeichnet.

Die Eingabeaufforderung der Boot-Umgebung wird im folgenden Beispiel angezeigt:

```
LOADER>
```

Lizenzierung in ONTAP 9.8 oder höher

Einige Funktionen erfordern Lizenzen, die als *Packages* ausgegeben werden, die eine oder mehrere Funktionen enthalten. Jeder Node im Cluster muss über seinen eigenen Schlüssel für jede Funktion im Cluster

verfügen.

Wenn Sie keine neuen Lizenzschlüssel haben, sind für den neuen Controller derzeit lizenzierte Funktionen im Cluster verfügbar und funktionieren weiterhin. Durch die Verwendung nicht lizenzierter Funktionen auf dem Controller können Sie jedoch möglicherweise die Einhaltung Ihrer Lizenzvereinbarung verschließen. Sie müssen daher nach Abschluss des Upgrades den neuen Lizenzschlüssel oder die neuen Schlüssel für den neuen Controller installieren.

Alle Lizenzschlüssel sind 28 Groß-alphabetische Zeichen lang. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken, wo Sie neue 28-stellige Lizenzschlüssel für ONTAP 9.8 erhalten. Oder höher. Die Schlüssel sind im Abschnitt „*My Support*“ unter „*Software licenses*“ verfügbar. Falls auf der Website keine Lizenzschlüssel vorhanden ist, wenden Sie sich an Ihren NetApp Ansprechpartner.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Storage-Verschlüsselung

Die ursprünglichen oder die neuen Nodes sind möglicherweise für die Storage-Verschlüsselung aktiviert. In diesem Fall müssen Sie in diesem Verfahren weitere Schritte durchführen, um zu überprüfen, ob die Speicherverschlüsselung ordnungsgemäß eingerichtet ist.

Falls Sie Storage Encryption verwenden möchten, müssen alle dem Node zugeordneten Festplattenlaufwerke über Self-Encrypting Drives verfügen.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren

Fehlerbehebung

Dieses Verfahren enthält Vorschläge zur Fehlerbehebung.

Falls beim Upgrade der Controller Probleme auftreten, finden Sie weitere Informationen im "Fehlerbehebung" Abschnitt am Ende des Verfahrens für weitere Informationen und mögliche Lösungen.

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Die erforderlichen Tools und Dokumentationen

Sie müssen über spezielle Tools verfügen, um die neue Hardware zu installieren, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren. Sie müssen außerdem die für das Controller-Upgrade wichtigen Informationen aufzeichnen. Zum Aufzeichnen von Informationen wird ein Arbeitsblatt bereitgestellt.

Für die Durchführung des Upgrades benötigen Sie die folgenden Tools:

- Erdungsband
- #2 Kreuzschlitzschraubendreher

Wechseln Sie zum "Quellen" Abschnitt für den Zugriff auf die Liste der für dieses Upgrade erforderlichen Referenzdokumente.

Worksheet: Zu erfassend vor und während des Controller-Upgrades

Sie sollten bestimmte Informationen sammeln, um das Upgrade der ursprünglichen Nodes zu unterstützen. Diese Informationen umfassen Node-IDs, Port- und LIF-Details, Lizenzschlüssel und IP-Adressen.

Sie können das folgende Arbeitsblatt verwenden, um die Informationen für eine spätere Verwendung im Verfahren aufzuzeichnen:

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
Modell, System-ID, Seriennummer der ursprünglichen Nodes	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Phase 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4* Stufe 6: *Decommission das alte System*	
Shelf- und Festplatteninformationen, Flash Storage-Details, Arbeitsspeicher, NVRAM und Adapterkarten auf den ursprünglichen Nodes	Phase 1: *Vorbereiten der Knoten für das Upgrade*	Während des gesamten Verfahrens	
Online-Aggregate und Volumes auf den ursprünglichen Nodes	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Während des gesamten Verfahrens zur Überprüfung, ob Aggregate und Volumes online bleiben, außer bei kurzen Standortverlagerungen	
Ausgabe von Befehlen `network port vlan show` Und `network port ifgrp show`	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 3: *Map Ports von node1 nach node3* Stufe 5: *Map Ports von node2 nach node4*	
(Nur SAN-Umgebungen) Standardkonfiguration von FC-Ports	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Beim Konfigurieren von FC-Ports auf den neuen Nodes	
(Systeme der V-Series oder Systeme mit FlexArray-Virtualisierungssoftware) Topologie für V-Series Systeme oder Systeme mit FlexArray Virtualisierungssoftware	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4*	
IP-Adresse der SPs	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 6: *Bestätigen Sie, dass die neuen Controller korrekt eingerichtet sind*	

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
Lizenzschlüssel	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 6: *Bestätigen Sie, dass die neuen Controller korrekt eingerichtet sind*	
IP-Adresse für den externen Schlüsselverwaltungsserver	Phase 1: *Rekey Disks für Speicherverschlüsselung*	Phase 6: *Storage Encryption auf den neuen Nodes einrichten*	
Name und Pfad des per Web zugänglichen Verzeichnisses, bei dem Sie Dateien auf die Nodes als Netzboot herunterladen	Stufe 1: *Netzboot vorbereiten*	Stufe 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4*	
LIFs für nicht-SAN-Daten im Besitz von Node1	Phase 2: *Verschieben Sie nicht-SAN-logische Datenschnittstellen von node1 auf node2*	Später im Abschnitt	
Cluster, Intercluster, Node-Management, Cluster-Management und physische Ports	Phase 2: *Node1-Informationen aufzeichnen*	Stufe 3: *Installieren und Booten node3* Stufe 3: *Kartenanschlüsse von node1 nach node3*	
Ports auf neuen Nodes	Phase 3: *Map Ports von node1 nach node3*	Später im Abschnitt und im Abschnitt *Kartenanschlüsse von node2 nach node4*	
Verfügbare Ports und Broadcast-Domänen auf Knoten 3	Phase 3: *Map Ports von node1 nach node3*	Später im Abschnitt	
Logische Schnittstellen (Non-SAN) sind nicht im Besitz von node2	*Verschieben von LIFs für nicht-SAN-Daten, die zu node1 von node2 zu node3 gehören und SAN-LIFs auf node3* überprüfen	Später im Abschnitt	
LIFs für nicht-SAN-Daten im Besitz von node2	Phase 3: *Verschieben Sie nicht-SAN-logische Datenschnittstellen von node2 auf node3*	Später im Abschnitt	
Cluster, Intercluster, Node-Management, Cluster-Management und physische Ports	Stufe 4: *Node2-Informationen aufzeichnen*	Stufe 5: *Installation und Booten von node4* Stufe 5:_ Kartenanschlüsse von node2 nach node4_	
Cluster-Netzwerk-Ports auf node4	Stufe 5: *Map Ports von node2 nach node4*	Später im Abschnitt	

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
Verfügbare Ports und Broadcast-Domänen auf node4	Stufe 5: *Map Ports von node2 nach node4*	Später im Abschnitt	
Private und öffentliche SSL-Zertifikate für das Storage-System und private SSL-Zertifikate für jeden Schlüsselmanagementserver	Phase 6: *Storage Encryption auf den neuen Nodes einrichten*	Später im Abschnitt	

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 bestätigen Sie, dass interne Festplatten keine Root-Aggregate oder Datenaggregate enthalten, die Nodes für das Upgrade vorbereiten und mehrere Vorabprüfungen durchführen. Unter Umständen müssen Sie auch Festplatten für die Storage-Verschlüsselung rekeysen und die neuen Controller als Netzboot vorbereiten.

Schritte

1. "Ermitteln Sie, ob der Controller über Aggregate auf internen Festplatten verfügt"
2. "Bereiten Sie die Knoten für ein Upgrade vor"
3. "Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager"
4. "SnapMirror Beziehungen stilllegen"
5. "Vorbereitungen für den Netzboot"

Ermitteln Sie, ob der Controller über Aggregate auf internen Festplatten verfügt

Wenn Sie Controller mit internen Festplatten aktualisieren, müssen Sie mehrere Befehle ausführen und deren Ausgabe überprüfen, um zu bestätigen, dass keines der internen Festplatten Root-Aggregate oder Datenaggregate enthält.

Über diese Aufgabe

Wenn Sie Controller nicht mit Aggregaten auf internen Festplatten aktualisieren, lassen Sie diesen Abschnitt überspringen und fahren Sie mit dem Abschnitt fort "Bereiten Sie die Knoten für ein Upgrade vor".

Schritte

1. Geben Sie die nodeshell, einmal für jeden der ursprünglichen Knoten.

   ```
   system node run -node node_name
   ```

2. Anzeigen der internen Laufwerke:

   ```
   sysconfig -av
   ```

Das System zeigt ausführliche Informationen über die Konfiguration des Node, einschließlich Storage, an. Diese Informationen werden in der im folgenden Beispiel gezeigten Teilausgabe angezeigt:

```
node> sysconfig -av
slot 0: SAS Host Adapter 0a (PMC-Sierra PM8001 rev. C, SAS, UP)
                Firmware rev: 01.11.06.00
                 Base WWN: 5:00a098:0008a3b:b0
                 Phy State: [0] Enabled, 6.0 Gb/s
                            [1] Enabled, 6.0 Gb/s
                            [2] Enabled, 6.0 Gb/s
                            [3] Enabled, 6.0 Gb/s
                ID Vendor Model FW Size
                00.0 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.1 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.2 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.3 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.4 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.5 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.6 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.7 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.8 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.9 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.10: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.11: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
...
```

3. Untersuchen Sie die Speicherausgabe des `sysconfig -av` Befehl, um die internen Festplattenlaufwerke zu identifizieren, und notieren Sie dann die Informationen.

   Interne Laufwerke haben "00." zu Beginn ihrer ID. „00.“ gibt ein internes Festplatten-Shelf an, und die Zahl nach dem Dezimalpunkt gibt das einzelne Festplattenlaufwerk an.

4. Geben Sie auf beiden Controllern den folgenden Befehl ein:

   `aggr status -r`

Das System zeigt den Aggregatstatus des Node an, wie in der Teilausgabe im folgenden Beispiel dargestellt:

```
node> aggr status -r
Aggregate aggr2 (online, raid_dp, parity uninit'd!) (block checksums)
Plex /aggr2/plex0 (online, normal, active)
RAID group /aggr2/plex0/rg0 (normal, block checksums)

RAID Disk Device    HA SHELF BAY CHAN Pool Type RPM  Used (MB/blks)
Phys (MB/blks)
--------- --------- -- ----- --- ---- ---- ---- ---- ------------------
------------------
dparity   0a.00.1   0a   0    1  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
parity    0a.00.3   0a   0    3  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
data      0a.00.9   0a   0    9  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
...
```

Das Gerät, das zum Erstellen des Aggregats verwendet wird, ist möglicherweise keine physische Festplatte, sondern möglicherweise eine Partition.

5. Überprüfen Sie die Ausgabe des `aggr status -r` Befehl, um die Aggregate mithilfe interner Festplatten zu identifizieren und dann die Informationen aufzuzeichnen.

   Im Beispiel im vorherigen Schritt verwendet „aggr2“ interne Laufwerke, wie durch die Shelf-ID von „0“ angegeben.

6. Geben Sie bei beiden Controllern den folgenden Befehl ein:

   ```
   aggr status -y
   ```

   Das System zeigt Informationen zu den Volumes auf dem Aggregat an, wie in der teilweise Ausgabe im folgenden Beispiel dargestellt:

```
node> aggr status -v
...
 aggr2   online   raid_dp, aggr    nosnap=off, raidtype=raid_dp,
raidsize=14,
                  64-bit           raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off, resyncsnaptime=60,
                                   fs_size_fixed=off,
lost_write_protect=on,
                                   ha_policy=cfo, hybrid_enabled=off,
percent_snapshot_space=0%,
                                   free_space_realloc=off, raid_cv=on,
thorough_scrub=off
         Volumes: vol6, vol5, vol14
...
 aggr0   online   raid_dp, aggr    root, diskroot, nosnap=off,
raidtype=raid_dp,
                  64-bit           raidsize=14, raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off,  resyncsnaptime=60,
fs_size_fixed=off,
                                   lost_write_protect=on, ha_policy=cfo,
hybrid_enabled=off,
                                   percent_snapshot_space=0%,
free_space_realloc=off, raid_cv=on
         Volumes: vol0
```

Basierend auf der Ausgabe in Schritt 4 Schritt 6 verwendet aggr2 drei interne Laufwerke – „0a.00.1“, „0a.00.3“ und „0a.00.9“ – und die Volumes auf „aggr2“ sind „vol6“, „vol5“ und „vol14“. Auch in der Ausgabe von Schritt 6 enthält die Auslesung für „aggr0“ das Wort „root“ am Anfang der Information für das Aggregat. Das bedeutet, dass es ein Root-Volume enthält.

7. Überprüfen Sie die Ausgabe des `aggr status -v` Befehl zur Ermittlung der Volumes, die zu beliebigen Aggregaten gehören, die sich auf einem internen Laufwerk befinden und ob eines dieser Volumes ein Root-Volume enthalten soll
8. Beenden Sie den nodeshell, indem Sie auf jedem Controller den folgenden Befehl eingeben:

   `exit`

9. Führen Sie eine der folgenden Aktionen durch:

Wenn die Controller	Dann…
Enthalten keine Aggregate auf internen Festplatten	Fahren Sie mit diesem Verfahren fort.

Wenn die Controller	Dann…
Enthalten Aggregate, aber keine Volumes auf den internen Festplattenlaufwerken	Fahren Sie mit diesem Verfahren fort. Bevor Sie fortfahren, müssen Sie die Aggregate offline setzen und dann die Aggregate auf den internen Festplattenlaufwerken zerstören. Siehe "Quellen" Verbinden mit *Disk und Aggregatmanagement mit CLI* Inhalt für Informationen über das Managen von Aggregaten.
Enthalten nicht-Root-Volumes auf den internen Laufwerken	Fahren Sie mit diesem Verfahren fort. Bevor Sie fortfahren, müssen Sie die Volumes zu einem externen Festplatten-Shelf verschieben, die Aggregate offline platzieren und dann die Aggregate auf den internen Festplattenlaufwerken zerstören. Siehe "Quellen" Informationen über das Verschieben von Volumes erhalten Sie unter Verweis auf das Management von *Festplatte und Aggregaten mit dem CLI* Inhalt.
Enthalten Root-Volumes auf den internen Laufwerken	Fahren Sie mit diesem Verfahren nicht fort. Sie können ein Upgrade der Controller durchführen, indem Sie auf verweisen "Quellen" Zum Verlinken auf die *NetApp Support Site* und das Verfahren *Aktualisieren der Controller Hardware auf einem Node-Paar, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.
Enthalten nicht-Root-Volumes auf den internen Laufwerken und Sie können die Volumes nicht in einen externen Speicher verschieben	Fahren Sie mit diesem Verfahren nicht fort. Sie können die Controller mithilfe des Verfahrens *aktualisieren Sie die Controller-Hardware auf einem Node-Paar, auf dem Clustered Data ONTAP ausgeführt wird, indem Sie Volumes* verschieben. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken, auf die Sie Zugriff haben.

Bereiten Sie die Knoten für ein Upgrade vor

Bevor Sie die ursprünglichen Nodes ersetzen können, müssen Sie bestätigen, dass sich die Nodes in einem HA-Paar befinden, dass keine fehlenden oder ausgefallenen Festplatten vorhanden sind, auf den Storage der jeweils anderen Nodes zugreifen können und keine Daten-LIFs besitzen, die den anderen Nodes im Cluster zugewiesen sind. Sie müssen auch Informationen über die ursprünglichen Nodes sammeln und bestätigen, dass alle Knoten im Cluster Quorum sind, wenn sich der Cluster in einer SAN-Umgebung befindet.

Schritte

1. Vergewissern Sie sich, dass jeder der ursprünglichen Nodes über ausreichende Ressourcen verfügt, um den Workload beider Nodes im Übernahmemodus angemessen zu unterstützen.

Siehe "Quellen" Um zu *High Availability Management* zu verlinken und im Abschnitt „ Best Practices für HA-Paare_“ zu folgen. Keine der ursprünglichen Nodes sollte mit einer Auslastung von über 50 % laufen. Wenn ein Node eine Auslastung von unter 50 % aufweist, kann er die Lasten für beide Nodes während des Controller-Upgrades verarbeiten.

2. Führen Sie die folgenden Teilschritte durch, um eine Performance-Baseline für die ursprünglichen Nodes zu erstellen:
   a. Stellen Sie sicher, dass das Benutzerkonto für den Diagnosebenutzer entsperrt ist.

      Das diagnostische Benutzerkonto ist nur für diagnostische Zwecke auf niedriger Ebene gedacht und sollte nur unter Anleitung durch den technischen Support verwendet werden.

      Informationen zum Entsperren der Benutzerkonten finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

   b. Siehe "Quellen" Wenn Sie einen Link zur NetApp Support-Website_ erhalten möchten, können Sie den Performance and Statistics Collector (Perfstat Converged) herunterladen.

      Mit dem konvergenten Perfstat Tool können Sie eine Performance-Baseline für den Vergleich nach dem Upgrade erstellen.

   c. Erstellen Sie eine Performance-Baseline gemäß den Anweisungen auf der NetApp Support Site.
3. Siehe "Quellen" Einen Link zur NetApp Support Site_ öffnen und einen Support-Case auf der NetApp Support Site eröffnen.

   Sie können den Fall verwenden, um eventuelle Probleme während des Upgrades zu melden.

4. Überprüfen Sie, ob NVMEM oder NVRAM-Batterien der Node3 und node4 geladen sind, und laden Sie sie, falls nicht, auf.

   Sie müssen Node 3 und node4 physisch überprüfen, um zu ermitteln, ob die NVMEM- oder NVRAM-Batterien geladen sind. Informationen zu den LEDs für das Modell node3 und node4 finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

   Achtung Versuchen Sie nicht, den NVRAM-Inhalt zu löschen. Wenn der Inhalt des NVRAM gelöscht werden muss, wenden Sie sich an den technischen Support von NetApp.

5. Überprüfen Sie die Version von ONTAP auf node3 und node4.

   Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version der ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation neu laden. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.

   Informationen über die Version von ONTAP auf node3 und node4 sollten in den Versandkartons enthalten sein. Die ONTAP-Version wird angezeigt, wenn der Node hochgefahren wird oder Sie können den Node im Wartungsmodus booten und den Befehl ausführen:

   ```
   version
   ```

6. Überprüfen Sie, ob Sie zwei oder vier Cluster LIFs auf node1 und node2 haben:

```
network interface show -role cluster
```

Das System zeigt alle Cluster-LIFs an, wie im folgenden Beispiel gezeigt:

```
cluster::> network interface show -role cluster
        Logical    Status     Network          Current  Current Is
Vserver Interface  Admin/Oper Address/Mask     Node     Port    Home
------- ---------- ---------- ---------------- -------- ------- ----
node1
        clus1      up/up      172.17.177.2/24  node1    e0c     true
        clus2      up/up      172.17.177.6/24  node1    e0e     true
node2
        clus1      up/up      172.17.177.3/24  node2    e0c     true
        clus2      up/up      172.17.177.7/24  node2    e0e     true
```

7. Wenn Sie zwei oder vier Cluster LIFs auf node1 oder node2 haben, stellen Sie sicher, dass Sie beide Cluster LIFs über alle verfügbaren Pfade pingen können, indem Sie die folgenden Unterschritte ausführen:

   a. Geben Sie die erweiterte Berechtigungsebene ein:

      ```
      set -privilege advanced
      ```

      Vom System wird die folgende Meldung angezeigt:

      ```
      Warning: These advanced commands are potentially dangerous; use them
      only when directed to do so by NetApp personnel.
      Do you wish to continue? (y or n):
      ```

   b. Eingabe `y`.

   c. Pingen der Knoten und Testen der Konnektivität:

      ```
      cluster ping-cluster -node node_name
      ```

      Vom System wird eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::*> cluster ping-cluster -node node1
Host is node1
Getting addresses from network interface table...
Local = 10.254.231.102 10.254.91.42
Remote = 10.254.42.25 10.254.16.228
Ping status:
...
Basic connectivity succeeds on 4 path(s) Basic connectivity fails on 0
path(s)
................
Detected 1500 byte MTU on 4 path(s):
Local 10.254.231.102 to Remote 10.254.16.228
Local 10.254.231.102 to Remote 10.254.42.25
Local 10.254.91.42 to Remote 10.254.16.228
Local 10.254.91.42 to Remote 10.254.42.25
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

+
Wenn der Node zwei Cluster Ports verwendet, sollten Sie sehen, dass er in vier Pfaden kommunizieren kann, wie im Beispiel dargestellt.

a. Zurück zur Berechtigung auf Administratorebene:

   ```
   set -privilege admin
   ```

8. Vergewissern Sie sich, dass sich node1 und node2 in einem HA-Paar befinden und überprüfen Sie, dass die Knoten miteinander verbunden sind und dass Übernahme möglich ist:

   ```
   storage failover show
   ```

   Das folgende Beispiel zeigt die Ausgabe, wenn die Nodes miteinander verbunden sind und Takeover möglich ist:

   ```
   cluster::> storage failover show
                                Takeover
   Node           Partner        Possible State Description
   -------------- -------------- -------- -------------------------------
   node1          node2          true     Connected to node2
   node2          node1          true     Connected to node1
   ```

   Beide Nodes sollten sich im partiellen Giveback enthalten. Das folgende Beispiel zeigt, dass sich node1 teilweise im Giveback befindet:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -------------------------------
node1          node2          true     Connected to node2, Partial
giveback
node2          node1          true     Connected to node1
```

Wenn einer der beiden Nodes sich als Teil des Giveback befindet, verwenden Sie den `storage failover giveback` Führen Sie den Befehl zum Giveback durch, und verwenden Sie dann den `storage failover show-giveback` Befehl um sicherzustellen, dass noch keine Aggregate zurückgegeben werden müssen. Ausführliche Informationen zu den Befehlen finden Sie unter "Quellen" Link zu *High Availability Management*.

9. Bestätigen Sie, dass weder node1 noch node2 die Aggregate besitzen, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   Wenn weder node1 noch node2 besitzt Aggregate, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer), gibt das System eine Meldung ähnlich dem folgenden Beispiel zurück:

```
cluster::> storage aggregate show -node node2 -is-home false -fields
owner-name,homename,state
There are no entries matching your query.
```

   Im folgenden Beispiel wird die Ausgabe des Befehls für einen Node mit dem Namen node2 angezeigt, der der Home-Inhaber, jedoch nicht der aktuelle Eigentümer von vier Aggregaten ist:

```
cluster::> storage aggregate show -node node2 -is-home false
              -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node2        online
aggr2         node1        node2        online
aggr3         node1        node2        online
aggr4         node1        node2        online

4 entries were displayed.
```

10. Führen Sie eine der folgenden Aktionen durch:

Wenn der Befehl in ausgeführt wird Schritt 9…	Dann…
Leere Ausgabe	Überspringen Sie Schritt 11, und fahren Sie mit fort Schritt 12.
Hatte eine Ausgabe	Gehen Sie zu Schritt 11.

11. [[man_prepare_Nodes_step11] Wenn node1 oder node2 Aggregate besitzt, für die es der aktuelle Eigentümer, aber nicht der Besitzer des Hauses ist, führen Sie die folgenden Teilschritte durch:

    a. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

    ```
    storage failover giveback -ofnode home_node_name
    ```

    b. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

    ```
    storage aggregate show -nodes node_name -is-home false -fields owner-name,
    home-name, state
    ```

    Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1
          -is-home true -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node1        online
aggr2         node1        node1        online
aggr3         node1        node1        online
aggr4         node1        node1        online

4 entries were displayed.
```

12. Bestätigen, dass node1 und node2 auf den Speicher des anderen zugreifen können und überprüfen, dass keine Festplatten fehlen:

    ```
    storage failover show -fields local-missing-disks,partner-missing-disks
    ```

    Im folgenden Beispiel wird die Ausgabe angezeigt, wenn keine Festplatten fehlen:

```
cluster::> storage failover show -fields local-missing-disks,partner-
missing-disks

node     local-missing-disks partner-missing-disks
-------- ------------------- ---------------------
node1    None                None
node2    None                None
```

Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.

13. Vergewissern Sie sich, dass node1 und node2 gesund sind und am Cluster teilnehmen können:

    `cluster show`

    Das folgende Beispiel zeigt die Ausgabe, wenn beide Nodes qualifiziert und ordnungsgemäß sind:

```
cluster::> cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
```

14. Legen Sie die Berechtigungsebene auf erweitert fest:

    `set -privilege advanced`

15. Bestätigen Sie, dass node1 und node2 dieselbe ONTAP-Version ausführen:

    `system node image show -node node1,node2 -iscurrent true`

    Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt:

```
cluster::*> system node image show -node node1,node2 -iscurrent true

                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node1
         image1   true    true    9.1         2/7/2017 20:22:06
node2
         image1   true    true    9.1         2/7/2017 20:20:48

2 entries were displayed.
```

16. Vergewissern Sie sich, dass weder node1 noch node2 Eigentümer sämtlicher Daten-LIFs sind, die zu anderen Nodes im Cluster gehören, und überprüfen Sie die `Current Node` Und `Is Home` Spalten in der Ausgabe:

    `network interface show -role data -is-home false -curr-node` *`node_name`*

    Das folgende Beispiel zeigt die Ausgabe, wenn node1 keine LIFs besitzt, die im Besitz anderer Nodes im Cluster sind:

    ```
    cluster::> network interface show -role data -is-home false -curr-node
    node1
     There are no entries matching your query.
    ```

    Das folgende Beispiel zeigt die Ausgabe, wenn Node1 dem anderen Node gehören wird, der Eigentümer von Daten-LIFs:

    ```
    cluster::> network interface show -role data -is-home false -curr-node
    node1

                Logical    Status     Network            Current
    Current Is
    Vserver     Interface  Admin/Oper Address/Mask       Node          Port
    Home
    ----------- ---------- ---------- ------------------ -------------
    ------- ----
    vs0
                data1      up/up      172.18.103.137/24  node1         e0d
    false
                data2      up/up      172.18.103.143/24  node1         e0f
    false

    2 entries were displayed.
    ```

17. Wenn die Ausgabe in Schritt 15 Zeigt, dass Node1 oder node2 Eigentümer beliebiger Daten-LIFs sind, die sich im Besitz anderer Nodes im Cluster befinden. Migrieren Sie die Daten-LIFs von node1 oder node2:

    ```
    network interface revert -vserver * -lif *
    ```

    Ausführliche Informationen zum `network interface revert` Befehl, siehe "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

18. Überprüfen Sie, ob node1 oder node2 ausgefallene Festplatten besitzt:

    ```
    storage disk show -nodelist node1,node2 -broken
    ```

    Wenn eine der Festplatten ausgefallen ist, entfernen Sie sie gemäß den Anweisungen in *Disk und Aggregat-Management mit der CLI*. (Siehe "Quellen" Verbinden mit *Disk und Aggregatmanagement mit CLI*.)

19. Sammeln Sie Informationen über node1 und node2, indem Sie die folgenden Unterschritte ausführen und die Ausgabe jedes Befehls aufzeichnen:

    - Diese Informationen werden Sie später im Verfahren verwenden.
    - Wenn Sie ein System mit mehr als zwei Cluster-Ports pro Node, wie z. B. einem FAS8080 oder AFF8080 System, haben Sie vor dem Upgrade die Cluster-LIFs zu zwei Cluster-Ports pro Node zu migrieren und neu zu starten. Wenn Sie das Controller-Upgrade mit mehr als zwei Cluster-Ports pro Node durchführen, fehlen möglicherweise nach dem Upgrade Cluster-LIFs auf dem neuen Controller.

    a. Notieren Sie das Modell, die System-ID und die Seriennummer beider Nodes:

    ```
    system node show -node node1,node2 -instance
    ```

    Sie verwenden die Informationen, um Festplatten neu zuzuweisen und die ursprünglichen Nodes außer Betrieb zu nehmen.

    b. Geben Sie in node1 und node2 den folgenden Befehl ein und notieren Sie Informationen über die Shelfs, die Anzahl der Festplatten in jedem Shelf, die Flash Storage-Details, den Arbeitsspeicher, NVRAM und die Netzwerkkarten aus der Ausgabe:

    ```
    run -node node_name sysconfig
    ```

    Sie können die Informationen verwenden, um Teile oder Zubehör zu identifizieren, die Sie auf node3 oder node4 übertragen möchten. Wenn Sie nicht wissen, ob die Nodes V-Series Systeme sind oder über FlexArray-Virtualisierungssoftware verfügen, können Sie das auch aus der Ausgabe lernen.

    c. Geben Sie sowohl bei node1 als auch bei node2 den folgenden Befehl ein und notieren Sie die Aggregate, die auf beiden Nodes online sind:

    ```
    storage aggregate show -node node_name -state online
    ```

Mithilfe dieser Informationen und der Informationen im folgenden Unterschritt können Sie überprüfen, ob die Aggregate und Volumes während des gesamten Verfahrens online bleiben, mit Ausnahme des kurzen Zeitraums, in dem sie während der Verschiebung offline sind.

d. Geben Sie sowohl für node1 als auch für node2 den folgenden Befehl ein und notieren Sie die Volumes, die auf beiden Knoten offline sind:

```
volume show -node node_name -state offline
```

Nach dem Upgrade führen Sie den Befehl erneut aus und vergleichen die Ausgabe mit der Ausgabe in diesem Schritt, um zu sehen, ob andere Volumes offline gegangen sind.

20. Geben Sie die folgenden Befehle ein, um zu ermitteln, ob Schnittstellengruppen oder VLANs auf node1 oder node2 konfiguriert sind:

```
network port ifgrp show

network port vlan show
```

Beachten Sie, ob Schnittstellengruppen oder VLANs auf node1 oder node2 konfiguriert sind. Diese Informationen benötigen Sie im nächsten Schritt und später im Verfahren.

21. Führen Sie die folgenden Teilschritte sowohl bei node1 als auch bei node2 durch, um zu bestätigen, dass die physischen Ports im weiteren Verlauf des Verfahrens korrekt zugeordnet werden können:

a. Geben Sie den folgenden Befehl ein, um zu ermitteln, ob außer den Failover-Gruppen auf dem Node Failover-Gruppen vorhanden sind `clusterwide`:

```
network interface failover-groups show
```

Failover-Gruppen sind Gruppen von Netzwerk-Ports, die sich im System befinden. Da durch ein Upgrade der Controller-Hardware der Standort physischer Ports geändert werden kann, können Failover-Gruppen während des Upgrades unbeabsichtigt geändert werden.

Das System zeigt Failover-Gruppen auf dem Node an, wie im folgenden Beispiel dargestellt:

```
cluster::> network interface failover-groups show

Vserver              Group              Targets
-------------------- ------------------ ----------
Cluster              Cluster            node1:e0a, node1:e0b
                                        node2:e0a, node2:e0b

fg_6210_e0c          Default            node1:e0c, node1:e0d
                                        node1:e0e, node2:e0c
                                        node2:e0d, node2:e0e

2 entries were displayed.
```

b. Wenn es andere Failover-Gruppen als gibt `clusterwide`Notieren Sie die Namen der Failover-Gruppen und die Ports, die zu den Failover-Gruppen gehören.

c. Geben Sie den folgenden Befehl ein, um zu ermitteln, ob auf dem Node konfigurierte VLANs vorhanden sind:

   `network port vlan show -node node_name`

   VLANs werden über physische Ports konfiguriert. Wenn sich die physischen Ports ändern, müssen die VLANs später im Verfahren neu erstellt werden.

   Das System zeigt VLANs an, die auf dem Knoten konfiguriert sind, wie im folgenden Beispiel dargestellt:

```
cluster::> network port vlan show

Network Network
Node    VLAN Name Port    VLAN ID MAC Address
------  --------- ------- ------- ------------------
node1   e1b-70    e1b     70      00:15:17:76:7b:69
```

a. Wenn auf dem Node VLANs konfiguriert sind, notieren Sie sich jeden Netzwerkport und die Verbindung zwischen VLAN-ID.

22. Führen Sie eine der folgenden Aktionen durch:

Wenn Interface Groups oder VLANS…	Dann…
Auf node1 oder node2	Vollständig Schritt 23 Und Schritt 24.
Nicht auf node1 oder node2	Gehen Sie zu Schritt 24.

23. [[man_prepare_Nodes_step23] Wenn Sie nicht wissen, ob sich node1 und node2 in einer SAN- oder nicht-SAN-Umgebung befinden, geben Sie den folgenden Befehl ein und überprüfen die Ausgabe:

    `network interface show -vserver vserver_name -data-protocol iscsi|fcp`

    Wenn iSCSI oder FC für die SVM konfiguriert ist, wird mit dem Befehl eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::> network interface show -vserver Vserver8970 -data-protocol
iscsi|fcp
There are no entries matching your query.
```

    Sie können bestätigen, dass sich der Knoten in einer NAS-Umgebung befindet, indem Sie den verwenden `network interface show` Befehl mit dem `-data-protocol nfs|cifs` Parameter.

    Wenn iSCSI oder FC für die SVM konfiguriert ist, wird mit dem Befehl eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::> network interface show -vserver vs1 -data-protocol iscsi|fcp

         Logical    Status     Network            Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask       Node     Port    Home
-------- ---------- ---------- ------------------ -------- ------- ----
vs1      vs1_lif1   up/down    172.17.176.20/24   node1    0d      true
```

24. Stellen Sie sicher, dass alle Knoten im Cluster Quorum sind, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie die erweiterte Berechtigungsebene ein:

       `set -privilege advanced`

       Vom System wird die folgende Meldung angezeigt:

       ```
       Warning: These advanced commands are potentially dangerous; use them
       only when directed to do so by NetApp personnel.
       Do you wish to continue? (y or n):
       ```

    b. Eingabe `y`.

    c. Überprüfen Sie einmal für jeden Node den Cluster-Service-Status im Kernel:

       `cluster kernel-service show`

       Vom System wird eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::*> cluster kernel-service show

Master        Cluster       Quorum        Availability  Operational
Node          Node          Status        Status        Status
------------- ------------- ------------- ------------- -------------
node1         node1         in-quorum     true          operational
              node2         in-quorum     true          operational

2 entries were displayed.
```

+
Nodes in einem Cluster sind Quorum, wenn eine einfache Mehrheit der Nodes in einem ordnungsgemäßen Zustand ist und miteinander kommunizieren kann. Weitere Informationen finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

    a. Zurück zur Administratorberechtigungsebene:

       `set -privilege admin`

25. Führen Sie eine der folgenden Aktionen durch:

Wenn der Cluster…	Dann…
Ist SAN konfiguriert	Gehen Sie zu Schritt 26.
Hat kein SAN konfiguriert	Gehen Sie zu Schritt 29.

26. Stellen Sie sicher, dass SAN LIFs auf node1 und node2 für jede SVM sind, bei der entweder SAN iSCSI oder FC Service aktiviert ist, indem Sie den folgenden Befehl eingeben und seine Ausgabe prüfen:

`network interface show -data-protocol iscsi|fcp -home-node node_name`

Der Befehl zeigt SAN LIF-Informationen für node1 und node2 an. Die folgenden Beispiele zeigen den Status in der Spalte Status Admin/Oper nach oben/oben und geben an, dass SAN-iSCSI- und FC-Service aktiviert sind:

```
cluster::> network interface show -data-protocol iscsi|fcp
            Logical    Status     Network                  Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask             Node
Port    Home
----------- ---------- ---------- ------------------       ---------
------- ----
a_vs_iscsi  data1      up/up      10.228.32.190/21         node1     e0a
true
            data2      up/up      10.228.32.192/21         node2     e0a
true

b_vs_fcp    data1      up/up      20:09:00:a0:98:19:9f:b0  node1     0c
true
            data2      up/up      20:0a:00:a0:98:19:9f:b0  node2     0c
true

c_vs_iscsi_fcp data1   up/up      20:0d:00:a0:98:19:9f:b0  node2     0c
true
            data2      up/up      20:0e:00:a0:98:19:9f:b0  node2     0c
true
            data3      up/up      10.228.34.190/21         node2     e0b
true
            data4      up/up      10.228.34.192/21         node2     e0b
true
```

Alternativ können Sie ausführlichere LIF-Informationen anzeigen, indem Sie den folgenden Befehl eingeben:

`network interface show -instance -data-protocol iscsi|fcp`

27. Erfassen Sie die Standardkonfiguration aller FC-Ports an den ursprünglichen Nodes, indem Sie den folgenden Befehl eingeben und die Ausgabe für Ihre Systeme aufzeichnen:

    ```
    ucadmin show
    ```

    Der Befehl zeigt Informationen zu allen FC-Ports im Cluster an, wie im folgenden Beispiel dargestellt:

    ```
    cluster::> ucadmin show

                   Current Current   Pending Pending   Admin
    Node    Adapter Mode    Type      Mode    Type      Status
    ------- ------- ------- --------- ------- --------- -----------
    node1   0a      fc      initiator -       -         online
    node1   0b      fc      initiator -       -         online
    node1   0c      fc      initiator -       -         online
    node1   0d      fc      initiator -       -         online
    node2   0a      fc      initiator -       -         online
    node2   0b      fc      initiator -       -         online
    node2   0c      fc      initiator -       -         online
    node2   0d      fc      initiator -       -         online
    8 entries were displayed.
    ```

    Sie können die Informationen nach dem Upgrade verwenden, um die Konfiguration von FC-Ports auf den neuen Nodes einzustellen.

28. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware aktualisieren, erfassen Sie Informationen über die Topologie der Original-Nodes, indem Sie den folgenden Befehl eingeben und die Ausgabe aufzeichnen:

    ```
    storage array config show -switch
    ```

    Das System zeigt Topologieinformationen wie im folgenden Beispiel dargestellt an:

```
cluster::> storage array config show -switch

      LUN LUN                                    Target Side Initiator
Side Initi-
Node  Grp Cnt Array Name    Array Target Port  Switch Port Switch Port
ator
----- --- --- ------------- ------------------ -----------
-------------- ------
node1 0   50  I_1818FAStT_1
                            205700a0b84772da   vgbr6510a:5
vgbr6510s164:3  0d
                            206700a0b84772da   vgbr6510a:6
vgbr6510s164:4  2b
                            207600a0b84772da   vgbr6510b:6
vgbr6510s163:1  0c
node2 0   50  I_1818FAStT_1
                            205700a0b84772da   vgbr6510a:5
vgbr6510s164:1  0d
                            206700a0b84772da   vgbr6510a:6
vgbr6510s164:2  2b
                            207600a0b84772da   vgbr6510b:6
vgbr6510s163:3  0c
                            208600a0b84772da   vgbr6510b:5
vgbr6510s163:4  2a
7 entries were displayed.
```

29. die folgenden Teilschritte ausführen:

    a. Geben Sie an einem der Original-Nodes den folgenden Befehl ein und notieren Sie die Ausgabe:

       `service-processor show -node * -instance`

    Das System zeigt auf beiden Nodes detaillierte Informationen zum SP an.

    a. Vergewissern Sie sich, dass der SP-Status lautet `online`.
    b. Vergewissern Sie sich, dass das SP-Netzwerk konfiguriert ist.
    c. Notieren Sie die IP-Adresse und andere Informationen zum SP.

       Möglicherweise möchten Sie die Netzwerkparameter der Remote-Verwaltungsgeräte, in diesem Fall die SPs, vom ursprünglichen System für die SPs auf den neuen Knoten wieder verwenden. Ausführliche Informationen zum SP finden Sie unter "Quellen" Link zu den Befehlen *Systemadministration Reference* und *ONTAP 9: Manual Page Reference*.

30. Wenn die neuen Nodes dieselben lizenzierten Funktionen wie die ursprünglichen Knoten haben sollen, geben Sie den folgenden Befehl ein, um die Clusterlizenzen auf dem ursprünglichen System anzuzeigen:

    `system license show -owner *`

Das folgende Beispiel zeigt die Websitelizenzen für Cluster1:

```
system license show -owner *
Serial Number: 1-80-000013
Owner: cluster1

Package           Type    Description           Expiration
----------------- ------- --------------------- -----------
Base              site    Cluster Base License  -
NFS               site    NFS License           -
CIFS              site    CIFS License          -
SnapMirror        site    SnapMirror License    -
FlexClone         site    FlexClone License     -
SnapVault         site    SnapVault License     -
6 entries were displayed.
```

31. Beschaffung neuer Lizenzschlüssel für die neuen Nodes auf der *NetApp Support Site*. Siehe "Quellen" Zum Link zu *NetApp Support Site*.

    Falls auf der Website keine Lizenzschlüssel vorhanden ist, wenden Sie sich an Ihren NetApp Ansprechpartner.

32. Überprüfen Sie, ob im Original-System AutoSupport aktiviert ist, indem Sie auf jedem Node den folgenden Befehl eingeben und seine Ausgabe überprüfen:

    `system node autosupport show -node node1,node2`

    Die Befehlsausgabe gibt an, ob AutoSupport aktiviert ist. Wie im folgenden Beispiel gezeigt:

```
cluster::> system node autosupport show -node node1,node2

Node              State     From          To                Mail Hosts
----------------- --------- ------------- ----------------  ----------
node1             enable    Postmaster    admin@netapp.com  mailhost

node2             enable    Postmaster    -                 mailhost
2 entries were displayed.
```

33. Führen Sie eine der folgenden Aktionen durch:

Wenn das ursprüngliche System…	**Dann…**
Hat AutoSupport aktiviert…	Gehen Sie zu Schritt 34.

Wenn das ursprüngliche System…	Dann…
AutoSupport ist nicht aktiviert…	Aktivieren Sie AutoSupport, indem Sie den Anweisungen in der Systemverwaltungsreferenz_ folgen. (Siehe "Quellen" Zum Verknüpfen mit der Referenz *Systemadministration*.) **Hinweis:** AutoSupport ist standardmäßig aktiviert, wenn Sie Ihr Speichersystem zum ersten Mal konfigurieren. Sie können AutoSupport zwar jederzeit deaktivieren, jedoch sollten Sie sie aktiviert lassen. Wenn Sie AutoSupport aktivieren, können Sie erheblich dabei helfen, Probleme und Lösungen zu identifizieren, sollten bei Ihrem Storage-System Probleme auftreten.

34. Überprüfen Sie, ob AutoSupport mit den korrekten E-Mail-IDs für den Mailhost konfiguriert ist, indem Sie auf beiden Originalknoten den folgenden Befehl eingeben und die Ausgabe prüfen:

    `system node autosupport show -node node_name -instance`

    Ausführliche Informationen zu AutoSupport finden Sie unter "Quellen" Link zu den Befehlen *Systemadministration Reference* und *ONTAP 9: Manual Page Reference*.

35. Senden Sie eine AutoSupport-Nachricht für node1 an NetApp, indem Sie den folgenden Befehl eingeben:

    `system node autosupport invoke -node node1 -type all -message "Upgrading node1 from platform_old to platform_new"`

    Senden Sie jetzt keine AutoSupport Nachricht für node2 an NetApp. Sie gehen das später im Verfahren vor.

36. Überprüfen Sie, ob die AutoSupport-Meldung gesendet wurde, indem Sie den folgenden Befehl eingeben und die Ausgabe prüfen:

    `system node autosupport show -node *node1* -instance`

    Felder `Last Subject Sent:` Und `Last Time Sent:` Enthält den Nachrichtentitel der letzten gesendeten Nachricht und den Zeitpunkt, zu dem die Nachricht gesendet wurde.

37. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:

    - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
    - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

    FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

    SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

"Weitere Informationen zu unterstützten Self-Encrypting Drives".

Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung von Authentifizierungsschlüsseln verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager onboard show-backup` Befehl.

SnapMirror Beziehungen stilllegen

Bevor Sie das System mit dem Netzboot booten, müssen Sie sicherstellen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   > Wenn der Status lautet `Transferring`, Sie müssen diese Transfers abbrechen: `snapmirror abort -destination-vserver` *`vserver name`*

   Der Abbruch schlägt fehl, wenn die SnapMirror-Beziehung sich nicht im befindet `Transferring` Bundesland.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Vorbereitungen für den Netzboot

Nachdem Sie später noch Node3 und node4 physisch gerast haben, müssen Sie sie eventuell als Netzboot Netboot eingesetzt werden. Der Begriff *boots* bedeutet, dass Sie von einem 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.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.

- Siehe "Quellen" Um eine Verknüpfung zur NetApp Support-Website zu erhalten und die erforderlichen Systemdateien für Ihre Plattform und die richtige Version von ONTAP herunterzuladen.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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.

Sie müssen die Controller jedoch nicht per Netzboot fahren, wenn auf den Original-Controllern die gleiche Version von ONTAP 9 installiert ist. Wenn ja, können Sie diesen Abschnitt überspringen und mit fortfahren "Phase 3: Installieren und booten node3".

Schritte

1. auf der NetApp Support-Website können Sie die Dateien herunterladen, die zum Ausführen des Netzboots des Systems verwendet werden.
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. 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 FAS/AFF8000 Serie	Extrahieren Sie den Inhalt des `<ontap_version>_image.tgz` Datei zum Zielverzeichnis:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz`HINWEIS: Sie müssen den Inhalt des nicht extrahieren `<ontap_version>_image.tgz` Datei:

Sie verwenden Informationen in den Verzeichnissen in "Phase 3".

Stufe 2: Knoten1 verschieben und ausmustern

Phase-2-Übersicht

Während Phase 2 verschieben Sie Aggregate ohne Root-Root-Fehler von Knoten1 auf

Knoten2 und verschieben Daten-LIFs, die nicht-SAN-Daten-LIFs gehören, die sich im Besitz von node1 befinden, auf Knoten 2, einschließlich fehlgeschlagener oder Vetos. Sie notieren auch die notwendigen Node1-Informationen, die Sie später im Verfahren verwenden können, und setzen dann node1 aus.

Schritte

1. "Verlagerung von Aggregaten außerhalb der Root-Ebene und NAS-Daten-LIFs, die sich im Besitz von node1 auf node2 befinden"
2. "Das Verschieben von NAS-Daten-LIFs von node1 auf node2"
3. "Node1-Informationen werden aufgezeichnet"
4. "Node1 ausmustern"

Verschiebung von nicht-Root-Aggregaten von node1 auf node2

Bevor Sie node1 durch node3 ersetzen können, müssen Sie die nicht-Root-Aggregate von node1 auf node2 verschieben, indem Sie den Befehl Storage Aggregate Relocation verwenden und dann die Verschiebung überprüfen.

Schritte

1. Verschieben der nicht-Root-Aggregate durch Ausfüllen der folgenden Teilschritte:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      ```
      set -privilege advanced
      ```

   b. Geben Sie den folgenden Befehl ein:

      ```
      storage aggregate relocation start -node node1 -destination node2 -aggregate
      -list * -ndo-controller-upgrade true
      ```

   c. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge werden im Hintergrund stattfinden. Um ein Aggregat verschieben zu können, dauerte der Vorgang einige Sekunden oder Minuten. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

   d. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:

      ```
      set -privilege admin
      ```

2. Überprüfen Sie den Versetzungsstatus, indem Sie auf node1 den folgenden Befehl eingeben:

   ```
   storage aggregate relocation show -node node1
   ```

   Die Ausgabe wird angezeigt `Done` Für ein Aggregat, nachdem es verlegt wurde.

   Warten Sie, bis alle nicht-Root-Aggregate im Besitz von node1 in node2 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

3. Führen Sie eine der folgenden Aktionen durch:

Wenn Umzug…	Dann…
Von allen Aggregaten ist erfolgreich	Gehen Sie zu Schritt 4.
Fällt ein Aggregate aus oder kommt ein Vetos vor	a. Überprüfen Sie die EMS-Protokolle auf Korrekturmaßnahmen. b. Führen Sie die Korrekturmaßnahme durch. c. Verschiebung ausgefallener oder Vetos von Aggregaten: `storage aggregate relocation start -node node1 - destination node2 -aggregate-list * -ndo -controller-upgrade true` d. Geben Sie bei der entsprechenden Aufforderung ein `y`. e. Zurück zur Administratorebene: `set -privilege admin`Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen: ◦ Veto-Prüfungen überschreiben: `storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade` ◦ Zielprüfungen überschreiben: `storage aggregate relocation start -override -destination-checks true -ndo-controller -upgrade` Siehe "Quellen" Link zum *Disk- und Aggregatmanagement mit dem CLI* Inhalt und den *ONTAP 9 Befehlen: Manual Page Reference* Weitere Informationen zu den Befehlen zum Verlegen von Speicheraggregaten.

4. Überprüfen Sie, ob alle nicht-Root-Aggregate online sind und ihren Status auf node2:

`storage aggregate show -node node2 -state online -root false`

Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

```
cluster::> storage aggregate show -node node2 state online -root false
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr_1
           744.9GB 744.8GB      0% online       5 node2
raid_dp,

normal
aggr_2     825.0GB 825.0GB      0% online       1 node2
raid_dp,

normal
2 entries were displayed.
```

Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

`storage aggregate online -aggregate *aggr_name*`

5. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 eingeben und seine Ausgabe prüfen:

   `volume show -node *node2* -state offline`

   Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

   `volume online -vserver *vserver-name* -volume *volume-name*`

   Der `vserver-name` Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

6. Geben Sie auf node2 den folgenden Befehl ein:

   `storage failover show -node *node2*`

   Die Ausgabe sollte die folgende Meldung anzeigen:

   ```
   Node owns partner's aggregates as part of the nondisruptive controller
   upgrade procedure.
   ```

7. Vergewissern Sie sich, dass node1 keine im Besitz von nicht-Root-Aggregaten ist, die online sind:

   `storage aggregate show -owner-name *node1* -ha-policy sfo -state online`

   Die Ausgabe sollte keine online nicht-Root-Aggregate anzeigen, die bereits in node2 verschoben wurden.

Verschieben Sie NAS-Daten-LIFs von node1 auf node2

Bevor Sie node1 durch node3 ersetzen können, müssen Sie die NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf node2 verschieben, wenn Sie ein Cluster mit zwei Nodes haben, oder auf einen dritten Node, wenn Ihr Cluster mehr als zwei Nodes hat. Die von Ihnen verwendete Methode hängt davon ab, ob das Cluster für NAS oder SAN konfiguriert ist.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. Sie müssen überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Führen Sie alle auf node1 gehosteten NAS-Daten-LIFs auf, indem Sie den folgenden Befehl eingeben und die Ausgabe erfassen:

   `network interface show -data-protocol nfs|cifs -curr-node node1`

```
 cluster::> network interface show -data-protocol nfs|cifs -curr-node
node1

          Logical     Status      Network             Current   Current
Is
 Vserver  Interface   Admin/Oper  Address/Mask        Node      Port
Home
 -------- ----------  ----------  ------------------  --------- -------
----
 vs0
          a0a         up/down     10.63.0.53/24       node1     a0a
true
          data1       up/up       10.63.0.50/18       node1     e0c
true
          rads1       up/up       10.63.0.51/18       node1     e1a
true
          rads2       up/down     10.63.0.52/24       node1     e1b
true
 vs1
          lif1        up/up       192.17.176.120/24   node1     e0c
true
          lif2        up/up       172.17.176.121/24   node1     e1a
true
```

2. Ändern Sie die Einstellungen zur automatischen Zurücksetzen aller LIFs auf node1 und node2:

   `network interface modify -vserver Vserver_name -lif LIF_name -auto-revert`

```
false
```

3. Nehmen Sie die folgenden Schritte auf, um alle NAS-Daten-LIFs zu migrieren, die auf Schnittstellengruppen und VLANs auf node1 gehostet werden:

   a. [[subepa] Migrieren Sie die LIFs, die auf einer beliebigen Interface Groups gehostet werden, und die VLANs auf node1 zu einem Port auf node2, der in der Lage ist, LIFs auf demselben Netzwerk wie die der Interface Groups zu hosten, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

   ```
   network interface migrate -vserver Vserver_name -lif LIF_name -destination
   -node node2 -destination-port netport|ifgrp
   ```

   b. Ändern Sie den Home-Port und den Home-Node der LIFs und VLANs in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

   ```
   network interface modify -vserver Vserver_name -lif LIF_name -home-node
   node2 - home-port netport|ifgrp
   ```

4. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 5 Bis Schritt 8.
San	Deaktivieren Sie alle SAN-LIFs auf dem Node, um sie für das Upgrade herunterzufahren: `network interface modify -vserver *Vserver-name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

5. NAS-Daten-LIFs von node1 nach node2 migrieren, indem Sie den folgenden Befehl eingeben, einmal für jede Daten-LIF:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name -destination
   -node node2 -destination-port data_port
   ```

6. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs an die richtigen Ports verschoben wurden und dass die LIFs den Status von „up“ aufweisen. Geben Sie dazu den folgenden Befehl an einem der beiden Nodes ein und überprüfen Sie die Ausgabe:

   ```
   network interface show -curr-node node2 -data-protocol nfs|cifs
   ```

7. Ändern Sie den Home-Node der migrierten LIFs:

   ```
   network interface modify -vserver Vserver-name -lif LIF_name -home-node node2
   -home-port port_name
   ```

8. Überprüfen Sie, ob die LIF den Port als ihren Home- oder aktuellen Port verwendet. Wenn der Port nicht zu Hause oder der aktuelle Port ist, fahren Sie mit fort Schritt 9:

   ```
   network interface show -home-node node2 -home-port port_name

   network interface show -curr-node node_name -curr-port port_name
   ```

9. Wenn die LIFs den Port als Home-Port oder aktuellen Port verwenden, ändern Sie die LIF und verwenden Sie einen anderen Port:

   ```
   network interface migrate -vserver Vserver-name -lif LIF_name
   -destination-node node_name -destination-port port_name

   network interface modify -vserver Vserver-name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

10. Wenn eine der LIFs ausgefallen sind, setzen Sie den Administrationsstatus der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

    ```
    network interface modify -vserver Vserver-name -lif LIF_name -home-node
    nodename -status-admin up
    ```

    Bei MetroCluster Konfigurationen können Sie die Broadcast-Domäne eines Ports möglicherweise nicht ändern, da dieser einem Port zugewiesen ist, der die LIF einer Ziel-Storage Virtual Machine (SVM) hostet. Geben Sie den folgenden Befehl von der entsprechenden Quell-SVM auf dem Remote-Standort ein, um die Ziel-LIF einem entsprechenden Port zuzuweisen:
    `metrocluster vserver resync -vserver Vserver_name`

11. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu überprüfen, ob auf node1 keine Daten-LIFs mehr vorhanden sind:

    ```
    network interface show -curr-node node1 -role data
    ```

Node1-Informationen aufzeichnen

Bevor Sie node1 herunterfahren und außer Betrieb nehmen können, müssen Sie Informationen über das Cluster-Netzwerk, die Management- und FC-Ports sowie seine NVRAM-System-ID aufzeichnen. Sie benötigen diese Informationen später im Verfahren, wenn Sie node1 Node3 zuordnen und Festplatten neu zuweisen.

Schritte

1. Geben Sie den folgenden Befehl ein, und erfassen Sie die Ausgabe:

   ```
   network route show
   ```

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

   ```
   cluster::> network route show

   Vserver         Destination    Gateway      Metric
    -------------- -------------- ----------- -------
    iscsi vserver  0.0.0.0/0       10.10.50.1  20
    node1          0.0.0.0/0       10.10.20.1  10
    ....
    node2          0.0.0.0/0       192.169.1.1 20
   ```

2. Geben Sie den folgenden Befehl ein und erfassen Sie die Ausgabe:

   ```
   vserver services name-service dns show
   ```

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

   ```
    cluster::> vserver services name-service dns show
                                                                        Name
    Vserver         State     Domains                                   Servers
    --------------- --------- ------------------------------------
   ---------------
    node 1 2        enabled   alpha.beta.gamma.netapp.com
   10.10.60.10,

   10.10.60.20
    vs_base1        enabled   alpha.beta.gamma.netapp.com,
   10.10.60.10,
                              beta.gamma.netapp.com,
   10.10.60.20
    ...
    ...
    vs peer1         enabled  alpha.beta.gamma.netapp.com,
   10.10.60.10,
                              gamma.netapp.com
   10.10.60.20
   ```

3. Suchen Sie die Cluster-Netzwerk- und Node-Management-Ports auf node1, indem Sie auf einem der Controller den folgenden Befehl eingeben:

   ```
   network interface show -curr-node node1 -role cluster,intercluster,node-
   mgmt,cluster-mgmt
   ```

   Das System zeigt die LIFs für das Cluster, das Intercluster, das Node-Management und das Cluster-Management für den Node im Cluster an, wie im folgenden Beispiel dargestellt:

```
 cluster::> network interface show -curr-node <node1>
            -role cluster,intercluster,node-mgmt,cluster-mgmt

              Logical       Status     Network            Current
Current Is
  Vserver     Interface     Admin/Oper Address/Mask       Node     Port
Home
  ----------- ------------- ---------- ------------------ --------
------- ----
  vserver1
              cluster mgmt   up/up     192.168.x.xxx/24   node1    e0c
true
  node1
              intercluster   up/up     192.168.x.xxx/24   node1    e0e
true
              clus1          up/up     169.254.xx.xx/24   node1    e0a
true
              clus2          up/up     169.254.xx.xx/24   node1    e0b
true
              mgmt1          up/up     192.168.x.xxx/24   node1    e0c
true
 5 entries were displayed.
```

Das System verfügt möglicherweise über keine Intercluster-LIFs.

4. Erfassen Sie die Informationen in der Ausgabe des Befehls in Schritt 3 Zur Verwendung im Abschnitt "Ports von node1 nach node3 zuordnen".

   Die Ausgabeinformationen sind erforderlich, um die neuen Controller-Ports den alten Controller-Ports zuzuordnen.

5. Geben Sie den folgenden Befehl für node1 ein:

   `network port show -node node1 -type physical`

   Das System zeigt die physischen Ports auf dem Node an, wie im folgenden Beispiel dargestellt:

```
 sti8080mcc-htp-008::> network port show -node sti8080mcc-htp-008 -type
physical

 Node: sti8080mcc-htp-008

                                                                        Ignore
                                                  Speed(Mbps)  Health   Health
 Port   IPspace  Broadcast Domain Link MTU   Admin/Oper   Status   Status
 ----   -------  ---------------- ---- ----  -----------  -------
-------
 e0M    Default  Mgmt             up   1500  auto/1000    healthy  false
 e0a    Default  Default          up   9000  auto/10000   healthy  false
 e0b    Default  -                up   9000  auto/10000   healthy  false
 e0c    Default  -                down 9000  auto/-       -        false
 e0d    Default  -                down 9000  auto/-       -        false
 e0e    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0f    Default  -                up   9000  auto/10000   healthy  false
 e0g    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0h    Default  Default          up   9000  auto/10000   healthy  false
 9 entries were displayed.
```

6. Notieren Sie die Ports und ihre Broadcast-Domänen.

   Die Broadcast-Domänen müssen später im Verfahren den neuen Ports auf dem neuen Controller zugeordnet werden.

7. Geben Sie den folgenden Befehl für node1 ein:

   `network fcp adapter show -node *node1*`

   Das System zeigt die FC-Ports auf dem Node an, wie im folgenden Beispiel dargestellt:

```
 cluster::> fcp adapter show -node <node1>
                      Connection  Host
 Node         Adapter Established Port Address
 ------------ ------- ----------- ------------
 node1
               0a     ptp         11400
 node1
               0c     ptp         11700
 node1
               6a     loop        0
 node1
               6b     loop        0
 4 entries were displayed.
```

8. Notieren Sie die Ports.

   Die Ausgabeinformationen sind erforderlich, um die neuen FC-Ports auf dem neuen Controller später im Verfahren zuzuordnen.

9. Falls Sie dies zuvor nicht getan haben, überprüfen Sie, ob auf node1 Schnittstellengruppen oder VLANs konfiguriert sind, indem Sie die folgenden Befehle eingeben:

   ```
   network port ifgrp show

   network port vlan show
   ```

   Sie verwenden die Informationen im Abschnitt "Ports von node1 nach node3 zuordnen".

10. Führen Sie eine der folgenden Aktionen durch:

Sie suchen…	Dann…
Die NVRAM-System-ID-Nummer im Abschnitt wurde aufgezeichnet "Bereiten Sie die Knoten auf das Upgrade vor".	Weiter mit dem nächsten Abschnitt "Node1 ausmustern".
Die NVRAM-System-ID-Nummer wurde nicht in den Abschnitt aufgezeichnet "Bereiten Sie die Knoten auf das Upgrade vor"	Vollständig Schritt 11 Und Schritt 12 Und dann weiter zu "Node1 ausmustern".

11. Geben Sie den folgenden Befehl auf einem der Controller ein:

    ```
    system node show -instance -node node1
    ```

    Das System zeigt Informationen über node1 an, wie im folgenden Beispiel dargestellt:

    ```
    cluster::> system node show -instance -node <node1>
                                Node: node1
                               Owner:
                            Location: GDl
                               Model: FAS6240
                       Serial Number: 700000484678
                           Asset Tag: -
                              Uptime: 20 days 00:07
                     NVRAM System ID: 1873757983
                           System ID: 1873757983
                              Vendor: NetApp
                              Health: true
                         Eligibility: true
    ```

12. notieren Sie die im Abschnitt zu verwendende NVRAM-System-ID "Installieren und booten Sie node3".

Node1 ausmustern

Um node1 außer Betrieb zu nehmen, müssen Sie das HA-Paar mit node2 deaktivieren, Node1 richtig herunterfahren und aus dem Rack oder Chassis entfernen.

Schritte

1. Überprüfen Sie die Anzahl der Nodes im Cluster:

   ```
   cluster show
   ```

   Das System zeigt die Nodes im Cluster an, wie im folgenden Beispiel dargestellt:

   ```
   cluster::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node1                 true    true
   node2                 true    true
   2 entries were displayed.
   ```

2. Speicherausfallschutz nach Bedarf deaktivieren:

Falls das Cluster…	Dann…

Eines Clusters mit zwei Nodes	a. Deaktivieren Sie die Hochverfügbarkeit des Clusters, indem Sie auf einem der Nodes den folgenden Befehl eingeben:
	`cluster ha modify -configured false`
	a. Deaktivier Speicher-Failover:
	`storage failover modify -node node1 -enabled false`

Ein Cluster mit mehr als zwei Nodes	Deaktivier Speicher-Failover: `storage failover modify -node node1 -enabled false`

   Wenn Sie Storage-Failover nicht deaktivieren, kann es zu einem Ausfall des Controller-Upgrades kommen, der den Datenzugriff unterbrechen und zu Datenverlusten führen kann.

3. Überprüfen Sie, ob der Storage-Failover deaktiviert wurde:

   ```
   storage failover show
   ```

   Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl, wenn Storage-Failover für einen Node deaktiviert wurde:

```
 cluster::> storage failover show
                                 Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node1          node2          false    Connected to node2, Takeover
                                        is not possible: Storage
failover is
                                        disabled

 node2          node1          false    Node owns partner's aggregates
as part
                                        of the nondisruptive controller
upgrade
                                        procedure. Takeover is not
possible:
                                        Storage failover is disabled
 2 entries were displayed.
```

4. Überprüfen Sie den Daten-LIF-Status:

   `network interface show -role data -curr-node node2 -home-node node1`

   Sehen Sie in der Spalte **Status Admin/Oper** nach, ob LIFs nicht verfügbar sind. Wenn LIFs ausgefallen sind, lesen Sie das "Troublehsoot" Abschnitt.

5. Führen Sie eine der folgenden Aktionen durch:

Falls das Cluster…	Dann…
Eines Clusters mit zwei Nodes	Gehen Sie zu Schritt 6.
Ein Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 8.

6. Zugriff auf die erweiterte Berechtigungsebene auf beiden Knoten:

   `set -privilege advanced`

7. Überprüfen Sie, ob die Cluster-HA deaktiviert wurde:

   `cluster ha show`

   Vom System wird die folgende Meldung angezeigt:

```
High Availability Configured: false
```

   Wenn Cluster HA nicht deaktiviert wurde, wiederholen Sie den Vorgang Schritt 2.

8. Prüfen Sie, ob node1 aktuell epsilon hält:

   `cluster show`

   Da in einem Cluster mit einer geraden Anzahl von Nodes eine Krawatte möglich ist, verfügt ein Node über eine zusätzliche fraktionale Abstimmungsgewichtung namens epsilon. Siehe "Quellen" Um weitere Informationen zur *System Administration Reference* zu erhalten.

   > Wenn Sie ein Cluster mit vier Nodes haben, liegt das Epsilon auf einem Node in einem anderen HA-Paar im Cluster.
   >
   > Wenn Sie ein HA-Paar in einem Cluster mit mehreren HA-Paaren aktualisieren, müssen Sie Epsilon auf den Node eines HA-Paars verschieben, ohne ein Controller-Upgrade durchführen zu müssen. Wenn Sie beispielsweise nodeA/nodeB in einem Cluster mit der HA-Paar-Konfiguration nodeA/nodeB und nodeC/nodded aktualisieren, müssen Sie Epsilon auf nodeC oder nodded verschieben.

   Das folgende Beispiel zeigt, dass bei node1 Epsilon gehalten wird:

   ```
   cluster::*> cluster show

   Node                  Health  Eligibility  Epsilon
   --------------------- ------- ------------ ------------
   node1                 true    true         true
   node2                 true    true         false
   ```

9. Wenn node1 das Epsilon hält, markieren Sie das Epsilon `false` Auf dem Knoten, so dass er auf die node2 übertragen werden kann:

   `cluster modify -node *node1* -epsilon false`

10. Übertragen Sie das Epsilon auf node2, indem Sie epsilon markieren `true` Auf Knoten 2:

    `cluster modify -node *node2* -epsilon true`

11. Vergewissern Sie sich, dass die Änderung in node2 aufgetreten ist:

    `cluster show`

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

    Das Epsilon für node2 sollte nun wahr sein und das Epsilon für node1 sollte falsch sein.

12. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

13. Zurück zur Administratorebene:

```
set -privilege admin
```

14. Stop node1 von der Eingabeaufforderung node1:

```
system node halt -node node1
```

> **Achtung**: Wenn sich Node1 im selben Gehäuse wie node2 befindet, schalten Sie das Gehäuse nicht über den Netzschalter oder durch Ziehen des Netzkabels aus. Wenn Sie das tun, wird node2, der Daten bereitstellt, ausfallen.

15. Wenn Sie vom System aufgefordert werden, zu bestätigen, dass Sie das System anhalten möchten, geben Sie ein `y`.

    Der Node wird an der Eingabeaufforderung der Boot-Umgebung angehalten.

16. Wenn in node1 die Eingabeaufforderung für die Boot-Umgebung angezeigt wird, entfernen Sie sie aus dem Chassis oder dem Rack.

    Sie können Node1 nach Abschluss des Upgrades außer Betrieb nehmen. Siehe "Ausmustern des alten Systems".

Phase 3: Installieren und booten Sie node3

Phase-3-Übersicht

In Phase 3 installieren und booten Sie Knoten3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu und verschieben Daten-LIFs und SAN-LIFs, die zu node1 gehören, von node2 auf node3. Außerdem werden alle Aggregate von node2 auf node3 verschoben und die Daten-LIFs und SAN-LIFs von node2 auf node3 verschoben.

Schritte

1. "Installieren und booten Sie node3"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest"
3. "Ports von node1 nach node3 zuordnen"
4. "Verschieben Sie die NAS-Daten-LIFs von node1 auf node2 und überprüfen Sie SAN LIFs auf node3"
5. "Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3"

6. "Verschieben Sie die NAS-Daten-LIFs von node2 auf node3"

Installieren und booten Sie node3

Sie müssen node3 im Rack installieren, Verbindungen von node1 zu node3, Boot node3 übertragen und ONTAP installieren. Sie müssen auch jede der freien Festplatten von node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die nicht früher auf node2 verschoben wurden, neu zuweisen.

Über diese Aufgabe

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten. Siehe "Vorbereitungen für den Netzboot".

Sie müssen jedoch nicht als Netzboot auf Node3 setzen, wenn es die gleiche oder eine höhere Version von ONTAP 9 hat, die auf node1 installiert ist.

> Wenn Sie ein mit Storage-Arrays verbundenes V-Series System oder ein System mit FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Anforderungen unbedingt zu beachten Schritt 1 Bis Schritt 5, Lassen Sie diesen Abschnitt bei Schritt 6 Und befolgen Sie die Anweisungen unter "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Geben Sie nach Bedarf Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 7.
>
> Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und anschließend mit fortfahren "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

   Wenn sich Node1 und Node2 in einem separaten Chassis befanden, können Sie Node3 in denselben Rack-Standort wie node1 platzieren. Wenn sich jedoch node1 mit node2 im selben Chassis befand, müssen Sie node3 in seinen eigenen Rack-Platz legen, vorzugsweise in der Nähe der Position von node1.

2. Installieren Sie Node3 im Rack gemäß der *Installations- und Setup-Anleitung* für Ihr Node-Modell.

   > Wenn Sie ein Upgrade auf ein System mit beiden Nodes im selben Chassis durchführen, installieren sie node4 sowohl im Chassis als auch in node3. Wenn Sie dies nicht tun, verhält sich der Node, wenn Sie node3 booten, wie in einer Dual-Chassis-Konfiguration. Und wenn Sie node4 booten, wird der Interconnect zwischen den Nodes nicht gestartet.

3. Kabelnode3, Verschieben der Verbindungen von node1 zu node3.

   Die folgenden Referenzen helfen Ihnen dabei, geeignete Kabelverbindungen zu machen. Gehen Sie zu "Quellen" Um eine Verbindung zu ihnen zu machen.

   - *Installations- und Setup-Anleitung* oder *Installationsanforderungen für die FlexArray-Virtualisierung und Referenz* für die node3-Plattform

- Das entsprechende Verfahren für das Festplatten-Shelf
- Die Dokumentation *High Availability Management*

Folgende Anschlüsse verkabeln:

- Konsole (Remote-Management-Port)
- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Möglicherweise müssen Sie die Interconnect-Karte oder die Cluster Interconnect-Kabelverbindung von node1 zu node3 nicht verschieben, da die meisten Plattform-Modelle über ein einzigartiges Interconnect-Kartenmodell verfügen. Für die MetroCluster-Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node1 zu node3 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Einschalten Sie die Stromversorgung auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im gleichen Chassis durchführen, wird node4 auch neu gebootet. Allerdings kann man den node4-Stiefel bis später ignorieren.

   > Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

   ```
   WARNING: The battery is unfit to retain data during a power outage. This
   is likely because the battery is discharged but could be due to other
   temporary conditions.
   When the battery is ready, the boot process will complete and services
   will be engaged.
   To override this delay, press 'c' followed by 'Enter'
   ```

5. Wenn die Warnmeldung in angezeigt wird Schritt 4, Nehmen Sie die folgenden Aktionen:
   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.
   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

      > **Achtung**: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden kann, kann dies zu einem Datenverlust führen.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Überspringen Sie Schritt 7 bis Schritt 12, und fahren Sie mit fort Schritt 13.
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Gehen Sie zu "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest" Und vervollständigen Sie die Unterabschnitte "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren", Je nach Ihrem System. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 7. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

7. Fügen Sie die FC-Initiator-Ports des neuen Knotens zu den Switch-Zonen hinzu.

   Wenn Ihr System über ein Tape-SAN verfügt, müssen Sie das Zoning für die Initiatoren benötigen. Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

8. Fügen Sie die FC-Initiator-Ports zum Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

   Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

9. Ändern Sie die WWPN-Werte (World Wide Port Name) in den Host- oder Volume-Gruppen, die mit Array LUNs auf dem Speicher-Array verknüpft sind.

   Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

10. Wenn Ihre Konfiguration ein Switch-basiertes Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
11. Überprüfen Sie, ob die Array-LUNs jetzt für node3 sichtbar sind:

    ```
    sysconfig -v
    ```

    Das System zeigt alle Array-LUNs an, die für jeden FC-Initiator-Port sichtbar sind. Wenn die Array-LUNs nicht sichtbar sind, können Sie Festplatten von node1 zu node3 später in diesem Abschnitt nicht neu zuweisen.

12. Drücken Sie Strg-C, um das Boot-Menü anzuzeigen und den Wartungsmodus auszuwählen.
13. Geben Sie in der Eingabeaufforderung für den Wartungsmodus den folgenden Befehl ein:

    ```
    halt
    ```

    Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

14. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, auf das Sie aktualisieren, in einem ist…	Dann…
Dual-Chassis-Konfiguration (mit Controllern in anderem Chassis)	Gehen Sie zu Schritt 15.
Einzel-Chassis-Konfiguration (mit Controllern im selben Chassis)	a. Schalten Sie das Konsolenkabel von node3 auf node4 um. b. Schalten Sie node4 ein, und unterbrechen Sie den Bootvorgang, indem Sie am Konsolenterminal Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen. Die Stromversorgung sollte bereits eingeschaltet sein, wenn sich beide Controller im gleichen Chassis befinden. verlassen sie node4 an der Boot-Umgebung Eingabeaufforderung; Sie kehren nach node4 in zurück "installieren und booten sie node4". c. Wenn die Warnmeldung in angezeigt wird Schritt 4, Folgen Sie den Anweisungen in Schritt 5 d. Schalten Sie das Konsolenkabel von node4 nach node3 zurück. e. Gehen Sie zu Schritt 15.

15. node3 für ONTAP konfigurieren:

```
set-defaults
```

16. Wenn Sie NetApp Storage Encryption (NSE)-Laufwerke installiert haben, führen Sie die folgenden Schritte aus.

Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

   Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager".

17. [[man_install3_step17] Wenn die auf node3 installierte ONTAP-Version dieselbe oder höher als die auf node1 installierte Version von ONTAP 9 ist, führen Sie die Liste auf und weisen Sie Festplatten der neuen node3 neu zu:

    `boot_ontap`

    Wenn dieser neue Node jemals in einem anderen Cluster oder HA-Paar verwendet wurde, müssen Sie ausgeführt werden `wipeconfig` Bevor Sie fortfahren. Andernfalls kann es zu Serviceausfällen oder Datenverlusten kommen. Wenden Sie sich an den technischen Support, wenn der Ersatz-Controller zuvor verwendet wurde, insbesondere dann, wenn auf den Controllern ONTAP im 7-Mode ausgeführt wurde.

18. Drücken Sie STRG-C, um das Startmenü anzuzeigen.
19. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	**Dann…**
Hat *Not* die richtige oder aktuelle ONTAP-Version auf node3	Gehen Sie zu Schritt 20.
Verfügt über die richtige oder aktuelle Version von ONTAP auf node3	Gehen Sie zu Schritt 25.

20. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

    Sie müssen den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder sonst kann während des Upgrades ein Datenausfall auftreten.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

21. Netzboot auf node3 ausführen:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Führt zu der Stelle, an der Sie das heruntergeladen haben `<ontap_version>_image.tgz` In "Schritt 1" Im Abschnitt *Vorbereiten für Netzboot*.

Unterbrechen Sie den Startvorgang nicht.

22. Wählen Sie im Startmenü die Option **(7) Neue Software installieren** zuerst.

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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

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 Versionen von ONTAP. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt die Startmedien und platziert dieselbe ONTAP-Version-ONTAP auf beiden Bildpartitionen.

23. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie dazu aufgefordert werden, das Paket einzugeben, geben Sie die folgende URL ein:

    `http://<web_server_ip>/<path_to_web-accessible_directory>/<ontap_version_image>.tgz`

24. führen Sie die folgenden Teilschritte durch:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

25. Wählen Sie **(5) Boot im Wartungsmodus** aus, indem Sie eingeben `5`, Und geben Sie dann ein `y` Wenn Sie dazu aufgefordert werden, den Startvorgang fortzusetzen.

26. bevor Sie fortfahren, fahren Sie mit fort "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest" Um alle erforderlichen Änderungen an den FC- oder UTA/UTA2-Ports auf dem Node vorzunehmen.

    Nehmen Sie die in diesen Abschnitten empfohlenen Änderungen vor, booten Sie den Node neu und wechseln Sie in den Wartungsmodus.

27. Suche nach der System-ID von node3:

    `disk show -a`

    Das System zeigt die System-ID des Node sowie Informationen über seine Festplatten an, wie im folgenden Beispiel dargestellt:

```
 *> disk show -a
 Local System ID: 536881109
 DISK     OWNER                    POOL   SERIAL    HOME          DR
 HOME                                     NUMBER
 -------- -------------            -----  -------- -------------
-------------
 0b.02.23 nst-fas2520-2(536880939) Pool0  KPG2RK6F nst-fas2520-
2(536880939)
 0b.02.13 nst-fas2520-2(536880939) Pool0  KPG3DE4F nst-fas2520-
2(536880939)
 0b.01.13 nst-fas2520-2(536880939) Pool0  PPG4KLAA nst-fas2520-
2(536880939)
 ......
 0a.00.0               (536881109) Pool0  YFKSX6JG
(536881109)
 ......
```

Möglicherweise wird die Meldung angezeigt `disk show: No disks match option -a.` Nach Eingabe des Befehls. Dies ist keine Fehlermeldung, sodass Sie mit dem Verfahren fortfahren können.

28. Spares des Rasign node1, alle Festplatten, die zum Root gehören, und alle nicht-Root-Aggregate, die früher in node2 verschoben wurden "Verschiebung von nicht-Root-Aggregaten von node1 auf node2".

Geben Sie das entsprechende Formular des ein `disk reassign` Befehl basierend auf der Frage, ob Ihr System freigegebene Festplatten hat:

Wenn Sie auf Ihrem System freigegebene Festplatten, Hybrid-Aggregate oder beides haben, müssen Sie die korrekte verwenden `disk reassign` Befehl aus der folgenden Tabelle.

Wenn Disk-Typ…	Führen Sie dann den Befehl aus…
Mit gemeinsamen Festplatten	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`* `-p` *`node2_sysid`*
Ohne gemeinsame Festplatten	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`*

Für das *`node1_sysid`* Wert: Verwenden Sie die in erfassten Informationen "Node1-Informationen aufzeichnen". Um den Wert für zu erhalten *`node3_sysid`*, Verwenden Sie die `sysconfig` Befehl.

Der `-p` Die Option ist nur im Wartungsmodus erforderlich, wenn freigegebene Festplatten vorhanden sind.

Der `disk reassign` Befehl gibt nur die Festplatten wieder, für die *`node1_sysid`* Ist der aktuelle Eigentümer.

Vom System wird die folgende Meldung angezeigt:

```
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)?
```

29. Geben Sie ein `n`.

Vom System wird die folgende Meldung angezeigt:

```
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)?
```

30. Geben Sie ein `y`

Vom System wird die folgende Meldung angezeigt:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)?
```

31. Geben Sie ein `y`.

32. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (zum Beispiel AFF A800 Systeme), setzen Sie das node1-Aggregat als root ein, um zu bestätigen, dass node3 aus dem Root-Aggregat von node1 startet.

> **Warnung**: Sie müssen die folgenden Teilschritte in der angegebenen Reihenfolge durchführen; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.

Im folgenden Verfahren wird node3 vom Root-Aggregat von node1 gestartet:

a. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node1 Aggregat:

```
aggr status -r
```

b. Überprüfen Sie den Status des node1-Aggregats:

```
aggr status
```

c. Bringen Sie das node1 Aggregat ggf. online:

```
aggr_online root_aggr_from_node1
```

d. Verhindern Sie, dass das node3 vom ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node3
```

e. Legen Sie das node1-Root-Aggregat als das neue Root-Aggregat für node3 fest:

```
aggr options aggr_from_node1 root
```

f. Überprüfen Sie, ob das Root-Aggregat von node3 offline ist und das Root-Aggregat für die von node1 hergebrachten Festplatten online ist und in den Root-Status eingestellt ist:

```
aggr status
```

> Wenn der vorherige Unterschritt nicht ausgeführt wird, kann node3 vom internen Root-Aggregat booten, oder es kann dazu führen, dass das System eine neue Cluster-Konfiguration übernimmt oder Sie aufgefordert werden, eine zu identifizieren.

Im Folgenden wird ein Beispiel für die Befehlsausgabe angezeigt:

```
-------------------------------------------------------------------
     Aggr State               Status          Options
aggr0_nst_fas8080_15 online   raid_dp, aggr   root, nosnap=on
                              fast zeroed
                              64-bit

  aggr0 offline               raid_dp, aggr   diskroot
                              fast zeroed
                              64-bit
-------------------------------------------------------------------
```

33. Überprüfen Sie, ob Controller und Chassis als konfiguriert sind `ha`:

```
ha-config show
```

Im folgenden Beispiel wird die Ausgabe des Befehls ha-config show angezeigt:

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

Systeme zeichnen sich in einem programmierbaren ROM (PROM) auf, unabhängig davon, ob sie sich in einem HA-Paar oder einer eigenständigen Konfiguration befinden. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

Wenn der Controller und das Chassis nicht als „ha“ konfiguriert wurden, korrigieren Sie die Konfiguration mit den folgenden Befehlen:

```
ha-config modify controller ha

ha-config modify chassis ha
```

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

```
ha-config modify controller mcc

ha-config modify chassis mcc
```

34. zerstören Sie die Mailboxen auf node3:

```
mailbox destroy local
```

Über die Konsole wird die folgende Meldung angezeigt:

```
Destroying mailboxes forces a node to create new empty mailboxes, which
clears any takeover state, removes all knowledge of out-of-date plexes
of mirrored volumes, and will prevent management services from going
online in 2-node cluster HA configurations. Are you sure you want to
destroy the local mailboxes?
```

35. Geben Sie ein `y` Bestätigen Sie an der Eingabeaufforderung, dass Sie die lokalen Mailboxen zerstören möchten.
36. Wartungsmodus beenden:

```
halt
```

Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

37. auf node2 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

```
date
```

38. auf node3 prüfen Sie das Datum an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

39. Ggf. Das Datum auf node3 einstellen:

```
set date mm/dd/yyyy
```

40. in node3 überprüfen Sie die Zeit an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

41. Ggf. Die Zeit auf node3 einstellen:

```
set time hh:mm:ss
```

42. Überprüfen Sie, ob die Partner-System-ID korrekt festgelegt ist, wie in angegeben Schritt 28 Schalter unter -p:

```
printenv partner-sysid
```

43. Ggf. Setzen Sie die Partner-System-ID auf node3:

    `setenv partner-sysid node2_sysid`

    Einstellungen speichern:

    `saveenv`

44. Öffnen Sie das Boot-Menü an der Eingabeaufforderung der Boot-Umgebung:

    `boot_ontap menu`

45. Wählen Sie im Boot-Menü die Option **(6) Flash aus Backup config** aktualisieren, indem Sie eingeben `6` An der Eingabeaufforderung.

    Vom System wird die folgende Meldung angezeigt:

    ```
    This will replace all flash-based configuration with the last backup to
    disks. Are you sure you want to continue?:
    ```

46. Geben Sie ein `y` An der Eingabeaufforderung.

    Der Startvorgang läuft normal weiter, und das System fordert Sie dann auf, die Unstimmigkeit der System-ID zu bestätigen.

    > Das System wird möglicherweise zweimal neu gestartet, bevor die Warnmeldung zur Nichtübereinstimmung angezeigt wird.

47. Bestätigen Sie die Diskrepanz, wie im folgenden Beispiel gezeigt:

    ```
    WARNING: System id mismatch. This usually occurs when replacing CF or
    NVRAM cards!
    Override system id (y|n) ? [n] y
    ```

    Der Node kann vor dem normalen Booten eine Runde des Neubootens durchlaufen.

48. Einloggen in node3.

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest

Wenn node3 integrierte FC-Ports, Onboard Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschluss abschließen Konfigurieren Sie FC-Ports auf node3, Oder UTA/UTA2-Ports in node3 prüfen und konfigurieren, Oder beide Abschnitte.

Für das NetApp Marketingmaterial wird möglicherweise der Begriff „UTA2“ verwendet, um CNA-Adapter und Ports zu beziehen. Die CLI verwendet jedoch den Begriff „CNA“.

- Wenn node3 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie zur springen "Ports von node1 nach node3 zuordnen".
- Wenn Sie jedoch ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware mit Storage-Arrays haben und node3 keine integrierten FC-Ports, Onboard UTA/UTA-Ports oder eine UTA/UTA2-Karte haben, kehren Sie zurück zu *Install and Boot node3* und fahren Sie fort "Schritt 22".

Optionen:

- Konfigurieren Sie FC-Ports auf node3
- UTA/UTA2-Ports in node3 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node3

Wenn node3 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in Betrieb nehmen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node1 haben, die Sie in gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder eine UTA/UTA2-Karte verfügt, konfigurieren Sie sie in UTA/UTA2-Ports in node3 prüfen und konfigurieren.

Wenn Ihr System über Speicherfestplatten verfügt, geben Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle ein. Wenn Sie über ein V-Series System oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie im Wartungsmodus in diesem Abschnitt Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Gehen Sie zu Schritt 5
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 2

2. Boot node3 und Zugriff auf Wartungsmodus:

```
boot_ontap maint
```

3. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Geben Sie den folgenden Befehl ein: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden.	Geben Sie den folgenden Befehl ein `ucadmin show`

Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

4. Vergleichen Sie die FC-Einstellungen von node3 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
5. Nehmen Sie eine der folgenden Aktionen:

Wenn die FC-Standardeinstellungen auf den neuen Nodes sind…	Dann…
Das gleiche wie jene, die ihr auf Node1 gefangen habt	Gehen Sie zu Schritt 11.
Anders als jene, die du auf Node1 gefangen hast	Gehen Sie zu Schritt 6.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node3 nach Bedarf, indem Sie einen der folgenden Befehle eingeben: • So programmieren Sie Zielanschlüsse: `system node hardware unified-connect modify -type
-t target -adapter *port_name*` ** So programmieren Sie Initiator-Ports: `system node hardware unified-connect modify -type	-t initiator -adapter *port_name*`  `-t` Ist der FC4-Typ: Target oder Initiator.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node3 nach Bedarf, indem Sie den folgenden Befehl eingeben: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

7. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `ucadmin show`

8. Beenden des Wartungsmodus durch Eingabe des folgenden Befehls:

```
halt
```

9. nach Eingabe des Befehls warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.

10. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder verfügt FlexArray Virtualisierungssoftware mit Clustered Data ONTAP 8.3	Boot Node3 und Wartung an der Eingabeaufforderung für die Boot-Umgebung: `boot_ontap maint`
Ist kein V-Series System oder verfügt über keine FlexArray Virtualisierungssoftware	Boot node3 an der Eingabeaufforderung Boot-Umgebung: `boot_ontap`

11. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, gehen Sie zu UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen UTA/UTA2-Ports in node3 prüfen und konfigurieren Und gehen Sie zu "Ports von node1 nach node3 zuordnen".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Wenn kein Knoten 3 über eine Karte oder Onboard-Ports verfügt, gehen Sie zu UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn kein Karten- oder Onboard-Port für node3 vorhanden ist, überspringen Sie UTA/UTA2-Ports in node3 prüfen und konfigurieren, Und zurück zu *Install und Boot node3* und wieder bei "Schritt 7".

UTA/UTA2-Ports in node3 prüfen und konfigurieren

Wenn node3 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie möglicherweise neu konfigurieren, je nachdem, wie Sie das aktualisierte System verwenden möchten.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

Wenn Sie einen Unified Target Adapter (UTA/UTA2)-Port für FC verwenden möchten, müssen Sie zuerst überprüfen, wie der Port konfiguriert ist.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

Sie können das verwenden `ucadmin show` Befehl zum Überprüfen der aktuellen Portkonfiguration:

```
*> ucadmin show
          Current  Current    Pending  Pending    Admin
 Adapter  Mode     Type       Mode     Type       Status
 -------  -------  ---------  -------  ---------  -----------
 0e       fc       target     -        initiator  offline
 0f       fc       target     -        initiator  offline
 0g       fc       target     -        initiator  offline
 0h       fc       target     -        initiator  offline
 1a       fc       target     -        -          online
 1b       fc       target     -        -          online
6 entries were displayed.
```

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht gleichzeitige NIC- und FCoE-Traffic über die gleiche 10-GbE-SFP+-Schnittstelle und unterstützt FC-Ziele.

UTA/UTA2-Ports befinden sich möglicherweise auf einem Adapter oder auf dem Controller und verfügen über die folgenden Konfigurationen. Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf der node3 überprüfen und gegebenenfalls ändern:

- UTA-/UTA2-Karten, die bestellt werden, werden vor dem Versand konfiguriert, um die von Ihnen geforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden vor dem Versand konfiguriert, um die Persönlichkeit zu erhalten, die Sie anfordern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, müssen Sie an der Eingabeaufforderung des Clusters die Befehle in diesem Abschnitt eingeben, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein VSeries-System verfügen oder über FlexArray-Virtualisierungssoftware verfügen und mit Speicherarrays verbunden sind, müssen Sie in diesem Abschnitt Befehle in der Eingabeaufforderung für den Wartungsmodus eingeben. Sie müssen sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit konfiguriert sind, und geben Sie auf node3 die folgenden Befehle ein:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt eine Ausgabe an, die den folgenden Beispielen entspricht:

```
cluster1::> system node hardware unified-connect show

                 Current  Current    Pending  Pending  Admin
Node  Adapter    Mode     Type       Mode     Type     Status
----  -------    -------  ---------  -------  -------  ------
f-a   0e         fc       initiator  -        -        online
f-a   0f         fc       initiator  -        -        online
f-a   0g         cna      target     -        -        online
f-a   0h         cna      target     -        -        online
f-b   0e         fc       initiator  -        -        online
f-b   0f         fc       initiator  -        -        online
f-b   0g         cna      target     -        -        online
f-b   0h         cna      target     -        -        online
12 entries were displayed.
```

```
*> ucadmin show
          Current  Current    Pending  Pending  Admin
Adapter   Mode     Type       Mode     Type     Status
-------   -------  ---------  -------  -------  ------
0e        fc       initiator  -        -        online
0f        fc       initiator  -        -        online
0g        cna      target     -        -        online
0h        cna      target     -        -        online
0e        fc       initiator  -        -        online
0f        fc       initiator  -        -        online
0g        cna      target     -        -        online
0h        cna      target     -        -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Untersuchung der Ausgabe des `system node hardware unified-connect show` Oder `ucadmin show` Befehl zum Bestimmen, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.

4. Nehmen Sie eine der folgenden Aktionen:

Wenn die UTA/UTA2-Ports…	**Dann…**
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Es gibt Storage-Festplatten, auf denen Clustered Data ONTAP 8.3 ausgeführt wird	Boot-Knoten3 und wechseln in den Wartungsmodus: `boot_ontap maint`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 6. Sie sollten sich bereits im Wartungsmodus befinden.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7.
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

7. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Ziel-Modus sind im Wartungsmodus automatisch offline.

8. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` Ist der Persönlichkeitsmodus, `fc` Oder `cna`.
   - `-t` Ist der Typ FC4, `target` Oder `initiator`.

   > Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

9. Überprüfen Sie die Einstellungen:

   `ucadmin show`

10. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…

Festplatten sind vorhanden	a. Anhalten des Systems:
	`halt`
	Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.
	b. Geben Sie den folgenden Befehl ein:
	`boot_ontap`

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Neubooten in den Wartungsmodus: `boot_netapp maint`

11. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist eine V-Series oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
cluster1::> system node hardware unified-connect show

                Current  Current    Pending  Pending      Admin
Node  Adapter   Mode     Type       Mode     Type         Status
----  -------   -------  ---------  -------  -----------  ------
f-a   1a        fc       initiator  -        -            online
f-a   1b        fc       target     -        initiator    online
f-a   2a        fc       target     cna      -            online
f-a   2b        fc       target     cna      -            online

4 entries were displayed.
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  ------
1a       fc       initiator  -        -          online
1b       fc       target     -        initiator  online
2a       fc       target     cna      -          online
2b       fc       target     cna      -          online
*>
```

12. Platzieren Sie alle Zielports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

13. Anschluss verkabeln.
14. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Ports von node1 nach node3 zuordnen".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zu *Install and Boot node3* zurück und fahren Sie bei fort "Schritt 7".

Ports von node1 nach node3 zuordnen

Sie müssen sicherstellen, dass die physischen Ports auf node1 den physischen Ports auf node3 korrekt zugeordnet werden. Somit kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Bevor Sie beginnen

Sie müssen von *Hardware Universe* bereits über die Ports auf den neuen Nodes verfügen. (Gehen Sie zu "Quellen" Zum Verknüpfen mit dem *Hardware Universe*). Sie verwenden die Informationen später in diesem Abschnitt und in "Weisen Sie Ports von node2 nach node4 zu".

Die Softwarekonfiguration von node3 muss mit der physischen Konnektivität von node3 übereinstimmen. Die IP-Konnektivität muss wiederhergestellt werden, bevor Sie mit dem Upgrade fortfahren.

Über diese Aufgabe

Die Port-Einstellungen können je nach Modell der Nodes variieren.

Schritte

1. Überprüfen Sie mit den folgenden Schritten, ob es sich um ein Cluster mit zwei Nodes ohne Switches handelt:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

      `network options switchless-cluster show`

      Beispiel:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

   +
   Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

   a. Zurück zur Administratorberechtigungsebene:

      `set -privilege admin`

2. Änderungen vornehmen:

   a. Ports ändern, die Teil der Cluster Broadcast Domain sein werden:

      `network port modify -node` *`node_name`* `-port` *`port_name`* `-mtu 9000 -ipspace Cluster`

      Dieses Beispiel fügt Cluster Port e1b hinzu auf „node1“:

```
network port modify -node node1 -port e1b -ipspace Cluster -mtu 9000
```

   b. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

      `network interface migrate -vserver` *`Vserver_name`* `-lif` *`lif_name`* `-source-node` *`node1`* `-destination-node` *`node1`* `-destination-port` *`port_name`*

      Wenn alle Cluster-LIFs migriert und die Cluster-Kommunikation eingerichtet ist, sollte das Cluster ein Quorum bilden.

   c. Ändern Sie den Startport der Cluster LIFs:

      `network interface modify -vserver Cluster -lif` *`lif_name`* `-home-port` *`port_name`*

   d. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports node1:port
```

e. Anzeigen des Funktionszustands von node1 und node3:

```
cluster show -node node1 -fields health
```

f. Führen Sie abhängig von der ONTAP-Version auf dem zu aktualisierenden HA-Paar eine der folgenden Aktionen durch:

Lautet Ihre ONTAP Version…	Dann…
9.8 bis 9.11.1	Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören: `::> network connections listening show -vserver Cluster`
9.12.1 oder höher	Überspringen Sie diesen Schritt und gehen Sie zu Schritt 3.

Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

g. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Wiederholen Sie den Unterschritt (f), um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 nachhört.

3. Ändern Sie die Mitgliedschaften der Broadcast-Domäne von physischen Ports, die Daten-LIFs hosten.

a. Listen Sie den Status der Erreichbarkeit aller Ports auf:

```
network port reachability show
```

b. Reparieren Sie die Erreichbarkeit der physischen Ports, gefolgt von VLAN-Ports, indem Sie den folgenden Befehl an jedem Port, jeweils einen Port, ausführen:

```
reachability repair -node node_name -port port_name
```

Es wird eine Warnung wie folgt erwartet. Überprüfen und eingeben `y` Oder `n` Gegebenenfalls:

```
WARNING: Repairing port "node_name:port" might cause it to move into
a different broadcast domain, which can cause LIFs to be re-homed
away from the port. Are you sure you want to continue? {y|n}:
```

c. Um ONTAP zum Abschließen der Reparatur zu aktivieren, warten Sie etwa eine Minute nach Ausführung des `reachability repair` Befehl am letzten Port.

d. Alle Broadcast-Domänen auf dem Cluster auflisten:

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

e. Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der vorhandenen Broadcast-Domänen entspricht, erstellt ONTAP neue Broadcast-Domains für diese Ports. Bei Bedarf können Sie die neu erstellten Broadcast-Domänen löschen, wenn alle deren Mitgliedsports zu Mitgliedsports der Interface Groups werden. Broadcast-Domänen löschen:

```
broadcast-domain delete -broadcast-domain broadcast_domain
```

f. Überprüfen Sie die Schnittstellengruppenkonfiguration und fügen Sie bei Bedarf Mitgliedsports hinzu oder löschen Sie sie.

Fügen Sie Mitgliedsports zu Schnittstellen-Gruppen-Ports hinzu:

```
ifgrp add-port -node node_name -ifgrp ifgrp_port -port port_name
```

Entfernen Sie Mitgliedsports aus Schnittstellen-Gruppen-Ports:

```
ifgrp remove-port -node node_name -ifgrp ifgrp_port -port port_name
```

g. Löschen Sie VLAN-Ports nach Bedarf und erstellen Sie sie neu. VLAN-Ports löschen:

```
vlan delete -node node_name -vlan-name vlan_port
```

VLAN-Ports erstellen:

```
vlan create -node node_name -vlan-name vlan_port
```

ⓘ Abhängig von der Komplexität der Netzwerkkonfiguration des aktualisierten Systems müssen Sie unter Umständen Teilschritte (a) bis (g) wiederholen, bis alle Ports dort richtig platziert sind, wo sie benötigt werden.

4. Wenn auf dem System keine VLANs konfiguriert sind, fahren Sie mit fort Schritt 5. Wenn VLANs konfiguriert sind, stellen Sie versetzte VLANs wieder her, die zuvor auf Ports konfiguriert wurden, die nicht mehr vorhanden sind oder auf Ports konfiguriert wurden, die in eine andere Broadcast-Domäne verschoben wurden.

a. Anzeigen der verschobenen VLANs:

```
cluster controller-replacement network displaced-vlans show
```

b. Stellen Sie die vertriebenen VLANs auf den gewünschten Zielanschluss wieder her:

```
displaced-vlans restore -node node_name -port port_name -destination-port
destination_port
```

c. Überprüfen Sie, ob alle vertriebenen VLANs wiederhergestellt wurden:

```
cluster controller-replacement network displaced-vlans show
```

d. Etwa eine Minute nach der Erstellung werden VLANs automatisch in die entsprechenden Broadcast-Domänen platziert. Überprüfen Sie, ob die wiederhergestellten VLANs in die entsprechenden Broadcast-Domänen platziert wurden:

```
network port reachability show
```

5. ab ONTAP 9.8 ändert ONTAP automatisch die Home Ports der LIFs, wenn die Ports während der Reparatur des Netzwerkports zwischen Broadcast-Domänen verschoben werden. Wenn der Home Port einer LIF auf einen anderen Knoten verschoben wurde oder nicht zugewiesen ist, wird diese LIF als vertriebene LIF dargestellt. Stellen Sie die Home-Ports der vertriebenen LIFs wieder her, deren Home-Ports nicht mehr vorhanden sind oder in einen anderen Node verschoben wurden.

a. Zeigen Sie die LIFs an, deren Home-Ports möglicherweise zu einem anderen Node verschoben oder nicht mehr vorhanden sind:

```
displaced-interface show
```

b. Stellen Sie den Home Port jeder logischen Schnittstelle wieder her:

```
displaced-interface restore -vserver Vserver_name -lif-name LIF_name
```

c. Überprüfen Sie, ob alle LIF Home Ports wiederhergestellt sind:

```
displaced-interface show
```

Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit für alle verbundenen Ports als „ok“ und den Status als „nicht-Erreichbarkeit“ für Ports ohne physische Konnektivität melden. Wenn Ports einen anderen Status als diese beiden melden, reparieren Sie die Erreichbarkeit wie in beschrieben Schritt 3.

6. überprüft, ob alle LIFs administrativ oben auf Ports liegen, die zu den richtigen Broadcast-Domänen gehören.

a. Prüfen Sie auf administrativ heruntergekommen LIFs:

```
network interface show -vserver Vserver_name -status-admin down
```

b. Prüfen Sie alle LIFs, die operativ inaktiv sind:

```
network interface show -vserver Vserver_name -status-oper down
```

c. Ändern Sie alle LIFs, die geändert werden müssen, um über einen anderen Home-Port zu verfügen:

```
network interface modify -vserver Vserver_name -lif LIF_name -home-port
home_port
```

> Für iSCSI LIFs muss die Modifikation des Home Ports die LIF administrativ heruntergefahren werden.

a. Zurücksetzen von LIFs, die nicht die Heimat ihrer jeweiligen Home-Ports sind:

```
network interface revert *
```

Verschieben Sie die NAS-Daten-LIFs von node1 auf node2 und überprüfen Sie SAN LIFs auf node3

Bevor Sie Aggregate von node2 auf node3 verschieben, müssen Sie die NAS-Daten-LIFs, die zu node1 gehören, verschieben, die sich zurzeit in node2 von node2 nach node3 befinden. Sie müssen außerdem die SAN-LIFs auf node3 überprüfen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Listen Sie alle NAS-Daten-LIFs auf, die nicht im Besitz von node2 sind, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe erfassen:

   ```
   network interface show -role data -curr-node node2 -is-home false -home-node
   node3
   ```

2. Wenn das Cluster für SAN-LIFs konfiguriert ist, notieren Sie die SAN-LIFs `adapter` Und `switch-port` Konfigurationsinformationen in diesem "Arbeitsblatt" Zur späteren Verwendung im Verfahren.

   a. Führen Sie die SAN-LIFs auf node2 auf und untersuchen Sie die Ausgabe:

   ```
   network interface show -data-protocol fc*
   ```

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------  ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Führen Sie die vorhandenen Konfigurationen auf und untersuchen Sie die Ausgabe:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Nehmen Sie eine der folgenden Aktionen:

Falls Knoten 1…	Dann…
Schnittstellengruppen oder VLANs wurden konfiguriert	Gehen Sie zu Schritt 4.
Schnittstellengruppen oder VLANs waren nicht konfiguriert	Überspringen Sie Schritt 4, und fahren Sie mit fort Schritt 5.

4. führen Sie die folgenden Teilschritte durch, um alle auf Schnittstellengruppen und VLANs gehosteten NAS-Daten-LIFs zu migrieren, die sich ursprünglich auf node1 von node2 auf node3 befanden:

   a. Migrieren Sie alle auf node2 gehosteten Daten-LIFs, die zuvor zu node1 auf einer Schnittstellengruppe gehörten, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

   ```
   network interface migrate -vserver vserver_name -lif LIF_name -destination
   -node node3 -destination-port netport|ifgrp
   ```

   b. Ändern Sie den Home-Port und den Home-Node der LIF in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node3 -home-port netport|ifgrp
   ```

   c. Migrieren Sie alle auf node2 gehosteten Daten-LIFs, die zuvor zu node1 auf einem VLAN-Port gehörten, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem

Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node3 -home-port netport|ifgrp
```

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 6 Und Schritt 7, überspringen Sie Schritt 8, und abgeschlossen Schritt 9 Bis Schritt 12.
San	Deaktivieren Sie alle SAN-LIFs auf dem Node, um sie für das Upgrade herunterzufahren: `network interface modify -vserver *vserver_name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

6. Wenn Datenports auf Ihren Plattformen nicht identisch sind, fügen Sie die Ports zur Broadcast-Domäne hinzu:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „8200-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain „Management“ im IPspace „Standard“ hinzu:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 8200-1:e0a, 8060-1:e0i
```

7. Migrieren Sie jede NAS-Daten-LIF auf node3, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

8. stellen Sie sicher, dass die Datenmigration persistent ist:

```
network interface modify -vserver vserver_name -lif LIF_name-home-port
netport|ifgrp -home-node node3
```

9. Bestätigen, dass sich die SAN-LIFs auf den richtigen Ports auf node3 befinden:

a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

```
network interface show -data-protocol iscsi|fcp -home-node node3
```

Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node
Port     Home
 -----------  ----------  ----------  ------------------
-------------  -------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node3
a0a      true
              data1       up/up       10.63.0.50/18       node3
e0c      true
              rads1       up/up       10.63.0.51/18       node3
e1a      true
              rads2       up/down     10.63.0.52/24       node3
e1b      true
 vs1
              lif1        up/up       172.17.176.120/24   node3
e0c      true
              lif2        up/up       172.17.176.121/24   node3
e1a      true
```

b. Überprüfen Sie das neue und `adapter` Und `switch-port` Die Konfigurationen sind korrekt, indem die Ausgabe von dem verglichen wird `fcp adapter show` Befehl mit den Konfigurationsinformationen, die Sie im Arbeitsblatt in aufgezeichnet haben Schritt 2.

Liste der neuen SAN LIF-Konfigurationen auf Knoten3:

```
fcp adapter show -fields switch-port,fc-wwpn
```

Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node        adapter fc-wwpn                 switch-port
----------- ------- ----------------------- -------------
cluster1-01 0a      50:0a:09:82:9c:13:38:00 ACME Switch:0
cluster1-01 0b      50:0a:09:82:9c:13:38:01 ACME Switch:1
cluster1-01 0c      50:0a:09:82:9c:13:38:02 ACME Switch:2
cluster1-01 0d      50:0a:09:82:9c:13:38:03 ACME Switch:3
cluster1-01 0e      50:0a:09:82:9c:13:38:04 ACME Switch:4
cluster1-01 0f      50:0a:09:82:9c:13:38:05 ACME Switch:5
cluster1-01 1a      50:0a:09:82:9c:13:38:06 ACME Switch:6
cluster1-01 1b      50:0a:09:82:9c:13:38:07 ACME Switch:7
cluster1-02 0a      50:0a:09:82:9c:6c:36:00 ACME Switch:0
cluster1-02 0b      50:0a:09:82:9c:6c:36:01 ACME Switch:1
cluster1-02 0c      50:0a:09:82:9c:6c:36:02 ACME Switch:2
cluster1-02 0d      50:0a:09:82:9c:6c:36:03 ACME Switch:3
cluster1-02 0e      50:0a:09:82:9c:6c:36:04 ACME Switch:4
cluster1-02 0f      50:0a:09:82:9c:6c:36:05 ACME Switch:5
cluster1-02 1a      50:0a:09:82:9c:6c:36:06 ACME Switch:6
cluster1-02 1b      50:0a:09:82:9c:6c:36:07 ACME Switch:7
16 entries were displayed
```

Wenn sich ein SAN LIF in der neuen Konfiguration nicht auf einem Adapter befindet, der noch an denselben angeschlossen ist `switch-port`, Es kann zu einem Systemausfall führen, wenn Sie den Node neu booten.

c. Wenn node3 irgendwelche SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der nicht in node1 vorhanden war oder einem anderen Port zugeordnet werden muss, verschieben Sie sie zu einem geeigneten Port auf node3, indem Sie die folgenden Teilschritte ausführen:

   i. Legen Sie den LIF-Status auf „down“ fest:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status -admin down`

   ii. Entfernen Sie das LIF aus dem Portsatz:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Geben Sie einen der folgenden Befehle ein:

      - Verschieben eines einzelnen LIF:

        `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home -port` *`new_home_port`*

      - Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen

neuen Port:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

> Sie müssen SAN-LIFs zu einem Port verschieben, der die gleiche Verbindungsgeschwindigkeit wie der ursprüngliche Port hat.

10. Ändern Sie den Status aller LIFs auf „up“, damit die LIFs den Datenverkehr auf dem Node akzeptieren und senden können:

```
network interface modify -home-port port_name -home-node node3 -lif data
-status-admin up
```

11. Geben Sie an jedem Node den folgenden Befehl ein, und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs an die richtigen Ports verschoben wurden und ob die LIFs den Status von „up“ aufweisen. Geben Sie dazu den folgenden Befehl an einem der Nodes ein und überprüfen Sie die Ausgabe:

```
network interface show -home-node node3 -role data
```

12. Wenn eine der LIFs nicht verfügbar ist, setzen Sie den Administrationsstatus der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

13. Senden Sie eine AutoSupport Nachricht nach dem Upgrade an NetApp für den Knoten1:

```
system node autosupport invoke -node node3 -type all -message "node1
successfully upgraded from platform_old to platform_new"
```

Arbeitsblatt: Informationen, die aufgezeichnet werden sollen, bevor NAS-Daten-LIFs in node3 verschoben werden

Um zu überprüfen, ob Sie die richtige Konfiguration haben, nachdem Sie SAN LIFs von node2 auf node3 verschoben haben, können Sie das folgende Arbeitsblatt verwenden, um die aufzuzeichnen `adapter` Und `switch-port` Informationen für jedes LIF.

Notieren Sie das LIF `adapter` Informationen aus dem `network interface show -data-protocol fc*` Befehlsausgabe und das `switch-port` Informationen aus dem `fcp adapter show -fields switch-port,fc-wwpn` Befehlsausgabe für node2.

Notieren Sie nach Abschluss der Migration zu node3 die LIF `adapter` Und `switch-port` Informationen für die LIFs auf Knoten 3 und überprüfen Sie, dass jede LIF noch mit derselben verbunden ist `switch-port`.

Knoten 2			Node3		
LIF	adapter	switch-port	LIF	adapter	switch-port

Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3

Bevor Sie node2 durch node4 ersetzen können, müssen Sie eine AutoSupport-Nachricht für node2 senden und dann die nicht-Root-Aggregate verschieben, die im Besitz von node2 sind, in node3.

Schritte

1. Senden Sie eine AutoSupport-Nachricht an NetApp für node2:

   `system node autosupport invoke -node` *`node2`* `-type all -message "Upgrading` *`node2`* `from` *`platform_old`* `to` *`platform_new`*`"`

2. Überprüfen Sie, ob die AutoSupport Meldung gesendet wurde:

   `system node autosupport show -node` *`node2`* `-instance`

   Die Felder „Letzter Betreff gesendet:“ und „Letzter Zeitpunkt gesendet:“ enthalten den Nachrichtentitel der letzten gesendeten Nachricht und den Zeitpunkt, zu dem die Nachricht gesendet wurde.

3. Verschiebung der nicht-Root-Aggregate:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Listen Sie die Aggregate auf, die Eigentum von node2 sind:

      `storage aggregate show -owner-name` *`node2`*

   c. Starten Sie die Aggregatverschiebung:

      `storage aggregate relocation start -node` *`node2`* `-destination` *`node3`* `-aggregate -list * -ndo-controller-upgrade true`

      Der Befehl sucht nur Aggregate außerhalb des Root-Bereichs.

   a. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge finden im Hintergrund statt. Für die Verschiebung eines Aggregats kann dieser Zeitraum von

wenigen Sekunden bis hin zu einigen Minuten dauern. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

4. Überprüfen Sie den Versetzungsstatus von node2:

```
storage aggregate relocation show -node node2
```

Die Ausgabe zeigt „Fertig“ für ein Aggregat an, nachdem es verschoben wurde.

Sie müssen warten, bis alle Aggregate, die sich im Besitz von node2 befinden, in node3 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

5. Führen Sie eine der folgenden Aktionen durch:

Bei Umzug von…	Dann…
Alle Aggregate waren erfolgreich	Gehen Sie zu Schritt 6.

Bei Umzug von…	Dann…

Aggregate sind ausgefallen oder sie wurden Vetos	a. Detaillierte Statusmeldung anzeigen:
	`storage aggregate show -instance`
	Sie können auch die EMS-Protokolle überprüfen, um die erforderlichen Korrekturmaßnahmen anzuzeigen.
	Der `event log show` Befehl listet alle Fehler auf, die aufgetreten sind.
	b. Führen Sie die Korrekturmaßnahme durch.
	c. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	d. Verschiebung ausgefallener oder Vetos von Aggregaten:
	`storage aggregate relocation start -node node2 -destination node3 -aggregate-list * -ndo -controllerupgrade true`
	e. Geben Sie bei der entsprechenden Aufforderung ein `y`.
	f. Zurück zur Administratorberechtigungsebene:
	`set -privilege admin`
	Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen:
	• Durch Überschreiben von Veto-Prüfungen:
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	• Durch Überschreiben von Zielprüfungen:
	`storage aggregate relocation start -override -destination-checks true -ndocontroller-upgrade`
	Weitere Informationen zu den Befehlen für die Verschiebung des Storage-Aggregats finden Sie unter "Quellen" Verbinden mit *Disk und Aggregat-Management mit den Befehlen CLI* und *ONTAP 9: Manual Page Reference*.

6. Stellen Sie sicher, dass alle nicht-Root-Aggregate online sind auf node3:

`storage aggregate show -node node3 -state offline -root false`

Wenn irgendwelche Aggregate offline gegangen sind oder fremd geworden sind, müssen Sie sie online

bringen, einmal für jedes Aggregat:

`storage aggregate online -aggregate aggr_name`

7. Vergewissern Sie sich, dass alle Volumes auf node3 online sind:

   `volume show -node node3 -state offline`

   Wenn Volumes auf Knoten3 offline sind, müssen Sie sie einmal für jedes Volume online bringen:

   `volume online -vserver Vserver-name -volume volume-name`

8. Vergewissern Sie sich, dass node2 keine Online-Aggregate besitzt, die nicht im Root-Modus sind:

   `storage aggregate show -owner-name node2 -ha-policy sfo -state online`

   Die Befehlsausgabe sollte nicht online nicht-Root-Aggregate anzeigen, da alle nicht-Root-Online-Aggregate bereits in node3 verschoben wurden.

Verschieben Sie die NAS-Daten-LIFs von node2 auf node3

Nachdem Sie die Aggregate von node2 auf node3 verschoben haben, müssen Sie die NAS-Daten-LIFs von node2 auf node3 verschieben.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie müssen überprüfen, ob die LIFs sich in den entsprechenden Ports befinden, nachdem Sie die LIFs von node3 nach node4 verschoben und node4 in den Online-Modus versetzt haben.

Schritte

1. Listen Sie alle NAS-Daten-LIFs auf, die sich im Besitz von node2 befinden, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe erfassen:

   `network interface show -data-protocol nfs|cifs -home-node node2`

   Im folgenden Beispiel wird die Befehlsausgabe für „node2“ gezeigt:

```
cluster::> network interface show -data-protocol nfs|cifs -home-node
node2
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node     Port
Home
 -----------  ----------  ----------  ------------------  -------
-------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node2    a0a
true
              data1       up/up       10.63.0.50/18       node2    e0c
true
              rads1       up/up       10.63.0.51/18       node2    e1a
true
              rads2       up/down     10.63.0.52/24       node2    e1b
true
 vs1
              lif1        up/up       172.17.176.120/24   node2    e0c
true
              lif2        up/up       172.17.176.121/24   node2    e1a
true
```

2. Nehmen Sie eine der folgenden Aktionen:

Falls Knoten 2…	Dann…
Schnittstellengruppen oder VLANs sind konfiguriert	Gehen Sie zu Schritt 3.
Schnittstellengruppen oder VLANs sind nicht konfiguriert	Überspringen Sie Schritt 3, und fahren Sie mit fort Schritt 4.

3. Nehmen Sie die folgenden Schritte durch, um die auf Schnittstellengruppen und VLANs auf node2 gehosteten NAS-Daten-LIFs zu migrieren:

   a. Migrieren Sie alle Daten-LIFs, die auf einer Schnittstellengruppe auf node2 gehostet werden, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

      `network interface migrate -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node3`* `-destination-port` *`netport|ifgrp`*

   b. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt A Um den Port und Node, der derzeit die LIFs hostet, geben Sie einmal für jeden Node den folgenden Befehl ein:

      `network interface modify -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node3`* `-homeport` *`netport|ifgrp`*

c. Migrieren Sie alle auf VLANs gehosteten LIFs auf node2 zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk wie die des VLANs zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -home-node
node3 -homeport netport|ifgrp
```

4. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 5 Bis Schritt 8.
San	Überspringen Sie Schritt 5 bis Schritt 8 und schließen Sie dann ab Schritt 9.
Sowohl NAS als auch SAN	Vollständig Schritt 5 Bis Schritt 9.

5. Wenn auf Ihren Plattformen nicht dieselben Daten-Ports vorhanden sind, fügen Sie die Ports der Broadcast-Domäne hinzu:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „6280-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain „Management“ im IPspace „Standard“ hinzu:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
           -broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

6. Migrieren Sie jede NAS-Daten-LIF auf node3 durch Eingabe des folgenden Befehls, einmal für jede LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

7. Überprüfen Sie, ob NAS-LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von „up“ haben, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network interface show -curr-node node3 -data-protocol cifs|nfs
```

8. Wenn eine der LIFs nicht verfügbar ist, setzen Sie den administrativen Status der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -status-admin up
```

9. Wenn Schnittstellengruppen oder VLANs konfiguriert sind, führen Sie die folgenden Teilschritte aus:

   a. Entfernen Sie die VLANs aus den Schnittstellengruppen:

      `network port vlan delete -node node_name -port ifgrp -vlan-id VLAN_ID`

   b. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu ermitteln, ob Schnittstellengruppen auf dem Node konfiguriert sind:

      `network port ifgrp show -node node_name -ifgrp ifgrp_name -instance`

      Das System zeigt Schnittstellengruppeninformationen für den Node an, wie im folgenden Beispiel gezeigt:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node2
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: MAC_address
    ort Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

   a. Wenn auf dem Node Schnittstellengruppen konfiguriert sind, notieren Sie die Namen der Interface Groups und der ihnen zugewiesenen Ports. Löschen Sie dann die Ports, indem Sie den folgenden Befehl eingeben, jeweils ein für jeden Port:

      `network port ifgrp remove-port -node node_name -ifgrp ifgrp_name -port port_name`

Phase 4: Notieren Sie Informationen und entfernen Sie node2

Phase-4-Übersicht

Während der Phase 4 notieren Sie node2 Informationen, die später im Verfahren verwendet werden sollen, und setzen dann node2 aus.

Schritte

1. "Node2-Informationen aufzeichnen"
2. "Node2 ausmustern"

Node2-Informationen aufzeichnen

Bevor Sie node2 herunterfahren und außer Betrieb nehmen können, müssen Sie Informationen über das Cluster-Netzwerk, die Management- und FC-Ports sowie seine NVRAM-System-ID aufzeichnen. Sie benötigen diese Informationen später im Verfahren,

wenn Sie node2 node4 zuordnen und Festplatten neu zuweisen.

Schritte

1. Ermitteln Sie die Cluster-Netzwerk-, Node-Management-, Cluster- und Cluster-Management-Ports auf node2:

   `network interface show -curr-node node_name -role cluster,intercluster,nodemgmt,cluster-mgmt`

   Das System zeigt die LIFs für diesen Node und andere Nodes im Cluster an, wie im folgenden Beispiel dargestellt:

```
cluster::> network interface show -curr-node node2 -role
cluster,intercluster,node-mgmt,cluster-mgmt
         Logical     Status     Network            Current     Current
Is
Vserver  Interface   Admin/Oper Address/Mask       Node        Port
Home
-------- ----------  ---------- ------------------ ----------  -------
----
node2
         intercluster up/up     192.168.1.202/24   node2       e0e
true
         clus1        up/up     169.254.xx.xx/24   node2       e0a
true
         clus2        up/up     169.254.xx.xx/24   node2       e0b
true
         mgmt1        up/up     192.168.0.xxx/24   node2       e0c
true
4 entries were displayed.
```

   > Das System verfügt möglicherweise über keine Intercluster-LIFs. Sie erhalten eine Cluster-Management-LIF nur auf einem Node eines Node-Paars. Eine LIF zum Cluster-Management wird in der Beispielausgabe von angezeigt "Schritt 1" In *Port-Informationen für Node1 aufzeichnen*.

2. Erfassen Sie die Informationen in der Ausgabe, die im Abschnitt verwendet werden sollen "Weisen Sie Ports von node2 nach node4 zu".

   Die Ausgabeinformationen sind erforderlich, um die neuen Controller-Ports den alten Controller-Ports zuzuordnen.

3. Physische Ports auf node2 bestimmen:

   `network port show -node node_name -type physical +`

   node_name Ist der Node, der migriert wird.

   Das System zeigt die physischen Ports auf node2 an, wie im folgenden Beispiel dargestellt:

```
cluster::> network port show -node node2 -type physical

                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node2
       e0M       Default      IP_address       up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

4. Notieren Sie die Ports und ihre Broadcast-Domänen.

   Die Broadcast-Domänen müssen später im Verfahren den Ports auf dem neuen Controller zugeordnet werden.

5. Bestimmen Sie die FC-Ports auf node2:

   `network fcp adapter show`

   Das System zeigt die FC-Ports auf dem node2 an, wie im folgenden Beispiel dargestellt:

```
cluster::> network fcp adapter show -node node2
                     Connection  Host
Node         Adapter Established Port Address
------------ ------- ----------- ------------
node2
             0a      ptp         11400
node2
             0c      ptp         11700
node2
             6a      loop        0
node2
             6b      loop        0
4 entries were displayed.
```

6. Notieren Sie die Ports.

   Die Ausgabeinformationen sind erforderlich, um die neuen FC-Ports auf dem neuen Controller später im Verfahren zuzuordnen.

7. Falls Sie dies zuvor noch nicht getan haben, überprüfen Sie, ob auf node2 Schnittstellengruppen oder VLANs konfiguriert sind:

```
ifgrp show

vlan show
```

Sie verwenden die Informationen im Abschnitt "Weisen Sie Ports von node2 nach node4 zu".

8. Führen Sie eine der folgenden Aktionen durch:

Sie suchen…	Dann…
Die NVRAM-System-ID-Nummer in wurde aufgezeichnet "Bereiten Sie die Knoten für ein Upgrade vor"	Gehen Sie zu "Node2 ausmustern".
Die NVRAM-System-ID-Nummer in wurde nicht aufgezeichnet "Bereiten Sie die Knoten für ein Upgrade vor"	Vollständig Schritt 9 Und Schritt 10 Und fahren Sie dann mit dem nächsten Abschnitt fort, "Node2 ausmustern".

9. die Attribute von node2 anzeigen:

```
system node show -instance -node node2
```

```
cluster::> system node show -instance -node node2
                                ...
                    NVRAM System ID: system_ID
                                ...
```

10. notieren Sie die im Abschnitt zu verwendende NVRAM-System-ID "installieren und booten sie node4".

Node2 ausmustern

Um node2 auszumustern, müssen Sie node2 richtig abschalten und aus dem Rack oder Gehäuse entfernen. Wenn sich das Cluster in einer SAN-Umgebung befindet, müssen Sie auch die SAN-LIFs löschen.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Falls das Cluster…	Dann…
Eines Clusters mit zwei Nodes	Gehen Sie zu Schritt 2.
Ein Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 9.

2. Zugriff auf die erweiterte Berechtigungsebene durch Eingabe des folgenden Befehls auf einem der beiden Knoten:

```
set -privilege advanced
```

3. Überprüfen Sie, ob die Cluster-HA deaktiviert wurde, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
cluster ha show
```

Vom System wird die folgende Meldung angezeigt:

```
High Availability Configured: false
```

4. Überprüfen Sie, ob node2 aktuell epsilon hält, indem Sie den folgenden Befehl eingeben und die Ausgabe prüfen:

```
cluster show
```

Das folgende Beispiel zeigt, dass auf node2 Epsilon steht:

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

Warning: Cluster HA has not been configured. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

2 entries were displayed.
```

> Wenn Sie ein HA-Paar in einem Cluster mit mehreren HA-Paaren aktualisieren, müssen Sie Epsilon auf den Node eines HA-Paars verschieben, ohne ein Controller-Upgrade durchführen zu müssen. Wenn Sie beispielsweise nodeA/nodeB in einem Cluster mit der HA-Paar-Konfiguration nodeA/nodeB und nodeC/nodded aktualisieren, müssen Sie Epsilon auf nodeC oder nodded verschieben.

5. Wenn das Epsilon auf node2 hält, markieren Sie Epsilon als `false` Auf dem Node, sodass er auf node3 übertragen werden kann:

```
cluster modify -node node2 -epsilon false
```

6. Übertragen Sie das Epsilon auf node3, indem Sie epsilon markieren `true` Auf Knoten 3:

```
cluster modify -node node3 -epsilon true
```

7. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

8. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

   `network options switchless-cluster show`

   ```
   cluster::*> network options switchless-cluster show
   Enable Switchless Cluster: false/true
   ```

   Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

9. Zurück zur Administratorebene:

   `set -privilege admin`

10. Stoppen Sie node2, indem Sie auf beiden Controllern den folgenden Befehl eingeben:
    `system node halt -node node2`
11. Nachdem der Knoten 2 vollständig heruntergefahren wurde, entfernen Sie ihn aus dem Gehäuse oder Rack. Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5: installieren und booten sie node4

Phase-5-Übersicht

In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 bis node4 zu und verschieben Daten-LIFs und SAN-LIFs, die zu node2 von node3 nach node4 gehören. Außerdem werden node2-Aggregate von Node3 nach node4 verschoben.

Schritte

1. "installieren und booten sie node4"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest"
3. "Weisen Sie Ports von node2 nach node4 zu"
4. "Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4"
5. "Verschiebung von nicht-Root-Aggregaten node2 von Node3 in node4"

installieren und booten sie node4

sie müssen node4 im Rack installieren, Node2-Verbindungen zu node4 übertragen und node4 booten. Sie müssen auch node2-Spares, alle Festplatten der Root-Partition und alle nicht-Root-Aggregate neu zuweisen, die nicht zu node3 früher verschoben wurden.

Über diese Aufgabe

Sie müssen node4 als Netzboot fahren, wenn nicht die gleiche Version von ONTAP 9 auf node2 installiert ist. Nachdem sie node4 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für den späteren Systemstart herunterladen, indem Sie den Anweisungen unter folgen "Vorbereitungen für den Netzboot"

Sie sind jedoch nicht verpflichtet, Netboot node4 zu starten, wenn es die gleiche oder eine höhere Version von ONTAP 9 hat, die auf node2 installiert ist.

- Wichtige Informationen:*
- Wenn Sie ein V-Series System oder ein System mit mit mit FlexArray Virtualisierungssoftware aktualisieren, die mit Storage-Arrays verbunden ist, müssen Sie diese vollständig ausführen Schritt 1 Bis Schritt 7, Lassen Sie diesen Abschnitt bei Schritt 8 Und befolgen Sie die Anweisungen unter "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Geben Sie bei Bedarf die Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und den Vorgang unter fortsetzen Schritt 9.
- Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und dann mit dem Abschnitt fortfahren "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. Nehmen Sie eine der folgenden Aktionen:

Wenn node4 wird in …	Dann…
Ein von Knoten 3 getrenntes Chassis	Gehen Sie zu Schritt 2.
Im gleichen Chassis mit Knoten3	Überspringen Sie die Schritte 2 und 3 und gehen Sie zu Schritt 4.

2. stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt.

   Wenn node4 sich in einem separaten Chassis von node3 befindet, können sie node4 an der gleichen Stelle wie node2 platzieren. Wenn sich Node3 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

3. installieren sie node4 im Rack gemäß den Anweisungen in der Anleitung *Installation and Setup Instructions* für das Node-Modell.
4. kabelnode4, die Verbindungen von node2 nach node4 verschieben.

   Die folgenden Referenzen helfen Ihnen dabei, geeignete Kabelverbindungen zu machen. Gehen Sie zu "Quellen" Um eine Verbindung zu ihnen zu machen.

   - *Installations- und Setup-Anleitung* oder *Installationsanforderungen für die FlexArray-Virtualisierung und Referenz* für die node4-Plattform
   - Das entsprechende Verfahren für das Festplatten-Shelf
   - Die Dokumentation *High Availability Management*

     Folgende Anschlüsse verkabeln:

   - Konsole (Remote-Management-Port)
   - Cluster-Ports

- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Sie müssen die Interconnect-Karte/FC_VI-Karte oder den Interconnect/FC_VI-Kabelanschluss von node2 auf node4 nicht verschieben, da die meisten Plattformmodelle über einzigartige Interconnect-Kartenmodelle verfügen.

5. Führen Sie eine der folgenden Aktionen durch:

Wenn node4 in…	Dann…
Im gleichen Chassis wie bei Node3	Gehen Sie zu Schritt 8.
Ein von Knoten 3 getrenntes Chassis	Gehen Sie zu Schritt 6.

6. Schalten Sie die Stromversorgung zu node4 ein, und unterbrechen Sie dann den Start, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Startumgebung zuzugreifen.

> Wenn Sie node4 booten, wird möglicherweise die folgende Meldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power
         outage. This is likely because the battery is
         discharged but could be due to other temporary
         conditions.
         When the battery is ready, the boot process will
         complete and services will be engaged.
         To override this delay, press 'c' followed by 'Enter'
```

7. Wenn die Warnmeldung in Schritt 6 angezeigt wird, führen Sie die folgenden Schritte aus:
   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.
   b. Lassen Sie den Akku laden und den Bootvorgang beenden.

> **Warnung: Die Verzögerung nicht außer Kraft setzen. Wenn der Akku nicht geladen werden kann, kann dies zu einem Datenverlust führen.**

8. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Überspringen Sie Schritt 9 bis Schritt 14, und fahren Sie mit fort Schritt 15.

Wenn Ihr System…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	a. Gehen Sie zum Abschnitt „ FC- oder UTA/UTA2-Konfiguration auf node4_“ und füllen Sie die Abschnitte aus "Konfigurieren Sie FC-Ports auf node4" Und "UTA/UTA2-Ports auf node4 prüfen und konfigurieren", Je nach Ihrem System. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 9. Vor dem Booten von ONTAP auf dem V-Series System müssen Sie die integrierten FC-Ports, UTA/UTA2-Ports und UTA/UTA2-Karten neu konfigurieren.

9. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

   Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

10. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

11. Ändern Sie die WWPN-Werte (World Wide Port Name) in den Host- oder Volume-Gruppen, die Array-LUNs auf dem Speicher-Array zugeordnet sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

12. Wenn die Konfiguration das Switch-basierte Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
13. Überprüfen Sie, ob die Array-LUNs nun für node4 sichtbar sind, indem Sie den folgenden Befehl eingeben und seine Ausgabe prüfen:

    ```
    sysconfig -v
    ```

    Das System zeigt alle Array-LUNs an, die für jeden FC-Initiator-Port sichtbar sind. Wenn die Array-LUNs nicht sichtbar sind, können Sie Festplatten von node2 nicht später in diesem Abschnitt neu zuweisen.

14. Drücken Sie Strg-C, um das Startmenü anzuzeigen, und wählen Sie Wartungsmodus aus.
15. Geben Sie in der Eingabeaufforderung für den Wartungsmodus den folgenden Befehl ein:

    ```
    halt
    ```

    Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

16. node4 für ONTAP konfigurieren:

    ```
    set-defaults
    ```

17. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.

Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option `(10) Set Onboard Key Manager recovery secrets`.

Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe "Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager".

18. Wenn die auf node4 installierte ONTAP-Version gleich oder höher als die auf node2 installierte Version von ONTAP 9 ist, geben Sie den folgenden Befehl ein:

```
boot_ontap menu
```

19. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Verfügt nicht über die richtige oder aktuelle ONTAP-Version unter node4	Gehen Sie zu Schritt 20.
Hat die richtige oder aktuelle Version von ONTAP auf node4	Gehen Sie zu Schritt 25.

20. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

Sie müssen den Management-Port und die IP-Adresse als Netzboot-Verbindung verwenden. Verwenden Sie keine LIF-IP-Adresse von Daten, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=`*`filer_addr`* `mask=`*`netmask`* `-gw=`*`gateway`* `dns=`*`dns_addr`* `domain=`*`dns_domain`* *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

21. Ausführen eines Netzboots auf node4:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_webaccessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_webaccessible_directory/ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In "Schritt 1" Im Abschnitt *Vorbereiten für Netzboot*.

Unterbrechen Sie den Startvorgang nicht.

22. Wählen Sie im Startmenü die Option `option (7) Install new software first`.

Mit dieser Menüoption wird das neue Data 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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der Data ONTAP und keine Upgrades von Controllern.

> 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 Versionen von ONTAP. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

23. [[man_install4_steep23] Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie y ein. Geben Sie dann die URL ein, wenn Sie nach dem Paket gefragt werden:

    ```
    http://<web_server_ip/path_to_web-
    accessible_directory/ontap_version>_image.tgz
    ```

24. Führen Sie die folgenden Teilschritte durch:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

25. Wählen Sie den Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
26. bevor Sie fortfahren, fahren Sie mit fort "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Um alle erforderlichen Änderungen an den FC- oder UTA/UTA2-Ports auf dem Node vorzunehmen. Nehmen Sie die in diesen Abschnitten empfohlenen Änderungen vor, starten Sie den Node neu, und wechseln Sie in den Wartungsmodus.
27. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe, um die System-ID von node4 zu finden:

    ```
    disk show -a
    ```

    Das System zeigt die System-ID des Node sowie Informationen über seine Festplatten an, wie im folgenden Beispiel dargestellt:

```
*> disk show -a
Local System ID: 536881109
DISK         OWNER                      POOL   SERIAL NUMBER   HOME
------------ -------------              -----  -------------
-------------
0b.02.23     nst-fas2520-2(536880939)   Pool0  KPG2RK6F        nst-
fas2520-2(536880939)
0b.02.13     nst-fas2520-2(536880939)   Pool0  KPG3DE4F        nst-
fas2520-2(536880939)
0b.01.13     nst-fas2520-2(536880939)   Pool0  PPG4KLAA        nst-
fas2520-2(536880939)
......
0a.00.0                   (536881109)   Pool0  YFKSX6JG
(536881109)
......
```

28. Weisen Sie node2 Ersatzteile, Festplatten, die zur Root gehören, und alle nicht-Root-Aggregate erneut zu, die im Abschnitt früher nicht in node3 verschoben wurden "Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3":

> Wenn Sie auf Ihrem System freigegebene Festplatten, Hybrid-Aggregate oder beides haben, müssen Sie die korrekte verwenden `disk reassign` Befehl aus der folgenden Tabelle.

Festplattentyp…	Führen Sie den Befehl aus…
Mit gemeinsamen Festplatten	`disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`* `-p` *`node3_sysid`*
Ohne Shared-Ressourcen	`disks disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`*

Für das `<node2_sysid>` Wert: Verwenden Sie die in erfassten Informationen "Schritt 10" Des Abschnitts *Record node2 information*. Für `*node4_sysid*`Verwenden Sie die Informationen, die in erfasst werden Schritt 23.

> Der `-p` Die Option ist nur im Wartungsmodus erforderlich, wenn freigegebene Festplatten vorhanden sind.

Der `disk reassign` Befehl weist nur die Festplatten zu, für die es erforderlich ist *`node2_sysid`* Ist der aktuelle Eigentümer.

Vom System wird die folgende Meldung angezeigt:

```
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
```

Eingabe `n` Wenn Sie aufgefordert werden, die Neuzuweisung der Festplatte abzubrechen.

Wenn Sie aufgefordert werden, die Neuzuweisung der Festplatte abzubrechen, müssen Sie eine Reihe von Eingabeaufforderungen beantworten, wie in den folgenden Schritten dargestellt:

a. Vom System wird die folgende Meldung angezeigt:

```
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
```

b. Eingabe `y` Um fortzufahren.

Vom System wird die folgende Meldung angezeigt:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)? y
```

a. Eingabe `y` Um die Aktualisierung der Festplatteneigentümer zu ermöglichen.

29. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. A800-Systeme), setzen sie node4 als root, um zu bestätigen, dass es aus dem Root-Aggregat von node2 startet.

> **Warnung: Sie müssen die folgenden Teilschritte in der angegebenen Reihenfolge durchführen; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.**

Mit dem folgenden Verfahren wird node4 vom Root-Aggregat von node2 gestartet:

a. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node2 Aggregat:

```
aggr status -r
```

b. Prüfen Sie den Gesamtstatus des node2-Aggregats:

```
aggr status
```

c. Bei Bedarf das node2 Aggregat online bringen:

```
aggr_online root_aggr_from_node2
```

d. Verhindern Sie, dass das node4 aus dem ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node4
```

e. Legen Sie das node2-Root-Aggregat als das neue Root-Aggregat für node4 fest:

```
aggr options aggr_from_node2 root
```

30. Vergewissern Sie sich, dass Controller und Chassis als konfiguriert sind `ha` Indem Sie den folgenden Befehl eingeben und die Ausgabe beobachten:

```
ha-config show
```

Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

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

Systeme zeichnen in EINEM PROM auf, ob sie in einem HA-Paar oder einer Standalone-Konfiguration sind. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

```
ha-config modify controller ha

ha-config modify chassis ha.
```

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

```
ha-config modify controller mcc

ha-config modify chassis mcc.
```

31. Löschen Sie die Mailboxen auf node4:

```
mailbox destroy local
```

32. Beenden des Wartungsmodus:

```
halt
```

Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

33. Überprüfen Sie in Knoten 3 das Systemdatum, die Uhrzeit und die Zeitzone:

```
date
```

34. Prüfen Sie am node4 das Datum an der Eingabeaufforderung für die Boot-Umgebung:

    `show date`

35. Legen Sie bei Bedarf das Datum auf node4 fest:

    `set date mm/dd/yyyy`

36. Prüfen Sie auf node4 die Zeit an der Eingabeaufforderung der Boot-Umgebung:

    `show time`

37. Stellen Sie bei Bedarf die Uhrzeit auf node4 ein:

    `set time hh:mm:ss`

38. Überprüfen Sie, ob die Partner-System-ID korrekt festgelegt ist, wie in beschrieben Schritt 26 Unter Option.

    `printenv partner-sysid`

39. Legen Sie bei Bedarf die Partner System-ID auf node4 fest:

    `setenv partner-sysid node3_sysid`

    a. Einstellungen speichern:

       `saveenv`

40. Rufen Sie das Boot-Menü an der Eingabeaufforderung der Boot-Umgebung auf:

    `boot_ontap menu`

41. Wählen Sie im Startmenü die Option **(6) Flash von Backup config** aktualisieren, indem Sie eingeben `6` An der Eingabeaufforderung.

    Vom System wird die folgende Meldung angezeigt:

    ```
    This will replace all flash-based configuration with the last backup to
    disks. Are you sure you want to continue?:
    ```

42. Eingabe `y` An der Eingabeaufforderung.

    Der Startvorgang läuft normal weiter, und das System fordert Sie auf, die Unstimmigkeit der System-ID zu bestätigen.

    > Das System wird möglicherweise zweimal neu gestartet, bevor die Warnmeldung zur Nichtübereinstimmung angezeigt wird.

43. Bestätigen Sie die Diskrepanz. Der Node kann vor dem normalen Booten eine Runde des Neubootens abschließen.
44. Melden Sie sich bei node4 an.

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest

Wenn node4 über integrierte FC-Ports, integrierte Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte verfügt, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschluss abschließen Konfigurieren Sie FC-Ports auf node4, Das UTA/UTA2-Ports auf node4 prüfen und konfigurieren, Oder beide Abschnitte.

Wenn node4 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie weiter gehen "Weisen Sie Ports von node2 nach node4 zu".

Wenn Sie jedoch ein V-Series System oder FlexArray-Virtualisierungssoftware haben und mit Storage-Arrays verbunden sind und node4 keine integrierten FC-Ports, Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie zum Abschnitt *Installation and Boot node4* zurückkehren und wieder aufnehmen "Schritt 9". stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt. Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node4
- UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node4

Wenn node4 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in den Dienst stellen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node2 haben, die Sie im Abschnitt gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder einen UTA/UTA2-Adapter verfügt, konfigurieren Sie sie in UTA/UTA2-Ports auf node4 prüfen und konfigurieren.

> Wenn im System Storage-Festplatten vorhanden sind, müssen Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle eingeben. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware haben, die mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Gehen Sie zu Schritt 5.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 2.

2. Zugriff auf den Wartungsmodus:

```
boot_ontap maint
```

3. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

4. Vergleichen Sie die FC-Einstellungen auf den neuen Nodes mit den Einstellungen, die Sie zuvor vom ursprünglichen Node erfasst haben.
5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node4 nach Bedarf: • So programmieren Sie Zielanschlüsse: `system node hardware unified-connect modify -type
-t target -adapter *port_name*` ** So programmieren Sie Initiator-Ports: `system node unified-connect modify type	-t initiator -adapter *port_name*` `-type` Ist der FC4-Typ, das Ziel oder der Initiator.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node4 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

6. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `system node unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `ucadmin show`

7. Führen Sie eine der folgenden Aktionen durch:

Wenn die FC-Standardeinstellungen auf den neuen Nodes sind…	Dann…
Das gleiche wie diejenigen, die Sie auf den ursprünglichen Knoten erfasst	Gehen Sie zu Schritt 11.
Anders als jene, die Sie auf den ursprünglichen Knoten erfasst haben	Gehen Sie zu Schritt 8.

8. Wartungsmodus beenden:

```
halt
```

9. Nachdem Sie den Befehl eingegeben haben, warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
10. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder verfügt über FlexArray Virtualisierungssoftware mit Data ONTAP 8.3.0 oder höher	Greifen Sie auf den Wartungsmodus zu, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `boot_ontap maint`
Ist kein V-Series System und verfügt nicht über FlexArray Virtualisierungssoftware	Boot node4 durch Eingabe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung: `boot_ontap`

11. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Gehen Sie zu UTA/UTA2-Ports auf node4 prüfen und konfigurieren Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt und gehen Sie zu "Weisen Sie Ports von node2 nach node4 zu" Wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Gehen Sie zu UTA/UTA2-Ports auf node4 prüfen und konfigurieren Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt *UTA/UTA2-Ports auf node4* überprüfen und konfigurieren, wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat, kehren Sie zum Abschnitt *Installieren und Booten von node4* zurück, und setzen Sie den Abschnitt unter fort "Schritt 9".

UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Wenn node4 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie je nach Nutzung des aktualisierten Systems konfigurieren.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht es, gleichzeitig NIC- und FCoE-Datenverkehr auf die gleiche 10-GbE-SFP+-Schnittstelle zu übertragen und das FC-Ziel zu unterstützen.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

UTA2-Ports können an einem Adapter oder auf dem Controller mit den folgenden Konfigurationen verwendet werden:

- UTA-/UTA2-Karten, die gleichzeitig mit dem Controller bestellt wurden, werden vor dem Versand konfiguriert, um die von Ihnen angeforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden konfiguriert (vor dem Versand), um die von Ihnen angeforderte Persönlichkeit zu besitzen.

Sie können jedoch die Konfiguration der UTA/UTA2-Ports auf node4 überprüfen und sie gegebenenfalls ändern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein MetroCluster FC-System, ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware verfügen, die mit Storage-Arrays verbunden ist, müssen Sie sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit mit einem der folgenden Befehle auf node4 konfiguriert werden:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node   Adapter  Mode     Type       Mode      Type      Status
----   -------  ---      ---------  -------   --------  -------
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Überprüfen Sie die Ausgabe des `system node hardware unified-connect show` Oder `ucadmin`

`show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.

4. Führen Sie eine der folgenden Aktionen durch:

Wenn die CNA-Ports…	Dann…
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Verfügt über Speicherfestplatten und führt Data ONTAP 8.3 aus	Boot-node4 und wechseln in den Wartungsmodus: `boot_ontap maint`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 6. Sie sollten sich bereits im Wartungsmodus befinden.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7.
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

7. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

```
storage disable adapter adapter_name
```

Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

8. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, geben Sie den folgenden Befehl ein, um die Konfiguration nach Bedarf zu ändern:

```
ucadmin modify -m fc|cna -t initiator|target adapter_name
```

- `-m` Ist der Personality Modus: FC oder 10GbE UTA.
- `-t` Ist der FC4-Typ: Target oder Initiator.

> Sie müssen FC Initiator für Tape-Laufwerke und FlexArray-Virtualisierungssysteme verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

9. Überprüfen Sie die Einstellungen, indem Sie den folgenden Befehl eingeben und seine Ausgabe überprüfen:

```
ucadmin show
```

10. Führen Sie eine der folgenden Aktionen aus:

Wenn das System…	Dann…

Festplatten sind vorhanden	a. Geben Sie den folgenden Befehl ein:
	`halt`
	Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.
	b. Geben Sie den folgenden Befehl ein:
	`boot_ontap`

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden und läuft Data ONTAP 8.3	Neustart in Wartungsmodus: `boot_ontap maint`

11. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Geben Sie den folgenden Befehl ein: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Geben Sie den folgenden Befehl ein: `ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`.

```
cluster1::> system node hardware unified-connect show
                Current  Current    Pending  Pending    Admin
Node  Adapter  Mode     Type       Mode     Type       Status
----  -------  -------  ---------  -------  -------    -----
f-a    1a      fc       initiator  -        -          online
f-a    1b      fc       target     -        initiator  online
f-a    2a      fc       target     cna      -          online
f-a    2b      fc       target     cna      -          online
4 entries were displayed.
```

```
*> ucadmin show
                Current Current    Pending  Pending    Admin
Node  Adapter   Mode    Type       Mode     Type       Status
----  -------   ------- ---------  -------  -------    -----
f-a     1a      fc      initiator  -        -          online
f-a     1b      fc      target     -        initiator  online
f-a     2a      fc      target     cna      -          online
f-a     2b      fc      target     cna      -          online
4 entries were displayed.
*>
```

12. Platzieren Sie alle Ziel-Ports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

13. Anschluss verkabeln.
14. Führen Sie eine der folgenden Aktionen aus:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Weisen Sie Ports von node2 nach node4 zu".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zum Abschnitt *Installieren und Starten von node4* zurück, und setzen Sie den Abschnitt unter fort "Schritt 9".

Weisen Sie Ports von node2 nach node4 zu

Sie müssen sicherstellen, dass die physischen Ports auf node2 den physischen Ports auf node4 korrekt zugeordnet werden. damit kann node4 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Bevor Sie beginnen

Sie müssen bereits über die Ports auf den neuen Nodes verfügen, um auf diese Informationen zuzugreifen, siehe "Quellen" Zum Verknüpfen mit der *Hardware Universe*. Die Informationen werden später in diesem Abschnitt verwendet.

die Softwarekonfiguration von node4 muss mit der physischen Konnektivität von node4 übereinstimmen. Die IP-Konnektivität muss wiederhergestellt werden, bevor Sie mit dem Upgrade fortfahren.

Über diese Aufgabe

Die Port-Einstellungen können je nach Modell der Nodes variieren.

Schritte

1. Führen Sie die folgenden Schritte durch, um zu überprüfen, ob es sich bei dem Setup um ein Cluster mit zwei Nodes ohne Switches handelt:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

      `network options switchless-cluster show`

      Beispiel:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster:  false/true
```

   +
   Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

   a. Kehren Sie mit dem folgenden Befehl zur Administrationsberechtigungsebene zurück:

      `set -privilege admin`

2. Nehmen Sie folgende Änderungen vor:

   a. Ändern Sie Ports, die Teil von sein werden `Cluster` Broadcast-Domäne:

      `network port modify -node` *`node_name`* `-port` *`port_name`* `-mtu 9000 -ipspace Cluster`

      Dieses Beispiel fügt Cluster-Port „e1b“ auf „node2“ hinzu:

      `network port modify -node node2 -port e1b -ipspace Cluster -mtu 9000`

   b. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

      `network interface migrate -vserver` *`vserver_name`* `-lif` *`lif_name`* `source-node node2 -destination-node node2 -destination-port` *`port_name`*

      Wenn alle Cluster-LIFs migriert und die Cluster-Kommunikation eingerichtet ist, sollte das Cluster ein Quorum bilden.

   c. Ändern Sie den Startport der Cluster LIFs:

      `network interface modify -vserver Cluster -lif` *`lif_name`* `–home-port` *`port_name`*

   d. Entfernen Sie die alten Ports aus dem `Cluster` Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports node2:port
```

e. Zeigen Sie das an `health` Zustand der Node2/node4:

```
cluster show -node node2 -fields health
```

f. Führen Sie abhängig von der ONTAP-Version auf dem zu aktualisierenden HA-Paar eine der folgenden Aktionen durch:

Lautet Ihre ONTAP Version…	Dann…
9.8 bis 9.11.1	Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören: `::> network connections listening show -vserver Cluster`
9.12.1 oder höher	Überspringen Sie diesen Schritt und gehen Sie zu Schritt 3.

Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

g. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Wiederholen Sie den Unterschritt (f), um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 nachhört.

3. Ändern Sie die Mitgliedschaften der Broadcast-Domänen von physischen Ports, die Daten-LIFs hosten.

a. Listen Sie den Status der Erreichbarkeit aller Ports auf:

```
network port reachability show
```

b. Reparieren Sie die Erreichbarkeit der physischen Ports, gefolgt von VLAN-Ports, indem Sie den folgenden Befehl an jedem Port, jeweils einen Port, ausführen:

`reachability repair -node node_name -port port_name`

Es wird eine Warnung wie folgt erwartet. Überprüfen und geben Sie ggf. y oder n ein:

```
Warning: Repairing port "node_name:port" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

c. Um ONTAP zum Abschließen der Reparatur zu aktivieren, warten Sie etwa eine Minute nach Ausführung des `reachability repair` Befehl am letzten Port.

d. Alle Broadcast-Domänen auf dem Cluster auflisten:

`network port broadcast-domain show`

e. Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der vorhandenen Broadcast-Domänen entspricht, erstellt ONTAP neue Broadcast-Domains für diese Ports. Bei Bedarf können Sie die neu erstellten Broadcast-Domänen löschen, wenn alle deren Mitgliedsports zu Mitgliedsports der Interface Groups werden. Broadcast-Domänen löschen:

`broadcast-domain delete -broadcast-domain broadcast_domain`

f. Überprüfen Sie die Schnittstellengruppenkonfiguration und fügen Sie bei Bedarf Mitgliedsports hinzu oder löschen Sie sie.

Fügen Sie Mitgliedsports zu Schnittstellen-Gruppen-Ports hinzu:

`ifgrp add-port -node node_name -ifgrp ifgrp_port -port port_name`

Entfernen Sie Mitgliedsports aus Schnittstellen-Gruppen-Ports:

`ifgrp remove-port -node node_name -ifgrp ifgrp_port -port port_name`

g. Löschen Sie VLAN-Ports nach Bedarf und erstellen Sie sie neu. VLAN-Ports löschen:

`vlan delete -node node_name -vlan-name vlan_port`

VLAN-Ports erstellen:

`vlan create -node node_name -vlan-name vlan_port`

ⓘ Abhängig von der Komplexität der Netzwerkkonfiguration des aktualisierten Systems müssen Sie unter Umständen Teilschritte (a) bis (g) wiederholen, bis alle Ports dort richtig platziert sind, wo sie benötigt werden.

4. Wenn keine VLANs im System konfiguriert sind, fahren Sie mit fort Schritt 5. Wenn VLANs konfiguriert sind, stellen Sie versetzte VLANs wieder her, die zuvor auf Ports konfiguriert wurden, die nicht mehr vorhanden sind oder auf Ports konfiguriert wurden, die in eine andere Broadcast-Domäne verschoben wurden.

a. Anzeigen der verschobenen VLANs:

```
cluster controller-replacement network displaced-vlans show
```

b. Stellen Sie die vertriebenen VLANs auf den gewünschten Zielanschluss wieder her:

```
displaced-vlans restore -node node_name -port port_name -destination-port
destination_port
```

c. Überprüfen Sie, ob alle vertriebenen VLANs wiederhergestellt wurden:

```
cluster controller-replacement network displaced-vlans show
```

d. Etwa eine Minute nach der Erstellung werden VLANs automatisch in die entsprechenden Broadcast-Domänen platziert. Überprüfen Sie, ob die wiederhergestellten VLANs in die entsprechenden Broadcast-Domänen platziert wurden:

```
network port reachability show
```

5. ab ONTAP 9.8 ändert ONTAP automatisch die Home Ports der LIFs, wenn die Ports während der Reparatur des Netzwerkports zwischen Broadcast-Domänen verschoben werden. Wenn der Home Port einer LIF auf einen anderen Knoten verschoben wurde oder nicht zugewiesen ist, wird diese LIF als vertriebene LIF dargestellt. Stellen Sie die Home-Ports der vertriebenen LIFs wieder her, deren Home-Ports nicht mehr vorhanden sind oder in einen anderen Node verschoben wurden.

a. Zeigen Sie die LIFs an, deren Home-Ports möglicherweise zu einem anderen Node verschoben oder nicht mehr vorhanden sind:

```
displaced-interface show
```

b. Stellen Sie den Home Port jeder logischen Schnittstelle wieder her:

```
displaced-interface restore -vserver vserver_name -lif-name lif_name
```

c. Überprüfen Sie, ob alle LIF Home Ports wiederhergestellt sind:

```
displaced-interface show
```

Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als melden `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn Ports einen anderen Status als diese beiden melden, reparieren Sie die Erreichbarkeit wie in beschrieben Schritt 3.

6. Überprüfen Sie, ob alle LIFs administrativ von Ports vorhanden sind, die zu den richtigen Broadcast-Domänen gehören.

a. Prüfen Sie auf administrativ heruntergekommen LIFs:

```
network interface show -vserver vserver_name -status-admin down
```

b. Prüfen Sie alle LIFs, die operativ inaktiv sind:

```
network interface show -vserver vserver_name -status-oper down
```

c. Ändern Sie alle LIFs, die geändert werden müssen, um über einen anderen Home-Port zu verfügen:

```
network interface modify -vserver vserver_name -lif lif_name -home-port
home_port
```

> Für iSCSI LIFs muss die Modifikation des Home Ports die LIF administrativ heruntergefahren werden.

a. Zurücksetzen von LIFs, die nicht die Heimat ihrer jeweiligen Home-Ports sind:

```
network interface revert *
```

Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4

Nachdem Sie die Ports von node2 nach node4 zugeordnet und bevor Sie node2-Aggregate von node3 auf node4 verschoben haben, müssen Sie die NAS-Daten-LIFs, die sich im Besitz von node2 befinden, verschieben, die sich zurzeit auf node3 von node3 nach node4 befinden. Sie müssen außerdem die SAN LIFs auf node4 überprüfen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs ordnungsgemäß sind und sich in den entsprechenden Ports befinden, nachdem Sie node4 in den Online-Modus versetzt haben.

Schritte

1. Führen Sie alle NAS-Daten-LIFs auf, die nicht im Besitz von node3 sind, durch Eingabe des folgenden Befehls auf einem der Nodes und Erfassung der Ausgabe auf:

```
network interface show -role data -curr-node node3 -is-home false
```

2. Wenn das Cluster für SAN LIFs konfiguriert ist, notieren Sie in diesem Fall die SAN LIFs und vorhandene Konfigurationsinformationen "Arbeitsblatt" Zur späteren Verwendung im Verfahren.

   a. Führen Sie die SAN-LIFs auf Knoten3 auf und untersuchen Sie die Ausgabe:

```
network interface show -data-protocol fc*
```

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------  ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Führen Sie die vorhandenen Konfigurationen auf und untersuchen Sie die Ausgabe:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Führen Sie eine der folgenden Aktionen durch:

Falls Knoten 2…	Beschreibung
Schnittstellengruppen oder VLANs wurden konfiguriert	Gehen Sie zu Schritt 4.
Schnittstellengruppen oder VLANs waren nicht konfiguriert	Überspringen Sie Schritt 4, und fahren Sie mit fort Schritt 5.

4. Nehmen Sie die folgenden Schritte durch, um alle NAS-Daten-LIFs zu migrieren, die auf Schnittstellengruppen und VLANs gehostet wurden, die sich ursprünglich auf node2 von node3 auf node4 befanden.

   a. Migrieren Sie alle auf node3 gehosteten LIFs, die zuvor node2 auf einer Schnittstellengruppe zu einem Port auf node4 gehören, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

      `network interface migrate -vserver` *`vserver_name`* `-lif` *`lif_name`* `-destination -node node4 –destination-port` *`netport|ifgrp`*

   b. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`datalif_name`* `-home-node node4 home-port` *`netport|ifgrp`*

   c. [[man_lif_verify_4_subsepc] Migrieren Sie alle auf node3 gehosteten LIFs, die zuvor zu node2 auf

einem VLAN-Port gehörten, zu einem Port auf node4, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif datalif_name
-destination-node node4 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif datalif_name -home-node
node4 home-port netport|ifgrp
```

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 6 Bis Schritt 9, überspringen Sie Schritt 10, und abgeschlossen Schritt 11 Bis Schritt 14.
San	Überspringen Sie Schritt 6 bis Schritt 9, und schließen Sie sie ab Schritt 10 Bis Schritt 14.
Sowohl NAS als auch SAN	Vollständig Schritt 6 Bis Schritt 14.

6. Wenn auf Ihren Plattformen nicht dieselben Daten-Ports vorhanden sind, geben Sie den folgenden Befehl ein, um die Ports der Broadcast-Domäne hinzuzufügen:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „6280-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain-Management im IPspace hinzu Standard:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrieren Sie jede LIF mit NAS-Daten auf node4, indem Sie einmal für jede logische Schnittstelle den folgenden Befehl eingeben:

```
network interface migrate -vserver vserver-name -lif datalif-name -destination
-node node4 -destination-port netport|ifgrp -home-node node4
```

8. Sicherstellen, dass die Datenmigration persistent ist:

```
network interface modify -vserver vserver_name -lif datalif_name -home-port
netport|ifgrp
```

9. Überprüfen Sie den Status aller Links als `up` Mit dem folgenden Befehl werden alle Netzwerk-Ports aufgelistet und ihre Ausgabe untersucht:

```
network port show
```

Das folgende Beispiel zeigt die Ausgabe von `network port show` Befehl mit einigen LIFs oben und anderen unten:

```
cluster::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node3
       a0a       Default      -                up       1500  auto/1000
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0a-1     Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
node4
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
12 entries were displayed.
```

10. Wenn die Ausgabe des `network port show` Befehl zeigt Netzwerkports an, die im neuen Node nicht verfügbar sind und in den alten Nodes vorhanden sind. Löschen Sie die alten Netzwerk-Ports, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie die erweiterte Berechtigungsebene ein, indem Sie den folgenden Befehl eingeben:

       `set -privilege advanced`

    b. Geben Sie für jeden alten Netzwerk-Port den folgenden Befehl ein:

       `network port delete -node` *`node_name`* `-port` *`port_name`*

    c. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:

       `set -privilege admin`

11. Bestätigen Sie, dass sich die SAN-LIFs auf den richtigen Ports an node4 befinden, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

       `network interface show -data-protocol iscsi|fcp -home-node node4`

       Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster::> network interface show -data-protocol iscsi|fcp -home-node
node4
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            a0a          up/down  10.63.0.53/24      node4
a0a     true
            data1        up/up    10.63.0.50/18      node4
e0c     true
            rads1        up/up    10.63.0.51/18      node4
e1a     true
            rads2        up/down  10.63.0.52/24      node4
e1b     true
vs1
            lif1         up/up    172.17.176.120/24  node4
e0c     true
            lif2         up/up    172.17.176.121/24  node4
```

b. Überprüfen Sie, ob die neue `adapter` Und `switch-port` Die Konfigurationen sind korrekt, indem die Ausgabe von dem verglichen wird `fcp adapter show` Befehl mit den neuen Konfigurationsinformationen, die Sie im Arbeitsblatt in aufgezeichnet haben Schritt 2.

   Liste der neuen SAN LIF-Konfigurationen auf node4:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

Wenn sich ein SAN LIF in der neuen Konfiguration nicht auf einem Adapter befindet, der noch an denselben angeschlossen ist `switch-port`, Es kann zu einem Systemausfall führen, wenn Sie den Node neu booten.

c. Wenn node4 eine SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der in node2 nicht vorhanden war, verschieben Sie sie in einen entsprechenden Port an node4, indem Sie einen der folgenden Befehle eingeben:

   i. Setzen Sie den LIF-Status auf „down“:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-status -admin down`

   ii. Entfernen Sie das LIF aus dem Portsatz:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Geben Sie einen der folgenden Befehle ein:

      - Verschieben eines einzelnen LIF:

        `network interface modify -lif` *`lif_name`* `-home-port` *`new_home_port`*

      - Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen neuen Port:

```
network interface modify {-home-port port_on_node2 -home-node node2
-role data} -home-port new_home_port_on_node4
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

Sie müssen SAN-LIFs zu einem Port verschieben, der die gleiche Verbindungsgeschwindigkeit wie der ursprüngliche Port hat.

12. Ändern Sie den Status aller LIFs in `up` Damit die LIFs Datenverkehr auf dem Node akzeptieren und senden können, indem Sie den folgenden Befehl eingeben:

```
network interface modify -vserver vserver_name -home-port port_name -home-node
node4 lif lif_name -status-admin up
```

13. Überprüfen Sie, ob alle SAN-LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von aufweisen `up` Wenn Sie auf einem der beiden Nodes den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network interface show -home-node node4 -role data
```

14. Wenn LIFs ausgefallen sind, setzen Sie den Administrationsstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif lif_name -status-admin up
```

Arbeitsblatt: Informationen, die aufgezeichnet werden sollen, bevor NAS-Daten-LIFs in node4 verschoben werden

Um zu überprüfen, ob Sie die richtige Konfiguration haben, nachdem Sie SAN LIFs von node3 nach node4 verschoben haben, können Sie das folgende Arbeitsblatt verwenden, um die aufzuzeichnen `adapter` Und `switch-port` Informationen für jedes LIF.

Notieren Sie das LIF `adapter` Informationen aus dem `network interface show -data-protocol fc*` Befehlsausgabe und das `switch-port` Informationen aus dem `fcp adapter show -fields switch-port,fc-wwpn` Befehlsausgabe für node3.

Notieren Sie nach Abschluss der Migration zu node4 die LIF `adapter` Und `switch-port` Informationen für die LIFs auf node4 und vergewissern Sie sich, dass jede LIF noch immer mit derselben verbunden ist `switch-port`.

Node3			**Node4**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Node3			Node4		

Verschiebung von nicht-Root-Aggregaten node2 von Node3 in node4

Nachdem node2's nicht-Root-Aggregate in node3 verschoben wurden, müssen Sie sie nun von node3 auf node4 verschieben.

Schritte

1. Geben Sie den folgenden Befehl auf beiden Controllern ein, und überprüfen Sie die Ausgabe, um zu ermitteln, welche nicht-Root-Aggregate verschoben werden sollen:

   ```
   storage aggregate show -owner-name node3 -home-id node2_system_id
   ```

2. Verschieben Sie die Aggregate, indem Sie die folgenden Teilschritte ausführen:

   a. Greifen Sie auf die erweiterte Berechtigungsebene zu, indem Sie den folgenden Befehl auf einem der Nodes eingeben:

      ```
      set -privilege advanced
      ```

   b. Geben Sie den folgenden Befehl ein:

      ```
      storage aggregate relocation start -node node3 -destination node4 -aggregate -list aggr_name1, aggr_name2… -ndo-controller-upgrade true
      ```

   Die Aggregatliste ist die Liste der Aggregate, deren Eigentümer node4 sind, die Sie in erhalten haben Schritt 1.

   a. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge finden im Hintergrund statt. Um ein Aggregat verschieben zu können, dauerte der Vorgang einige Sekunden oder Minuten. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

   b. Zurück zur Administratorebene:

      ```
      set -privilege admin
      ```

3. Standortstatus prüfen:

   ```
   storage aggregate relocation show -node node3
   ```

   Die Ausgabe wird angezeigt `Done` Für ein Aggregat, nachdem es verlegt wurde.

   Warten Sie, bis alle node2-Aggregate in node4 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

4. Führen Sie eine der folgenden Aktionen durch:

Bei Umzug von…	Dann…
Alle Aggregate waren erfolgreich	Gehen Sie zu Schritt 5.

Aggregate sind ausgefallen oder sie wurden Vetos gemacht	a. Überprüfen Sie die EMS-Protokolle auf Korrekturmaßnahmen.
	b. Führen Sie die Korrekturmaßnahme durch.
	c. Greifen Sie auf die erweiterte Berechtigungsebene zu, indem Sie den folgenden Befehl auf einem der Nodes eingeben:
	`set -privilege advanced`
	d. Verschiebung ausgefallener oder Vetos von Aggregaten:
	`storage aggregate relocation start -node node3 destination node4 -aggregate-list aggr_name1, aggr_name2… ndo-controller-upgrade true`
	Die aggregierte Liste enthält fehlerhafte oder Vetos zusammengesetzte Aggregate.
	e. Geben Sie bei der entsprechenden Aufforderung ein `y`.
	f. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:
	`set -privilege admin`
	Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen:
	• Veto-Prüfungen überschreiben:
	`storage aggregate relocation start -override -vetoes -ndo-controller-upgrade`
	• Zielprüfungen überschreiben:
	`storage aggregate relocation start -override -destination-checks -ndocontroller-upgrade`
	Weitere Informationen zu den Befehlen zum Verlegen von Storage-Aggregaten finden Sie unter "Quellen" Verbinden mit *Disk und Aggregat-Management mit den Befehlen CLI* und *ONTAP 9: Manual Page Reference*.

5. Überprüfen Sie, ob alle node2 nicht-Root-Aggregate online sind und ihren Status auf node4 haben:

   `storage aggregate show -node node4 -state offline -root false`

   Die node2 Aggregate wurden in der Ausgabe des Befehls in aufgeführt Schritt 1.

6. Wenn ein Aggregat offline gegangen ist oder fremd geworden ist, bringen Sie es mit dem folgenden Befehl

für jedes Aggregat online:

```
storage aggregate online -aggregate aggr_name
```

7. Überprüfen Sie, ob alle Volumes in node2 Aggregaten auf node4 online sind:

```
volume show -node node4 -state offline
```

8. Wenn Volumes auf node4 offline sind, bringen Sie sie online:

```
volume online -vserver vserver-name -volume volume_name
```

9. Senden Sie eine AutoSupport Nachricht nach dem Upgrade an NetApp für node4:

```
system node autosupport invoke -node node4 -type all -message "node2
successfully upgraded from platform_old to platform_new"
```

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

Authentifizierungsmanagement mit KMIP-Servern

Mit ONTAP 9.5 und höher können KMIP-Server (Key Management Interoperability Protocol) Authentifizierungsschlüssel managen.

Schritte

1. Hinzufügen eines neuen Controllers:

```
security key-manager setup -node new_controller_name
```

2. Fügen Sie den Schlüsselmanager hinzu:

```
security key-manager -add key_management_server_ip_address
```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

```
security key-manager restore -node new_controller_name
```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um die korrekte Einrichtung zu bestätigen, aktivieren Sie das HA-Paar. Außerdem überprüfen Sie, ob Node 3 und node 4 auf den Storage zugreifen können und ob keine der Daten-LIFs gehören, die zu anderen Nodes im Cluster gehören. Außerdem bestätigen Sie, dass Node 3 Eigentümer der Aggregate von Node 1 ist und node4 Eigentümer der Aggregate von Node 2 ist und die Volumes für beide Nodes online sind.

Schritte

1. Aktivieren Sie Storage Failover, indem Sie auf einem der Nodes den folgenden Befehl eingeben:

```
storage failover modify -enabled true -node node3
```

2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

```
storage failover show
```

Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ------------------
node3          node4          true     Connected to node4
node4          node3          true     Connected to node3
```

3. Führen Sie eine der folgenden Aktionen durch:

Wenn der Cluster ein…	Beschreibung
Cluster mit zwei Nodes	Aktivieren Sie die Hochverfügbarkeit im Cluster, indem Sie auf einem der Nodes den folgenden Befehl eingeben: `cluster ha modify -configured true`
Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 4.

4. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
cluster show
```

5. Stellen Sie sicher, dass node3 und node4 auf den Storage der jeweils anderen zugreifen können, indem

Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
storage failover show -fields local-missing-disks,partner-missing-disks
```

6. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Geben Sie dazu den folgenden Befehl ein und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn Node3 oder node4 im Besitz von Daten-LIFs sind, die sich im Besitz anderer Nodes im Cluster befinden, verwenden Sie die `network interface revert` Befehl zum Zurücksetzen der Daten-LIFs auf den Home-Eigentümer.

7. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

   ```
   storage aggregate show -owner-name node3
   storage aggregate show -owner-name node4
   ```

8. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node node3 -state offline
   volume show -node node4 -state offline
   ```

9. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie in erfasst haben "Schritt 19 (d)" In *die Nodes für Upgrade* vorbereiten und jedes der Offline-Volumes nach Bedarf durch Eingabe des folgenden Befehls ein Mal für jedes Volume den Online-Modus versetzen:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

10. Installieren Sie neue Lizenzen für die neuen Nodes, indem Sie den folgenden Befehl für jeden Node eingeben:

    ```
    system license add -license-code license_code,license_code,license_code…
    ```

    Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, jeden Lizenzschlüssel durch ein Komma getrennt.

11. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie den eingestellt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel in "Schritt 16" Von *Install and Boot node3*) müssen Sie die Variable aufheben:

    ```
    set diag; systemshell -node node_name -command sudo kenv -u -p
    kmip.init.maxwait
    ```

12. Geben Sie einen der folgenden Befehle ein, um alle alten Lizenzen von den ursprünglichen Nodes zu entfernen:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number node_serial_number -package
    licensable_package
    ```

    - Um alle abgelaufenen Lizenzen zu löschen, geben Sie Folgendes ein:

```
system license clean-up -expired
```

- Um alle nicht verwendeten Lizenzen zu löschen, geben Sie Folgendes ein:

```
system license clean-up -unused
```

- Geben Sie zum Löschen einer bestimmten Lizenz von einem Cluster die folgenden Befehle auf den Nodes ein:

```
system license delete -serial-number node1_serial_number -package *
system license delete -serial-number node2_serial_number -package *
```

Die folgende Ausgabe wird angezeigt:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

+
Eingabe `y` Um alle Pakete zu entfernen.

13. Überprüfen Sie die ordnungsgemäße Installation der Lizenzen, indem Sie den folgenden Befehl eingeben und seine Ausgabe überprüfen:

```
system license show
```

Sie können die Ausgabe mit der Ausgabe vergleichen, die Sie in erfasst haben "Schritt 30" Von *die Nodes für Upgrade vorbereiten*.

14. Konfigurieren Sie die SPs, indem Sie auf beiden Knoten den folgenden Befehl ausführen:

```
system service-processor network modify -node node_name
```

Gehen Sie zu "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen über die SPs und die Befehle *ONTAP 9: Manual Page Reference* für detaillierte Informationen zum `system service-processor network modify` Befehl.

15. Wenn Sie ein Cluster ohne Switches auf den neuen Nodes einrichten möchten, fahren Sie mit fort "Quellen" Um eine Verbindung zur *Network Support Site* herzustellen, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf Node3 und node4 aktiviert ist, führen Sie die Schritte in aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Führen Sie andernfalls die Schritte unter aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von

Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager show -status

   security key-manager query
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.
   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server.

      Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.
4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager restore -node new_controller_name
   ```

Einrichten von NetApp Volume oder Aggregte Verschlüsselung auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

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

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:

   a. Fügen Sie den Verschlüsselungsmanagementserver mit dem folgenden Befehl hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagement-Server erfolgreich hinzugefügt wurden. Verwenden Sie dazu den folgenden Befehl:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Verschlüsselungsmanagement-Server auf dem neuen Knoten, indem Sie den folgenden Befehl verwenden:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.

4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

Für…	Befehl
Externer Schlüsselmanager	`security key-manager external restore`Für diesen Befehl ist die OKM-Passphrase erforderlich
Onboard Key Manager (OKM)	`security key-manager onboard sync`

   Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder externe Verschlüsselungsmanagementserver nicht erreicht werden konnten. Stellen Sie diese Volumes

mithilfe der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "ARL Upgrade-Workflow". Die Informationen über mögliche Fehler werden in der Phase des Verfahrens aufgelistet.

- "Fehler bei der Aggregatverschiebung"
- "Neustarts, Panikspiele oder Energiezyklen"
- "Probleme, die in mehreren Phasen des Verfahrens auftreten können"
- "Fehler bei der LIF-Migration"
- "LIFs befinden sich bei ungültigen Ports nach dem Upgrade"

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   `storage aggregate relocation show`

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 waren, gehören node4 nach Abschluss des Upgrades

Beim Abschluss des Upgrade-Verfahrens muss die Knoten3 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node die Knoten1 hatten. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Unter den folgenden Umständen kann es nicht gelingen, Aggregate ordnungsgemäß zu verschieben und Node 1 als Home Node anstelle von Knoten3 zu verwenden:

- In Phase 3, wenn Aggregate von node2 auf node3 verschoben werden. Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen

werden kann, dann wird das Aggregat auf node2 zurückgelassen.

- Nach Stufe 4, wenn node2 durch node4 ersetzt wird. Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node4 als Home-Node statt node3 online.

Sie können das falsche Eigentümerproblem nach Phase 6 beheben, wenn ein Storage-Failover aktiviert wurde, indem Sie die folgenden Schritte durchführen:

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Liste der Aggregate zu erhalten:

   `storage aggregate show -nodes node4 -is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 Mit der Ausgabe, die Sie für node1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links auf node4:

   `storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3`

   Verwenden Sie das nicht `-ndo-controller-upgrade` Parameter während dieser Verschiebung.

4. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob node3 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate aggr1,aggr2,aggr3… -fields home-name`

   aggr1,aggr2,aggr3… Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht über Node3 als Hausbesitzer verfügen, können mit dem gleichen Relocation-Befehl in auf node3 verschoben werden Schritt 3.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, in Panik geraten oder aus- und wieder eingeschaltet werden. Die Lösung dieser Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikspiele oder Energiezyklen in Phase 2

Abstürze können vor, während oder unmittelbar nach Phase 2 auftreten, während der Sie Aggregate von node1 auf node2 verschieben, Daten-LIFs und SAN-LIFs im Besitz von node1 auf node2 verschieben, node1-Informationen aufzeichnen und Knoten1 ausmustern.

Node1 oder node2 stürzt vor Phase 2 ab, und HA ist noch aktiviert

Wenn node1 oder node2 vor Phase 2 abstürzt, wurden noch keine Aggregate verschoben und die HA-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während oder direkt nach Phase 2 ab, und HA ist noch aktiviert

Einige oder alle Aggregate wurden von node1 in node2 verschoben und die HA ist noch aktiviert. Node2 wird das Root-Volume von node1 und alle nicht-Root-Aggregate übernehmen, die nicht verschoben wurden.

Über diese Aufgabe

Das Eigentum an verlagerten Aggregaten sieht mit dem Eigentum nicht-Root-Aggregaten identisch aus, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat. Wenn node1 in den eintritt `waiting for giveback state`, Node2 wird alle node1 nicht-Root-Aggregate zurückgeben.

Schritte

1. Vollständig "Schritt 1" Im Abschnitt *Non-Root-Aggregate wieder von node1 nach node2* verschieben.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt nach Phase 2 ab, während HA deaktiviert ist

Node2 wird nicht übernehmen, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

   Möglicherweise sehen Sie einige Änderungen in der Ausgabe von `storage failover show` Befehl, aber das ist typisch und hat keine Auswirkung auf das Verfahren. Siehe Abschnitt Fehlerbehebung "Unerwarteter Storage-Failover zeigt die Befehlsausgabe an".

Node2 fällt während oder nach Phase 2 aus, bei aktiviertem HA

Node1 hat einige oder alle seine Aggregate in node2 verschoben. HA ist aktiviert.

Über diese Aufgabe

Node1 wird alle Aggregate node2 sowie alle eigenen Aggregate übernehmen, die es auf node2 verlagert hatte. Wenn node2 in den eintritt `Waiting for Giveback` Zustand: Node1 gibt alle Aggregate node2 zurück.

Schritte

1. Vollständig "Schritt 1" Im Abschnitt *Non-Root-Aggregate wieder von node1 nach node2* verschieben.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt nach Phase 2 ab und nach HA ist deaktiviert

Node1 wird nicht übernehmen.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall wird für alle Aggregate auftreten, während node2 gestartet wird.

2. Fahren Sie mit dem verbleibenden Upgrade des Node-Paars fort.

Neustarts, Panikspiele oder Energiezyklen in Phase 3

Ausfälle können während oder unmittelbar nach Phase 3 auftreten. In dieser Phase installieren und booten Sie Node3, weisen Ports von node1 zu node3 zu, verschieben Daten-LIFs und SAN-LIFs, die zu node1 und node2 zu node3 gehören, und verschieben alle Aggregate von node2 auf node3.

Knoten 2 Absturz in Phase 3 mit deaktiviertem HA und vor dem Verschieben von Aggregaten

Node3 wird nach einem Absturz nach einem node2 nicht mehr übernehmen, da HA bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall wird für alle Aggregate auftreten, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während Phase 3 ab, nachdem einige oder alle Aggregate verschoben wurden

Node2 hat einige oder alle seine Aggregate in Node3 verschoben, die Daten von Aggregaten bereitstellen, die umgezogen wurden. HA ist deaktiviert.

Über diese Aufgabe

Es wird ein Client-Ausfall für Aggregate geben, die nicht verlagert wurden.

Schritte

1. Knoten 2 aufbring.
2. Verschieben Sie die verbleibenden Aggregate durch Abschluss "Schritt 1" Bis "Schritt 3" Im Abschnitt *Non-Root-Aggregate von node2 auf node3* verschieben.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während Phase 3 und vor node2 hat alle Aggregate verschoben

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während der Phase 3 während der Aggregatverschiebung ab

Falls node3 abstürzt, während node2 Aggregate zu node3 verschoben wird, wird node2 die Verschiebung aller verbleibenden Aggregate abbrechen.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Knoten 3 verlagert wurden, begegnen ein Client-Ausfall, während node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Vollständig "Schritt 3" Wieder im Abschnitt *Verschiebung von nicht-Root-Aggregaten von node2 zu node3*.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 startet nach einem Absturz in Phase 3 nicht

Aufgrund eines katastrophalen Ausfalls kann nach einem Absturz in Phase 3 nicht node3 gestartet werden.

Schritt

1. Wenden Sie sich an den technischen Support.

Node2 stürzt nach Phase 3 aber vor Phase 5 ab

Node3 stellt weiterhin Daten für alle Aggregate bereit. Das HA-Paar ist deaktiviert.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt nach Phase 3, aber vor Phase 5 ab

Node3 stürzt nach Phase 3, aber vor Phase 5 ab. Das HA-Paar ist deaktiviert.

Schritte

1. Knoten 3 aufbring.

   Es gibt einen Client-Ausfall für alle Aggregate.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikspiele oder Energiezyklen in Phase 5

Es können zu Abstürzen kommen, während Phase 5, in der Sie node4 installieren und booten, Ports von node2 nach node4 abbilden, Daten-LIFs und SAN-LIFs, die zu node2 von node3 nach node4 gehören, und alle Aggregate von node2 in node4 verschieben.

Node3 stürzt in Phase 5 ab

Node3 hat einige oder alle node2 Aggregate in node4 verschoben. Node4 übernimmt nicht, dient aber weiterhin nicht-Root-Aggregate, die node3 bereits verschoben hat. Das HA-Paar ist deaktiviert.

Über diese Aufgabe

Es gibt einen Ausfall für den Rest der Aggregate, bis node3 wieder hochfährt.

Schritte

1. Knoten 3 aufbring.
2. Verschiebung der verbleibenden Aggregate, die zu Knoten 2 gehörten, durch Wiederholung "Schritt 1" Bis "Schritt 3" Im Abschnitt *Verschiebung der nicht-Root-Aggregate von node2 nach node3*.

3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node4 stürzt in Phase 5 ab

Node3 hat einige oder alle node2 Aggregate in node4 verschoben. Node3 übernimmt nicht die Übernahme, dient aber weiterhin nicht-Root-Aggregate, die Node3 besitzt, sowie solche, die nicht verlagert wurden. HA ist deaktiviert.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis node4 wieder hochfährt.

Schritte

1. bringen sie node4 auf.
2. Verschiebung der verbleibenden Aggregate, die zu node2 gehörten, durch erneute Fertigstellung "Schritt 1" Bis "Schritt 3" In *Verschiebung der nicht-Root-Aggregate von node2 nach node4*.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------   --------- -----------------
node1    node2      false     Unknown
node2    node1      false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder Panic:

```
cluster::> storage failover show

                    Takeover
Node      Partner   Possible  State Description
-------  --------  --------- -----------------
node1     node2     -         Unknown
node2     node1     false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports „ausgefallen“ ist.

LIFs befinden sich bei ungültigen Ports nach dem Upgrade

Nach Abschluss des Upgrades befinden sich die logischen FC-Schnittstellen (LIFs) bei einer MetroCluster-Konfiguration möglicherweise auf falschen Ports. Sie können einen Neusynchronisierung durchführen, um die LIFs den richtigen Ports zuzuweisen.

Schritt

1. Geben Sie das ein `metrocluster vserver resync` Befehl zum Neuzuweisen der LIFs zu den richtigen Ports.

   ```
   metrocluster vserver resync -vserver vserver_name fcp-mc.headupgrade.test.vs
   ```

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.

Inhalt	Beschreibung
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.

Inhalt	Beschreibung
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe", Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.

Manuelles Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version

Überblick

Dieses Verfahren beschreibt das Upgrade der Controller-Hardware mithilfe von Aggregate Relocation (ARL) für die folgenden Systemkonfigurationen:

Methode	ONTAP-Version	Unterstützte Systeme
Manuelles Upgrade mit ARL	9.7 oder früher	• FAS System zu FAS System • FAS System auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System • AFF System zu AFF System • System mit FlexArray Virtualisierungssoftware oder einem V-Series System auf einem FAS System, vorausgesetzt, dass das System mit FlexArray Virtualisierungssoftware oder V-Series System keine Array-LUNs besitzt. • V-Series Systeme auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System

Während des Verfahrens führen Sie ein Upgrade der ursprünglichen Controller Hardware mit der Ersatz-Controller-Hardware durch. Hierbei werden die Eigentumsrechte an Aggregaten verschoben, die nicht mit Root-Berechtigungen verbunden sind. Sie migrieren Aggregate mehrmals von Node zu Node, um zu bestätigen, dass mindestens ein Node während des Upgrades Daten von den Aggregaten bereitstellt. Außerdem migrieren Sie Daten-logische Schnittstellen (LIFs) und weisen Sie die Netzwerk-Ports auf dem neuen Controller den Schnittstellengruppen zu, während Sie fortfahren.

In diesem Dokument werden die ursprünglichen Knoten *node1* und *node2* genannt, und die neuen Knoten werden *node3* und *node4* genannt. Während des beschriebenen Verfahrens wird node1 durch node3 ersetzt und node2 durch node4 ersetzt. Die Begriffe *node1*, *node2*, *node3* und *node4* werden nur verwendet, um zwischen den ursprünglichen und neuen Knoten zu unterscheiden. Wenn Sie das Verfahren befolgen, müssen Sie die richtigen Namen Ihrer ursprünglichen und neuen Knoten ersetzen. In der Realität ändern sich jedoch die Namen der Nodes nicht: node3 hat den Namen node1 und node4 hat nach dem Upgrade der Controller-Hardware den Namen node2. In diesem Dokument wird der Begriff „ Systems with FlexArray Virtualization Software_“ verwendet, um sich auf Systeme zu beziehen, die zu diesen neuen Plattformen gehören. Dabei wird der Begriff *V-Series System* verwendet, um sich auf die separaten Hardware-Systeme zu beziehen, die an Storage-Arrays angeschlossen werden können

Wichtige Informationen:

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie müssen auch lesen und verstehen, die "Richtlinien für das Controller-Upgrade mit ARL" Und das "ARL Upgrade-Workflow" Abschnitte vor Beginn der Aktualisierung.
- Bei dieser Vorgehensweise wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn bereits die Ersatz-Controller-Hardware verwendet wurde, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP in 7-Mode ausgeführt wurde.
- Mit diesem Verfahren können Sie die Controller-Hardware in Clustern mit mehr als zwei Nodes aktualisieren. Sie müssen jedoch für jedes Hochverfügbarkeitspaar (HA) im Cluster separat vorgehen.
- Dieses Verfahren gilt für FAS Systeme, V-Series Systeme, AFF Systeme und Systeme mit FlexArray Virtualisierungssoftware. FAS Systeme, die nach ONTAP 9 freigegeben wurden, können an Speicher-Arrays angebunden werden, wenn die erforderliche Lizenz installiert ist. Die vorhandenen Systeme der V-Serie werden von ONTAP 9 unterstützt. Informationen zu den Modellen Storage Array und V-Series finden Sie unter "Quellen" Um zu *Hardware Universe* zu verlinken und eine Support-Matrix zur *V-Serie* zu erhalten.
- Dieses Verfahren gilt für MetroCluster Konfigurationen mit vier und acht Nodes und ONTAP 9.5 und früher. Weitere Informationen zu MetroCluster Konfigurationen mit ONTAP 9.6 und höher finden Sie unter "Quellen" Verknüpfung mit den Befehlen „System Controller Replace“ zum Aktualisieren der Controller-Hardware, die ONTAP 9.5 auf ONTAP 9.7_ ausführt.

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

In diesem Inhalt wird beschrieben, wie Sie die Storage Controller in einem HA-Paar mit neuen Controllern aktualisieren und dabei alle vorhandenen Daten und Festplatten beibehalten. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Verwenden Sie diese Inhalte unter folgenden Umständen:

- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind in der Verwaltung von ONTAP erfahren und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.
- Sie verfügen über ein System, bei dem Fabric MetroCluster Konfigurationen mit 4 und 8 Nodes mit ONTAP 9.5 oder einer älteren Version verwendet werden.

Dabei können Sie NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) verwenden.

Wenn Sie eine andere Methode zum Upgrade der Controller-Hardware bevorzugen und bereit sind, Volume-Verschiebungen durchzuführen, lesen Sie "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Siehe "Quellen" Zum Link zum Dokumentationszentrum *ONTAP 9*, wo Sie auf die Produktdokumentation zu ONTAP 9 zugreifen können.

ARL Upgrade-Workflow

Bevor Sie die Nodes mit ARL aktualisieren, sollten Sie unbedingt verstehen, wie das Verfahren funktioniert. In diesem Dokument wird das Verfahren in mehrere Phasen unterteilt.

Aktualisieren Sie das Node-Paar

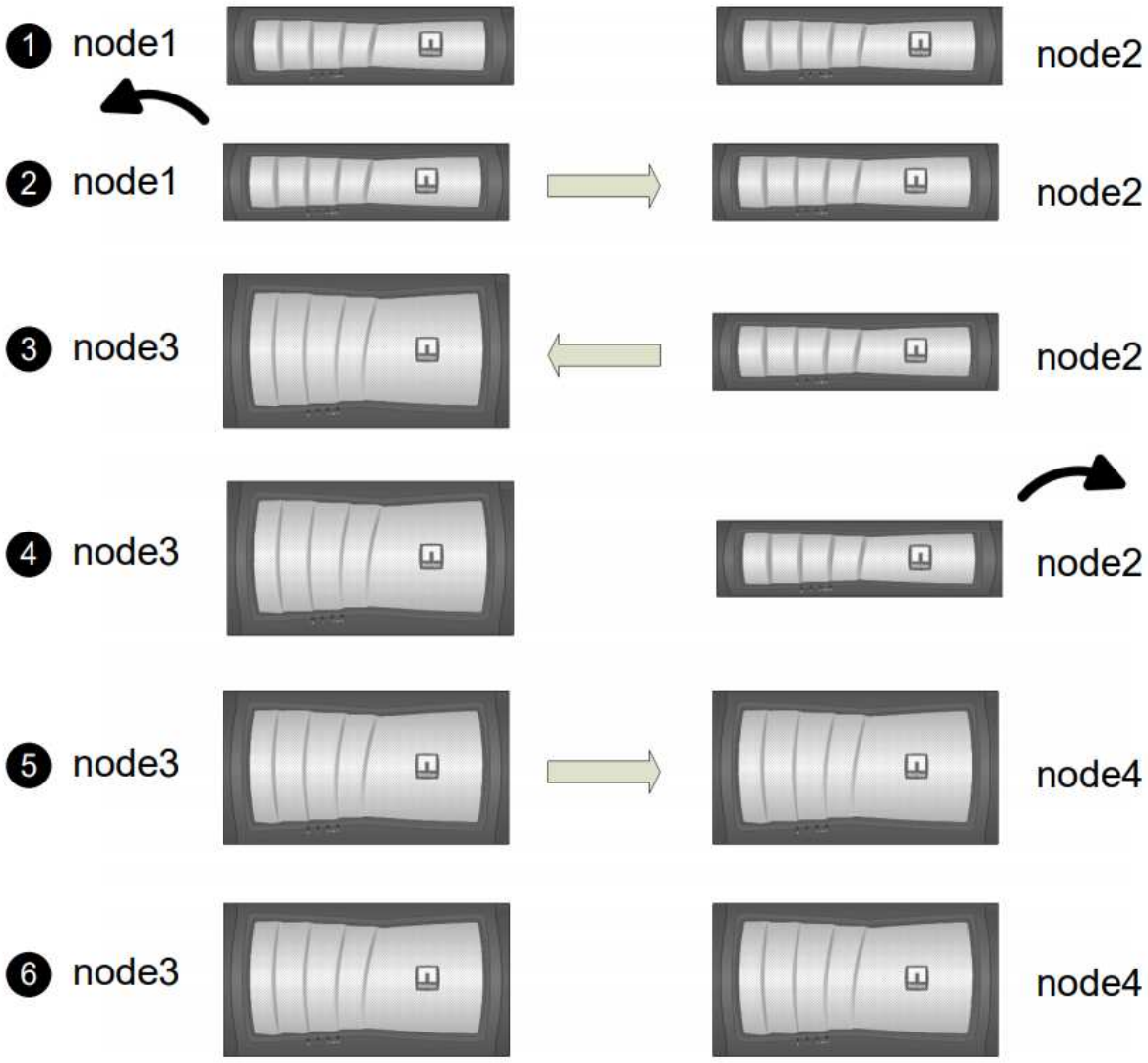
Zum Upgrade des Node-Paars müssen Sie die ursprünglichen Nodes vorbereiten und anschließend eine Reihe von Schritten sowohl auf den ursprünglichen als auch auf den neuen Nodes durchführen. Anschließend können Sie die ursprünglichen Knoten außer Betrieb nehmen.

Übersicht über die ARL-Upgrade-Sequenz

Während des Verfahrens aktualisieren Sie die ursprüngliche Controller Hardware mit der Ersatz-Controller-Hardware, einem Controller gleichzeitig. Nutzen Sie die HA-Paar-Konfiguration, um das Eigentum von Aggregaten ohne Root-Berechtigungen zu verschieben. Alle Aggregate außerhalb der Root-Ebene müssen zwei Umlagerungen durchlaufen, um das endgültige Ziel zu erreichen, nämlich den korrekten aktualisierten Node.

Jedes Aggregat hat einen Hausbesitzer und aktuellen Eigentümer. Der Hausbesitzer ist der eigentliche Eigentümer des Aggregats, und der aktuelle Eigentümer ist der temporäre Eigentümer.

Die folgende Abbildung zeigt die Phasen des Verfahrens. Die dicken, hellgrauen Pfeile stehen für die Verschiebung der Aggregate und die Verschiebung der LIFs. Die dünneren schwarzen Pfeile stellen die Entfernung der ursprünglichen Nodes dar. Die kleineren Controller Images stellen die ursprünglichen Nodes dar und die größeren Controller Images repräsentieren die neuen Nodes.



Die folgende Tabelle beschreibt die grundlegenden Aufgaben, die Sie in den einzelnen Phasen ausführen, und den Zustand der Aggregateigentümer am Ende der Phase. Detaillierte Schritte sind im weiteren Verlauf des Verfahrens aufgeführt:

Stufe	Beschreibung
"Phase 1: Upgrade vorbereiten"	In Phase 1 bestätigen Sie, dass interne Festplatten keine Root-Aggregate oder Datenaggregate enthalten, die Nodes für das Upgrade vorbereiten und mehrere Vorabprüfungen durchführen. Gegebenenfalls können Sie Festplatten für die Storage-Verschlüsselung neu verschlüsseln und die neuen Controller in Vorbereitung nehmen. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate. • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate.
"Stufe 2: Node1 ausmustern"	Während Phase 2 verschieben Sie Aggregate ohne Root-Root-Fehler von Knoten1 auf Knoten2 und verschieben Daten-LIFs, die nicht-SAN-Daten-LIFs gehören, die sich im Besitz von node1 befinden, auf Knoten 2, einschließlich fehlgeschlagener oder Vetos. Sie notieren die nötigen Node1-Informationen, die später im Verfahren verwendet werden müssen, und setzen dann Node1 aus. Gesamteigentum am Ende von Phase 2: • Node1 ist der Hausbesitzer von node1 Aggregaten. • Node2 ist der aktuelle Besitzer von node1 Aggregaten. • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten.
"Phase 3: Installieren und booten node3"	In Phase 3 installieren und booten Sie Node3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu, überprüfen die Installation und verschieben Daten-LIFs und SAN-LIFs, die zu node1 gehören, von node2 auf node3. Außerdem werden alle Aggregate von node2 auf node3 verschoben und die Daten-LIFs und SAN-LIFs von node2 auf node3 verschoben. Gesamteigentum am Ende von Stufe 3: • Node2 ist der Hausbesitzer von node2 Aggregate, aber nicht der aktuelle Eigentümer. • Node3 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehören. • Node2 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die zu node2 gehören, aber nicht der Hausbesitzer.

Stufe	Beschreibung
"Stufe 4: Außer Dienst 2"	Während Phase 4 notieren Sie die nötigen Node2-Informationen, die später im Verfahren verwendet werden sollen, und nehmen dann die Node2-Daten in den Ruhestand. Es findet keine Änderungen am Aggregateigentum statt.
"Phase 5: Installieren und booten node4"	In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 nach node4 zu, überprüfen die installation von node4 und verschieben Daten-LIFs und SAN-LIFs, die zu node2 gehören, von node3 auf node4. Außerdem werden node2-Aggregate von node3 nach node4 verschoben und die Daten-Knoten2-NAS-LIFs von node3 auf node4 verschoben. Gesamteigentum am Ende von Stufe 5: • Node3 ist der Hausbesitzer und aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Node4 ist der Hausbesitzer und aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Phase 6: Das Upgrade abschließen"	In Phase 6 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden und Storage Encryption oder NetApp Volume Encryption einrichten, wenn die neuen Nodes verschlüsselt sind. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden. ⓘ Die Disaster-Recovery-Updates für Storage Virtual Machine (SVM) werden nicht gemäß den zugewiesenen Zeitplänen unterbrochen. Es findet keine Änderungen am Aggregateigentum statt.

Richtlinien für das Controller-Upgrade mit ARL

Um zu verstehen, ob Sie bei einem Controller-Upgrade von ONTAP 9.0 bis 9.7 mit Aggregate Relocation (ARL) arbeiten können, hängt von der Plattform und der Konfiguration der ursprünglichen Controller sowie von den Ersatz-Controllern ab.

Unterstützte Upgrades für ARL

Unter den folgenden Umständen können Sie ein Upgrade eines Node-Paars mit ARL durchführen:

- Die ursprünglichen Controller und die Ersatz-Controller müssen vor dem Upgrade dieselbe Version von ONTAP 9.x ausgeführt werden.
- Die Ersatz-Controller müssen die gleiche oder eine höhere Kapazität aufweisen als die ursprünglichen Controller. Bei gleicher oder höherer Kapazität werden Attribute bezeichnet, beispielsweise die Maximalanzahl für NVRAM, Volume, LUN oder Aggregate. Er bezieht sich auch auf die maximale Volume- oder Aggregatgröße der neuen Nodes.

- Sie können die folgenden Systemtypen aktualisieren:
  - Einem FAS System auf ein FAS System.
  - Ein FAS System auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System.
  - Einem AFF System auf ein AFF System.
  - Ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System auf einem FAS System, vorausgesetzt, dass das System mit FlexArray Virtualisierungssoftware oder V-Series System keine Array-LUNs besitzt.
  - Eines V-Series Systems auf ein System mit FlexArray Virtualisierungssoftware oder einem V-Series System

> Bevor Sie ein AFF-Systemupgrade durchführen, müssen Sie ONTAP auf Version 9.3P12, 9.4P6 oder 9.5P1 oder höher aktualisieren. Diese Versionsebenen sind für ein erfolgreiches Upgrade erforderlich.

- Bei einigen Upgrades des ARL-Controllers können Sie für das Upgrade temporäre Cluster-Ports auf dem Ersatz-Controller verwenden. Wenn Sie beispielsweise je nach Konfiguration der AFF A400 ein Upgrade von einem AFF A300 auf ein AFF A400 System durchführen, können Sie einen der beiden Mezzanine-Ports verwenden oder eine 10-GbE-Netzwerkschnittstellenkarte mit vier Ports für temporäre Cluster-Ports hinzufügen. Nachdem Sie ein Controller-Upgrade über temporäre Cluster-Ports abgeschlossen haben, können Sie Cluster unterbrechungsfrei zu 100-GbE-Ports auf dem Ersatz-Controller migrieren.
- Wenn Sie ONTAP 9.6P11, 9.7P8 oder neuere Versionen verwenden, wird empfohlen, die Aktivierung von Connectivity, Lebendigkeit und Availability Monitor (CLAM)-Übernahme zu aktivieren, um das Cluster bei bestimmten Node-Ausfällen in Quorum zurückzugeben. Der `kernel-service` Für Befehl ist der erweiterte Zugriff auf die Berechtigungsebene erforderlich. Weitere Informationen finden Sie unter: "NetApp KB-Artikel SU436: DIE CLAM-Übernahme hat sich die Standardkonfiguration geändert".
- Das Controller-Upgrade mit ARL wird auf Systemen unterstützt, die mit SnapLock Enterprise und SnapLock Compliance Volumes konfiguriert sind.

Sie müssen überprüfen, ob der ARL-Vorgang auf den Original- und Ersatz-Controllern ausgeführt werden kann. Sie müssen die Größe aller definierten Aggregate und die Anzahl der Festplatten überprüfen, die vom ursprünglichen System unterstützt werden. Vergleichen Sie dann die aggregierte Größe und Anzahl der vom neuen System unterstützten Festplatten. Informationen zum Zugriff auf diese Informationen finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*. Die Aggregatgröße und die Anzahl der vom neuen System unterstützten Festplatten müssen gleich oder größer sein als die Aggregatgröße und Anzahl der vom ursprünglichen System unterstützten Festplatten.

Sie müssen in den Cluster-Mischregeln validieren, ob neue Nodes zusammen mit den vorhandenen Nodes Teil des Clusters werden können, wenn der ursprüngliche Controller ersetzt wird. Weitere Informationen zu Regeln für die Kombination von Clustern finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

> Beide Systeme sind entweder hochverfügbarkeits- (HA) oder kein HA-System. Beide Nodes müssen entweder die Persönlichkeit aktiviert oder deaktiviert sein. Sie können einen Node nicht mit der All-Flash-optimierten Persönlichkeit kombinieren, die bei einem Node aktiviert ist, der nicht im gleichen HA-Paar die Persönlichkeit aktiviert hat. Wenn sich die Persönlichkeiten unterscheiden, wenden Sie sich an den technischen Support.

> Wenn das neue System weniger Steckplätze als das ursprüngliche System besitzt oder weniger oder unterschiedliche Ports vorhanden sind, müssen Sie dem neuen System möglicherweise einen Adapter hinzufügen. Siehe "Quellen" Link zum *Hardware Universe* auf der NetApp Support-Website, um Informationen zu bestimmten Plattformen zu erhalten.

Upgrades werden für ARL nicht unterstützt

Sie können die folgenden Aktualisierungen nicht ausführen:

- Zu bzw. von Controllern, die keine ONTAP Version von ONTAP 9.0 auf ONTAP 9.7 ausführen können

  Informationen zu Controller-Upgrades für Systeme mit Data ONTAP 7-Mode finden Sie unter "Quellen" Link zur NetApp Support Site_.

- Zum Austausch von Controllern, die die mit den ursprünglichen Controllern verbundenen Platten-Shelfs nicht unterstützen.

  Informationen zur Unterstützung von Festplatten finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

- Von Controllern mit Root-Aggregaten oder Datenaggregaten auf internen Laufwerken.

  Wenn Sie Controller mit Root-Aggregaten oder Datenaggregaten auf internen Festplattenlaufwerken aktualisieren möchten, lesen Sie "Quellen" Link zu *Upgrade durch Verschiebung von Volumes oder Storage* und Vorgang *Upgrade eines Node-Paares, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.

  Wenn Sie ONTAP auf Nodes in einem Cluster aktualisieren möchten, lesen Sie "Quellen" Link zu *Upgrade ONTAP*.

Annahmen und Terminologie

Dieses Dokument wird an folgende Annahmen geschrieben:

- Die Ersatz-Controller-Hardware ist neu und wurde nicht verwendet.

  Achtung: Da dieses Verfahren davon ausgeht, dass die Hardware des Ersatzcontrollers neu ist und nicht verwendet wurde, werden die erforderlichen Schritte zur Vorbereitung gebrauchter Controller mit dem ausgeführt `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Wenn bereits die Ersatz-Controller-Hardware verwendet wurde, müssen Sie sich an den technischen Support wenden, insbesondere wenn auf den Controllern Data ONTAP in 7-Mode ausgeführt wurde.

- Die Richtlinien zum Upgrade des Knotenpaars werden gelesen und verstanden.

  Achtung: Versuchen Sie nicht, den NVRAM-Inhalt zu löschen. Wenn Sie den Inhalt des NVRAM löschen müssen, wenden Sie sich an den technischen Support von NetApp.

- Sie führen den entsprechenden Befehl vor und nach dem aus `modify` Und die Ausgabe von beiden vergleichen `show` Befehle, um zu überprüfen, dass das `modify` Befehl erfolgreich.
- Wenn Sie über eine SAN-Konfiguration verfügen, stehen Ihnen auf dem HA-Paar lokale LIFs und Partner-LIFs für jede Storage Virtual Machine (SVM) zur Verfügung. Wenn Sie keine lokalen LIFs für jede SVM haben und keine Partner-LIFs haben, sollten Sie vor dem Upgrade die SAN-Daten-LIF auf dem Remote- und lokalen Node für diese SVM hinzufügen.
- Wenn Sie in einer SAN-Konfiguration Port-Sets haben, müssen Sie überprüfen, dass jeder gebundene Port-Satz mindestens eine LIF von jedem Node im HA-Paar enthält.

Bei diesem Verfahren wird der Begriff „*Boot Environment prompt*“ verwendet, um die Eingabeaufforderung auf einem Node, von dem Sie bestimmte Aufgaben ausführen können, zu lesen, z. B. beim Neubooten des Knotens und beim Drucken oder Festlegen von Umgebungsvariablen. Die Eingabeaufforderung wird manchmal informell als *Boot-Loader Prompt* bezeichnet.

Die Eingabeaufforderung der Boot-Umgebung wird im folgenden Beispiel angezeigt:

```
LOADER>
```

Lizenzierung nach ONTAP 9.7 oder früher

Einige Funktionen erfordern Lizenzen, die als *Packages* ausgegeben werden, die eine oder mehrere Funktionen enthalten. Jeder Node im Cluster muss über seinen eigenen Schlüssel für jede Funktion im Cluster verfügen.

Wenn Sie keine neuen Lizenzschlüssel haben, sind für den neuen Controller derzeit lizenzierte Funktionen im Cluster verfügbar und funktionieren weiterhin. Durch die Verwendung nicht lizenzierter Funktionen auf dem Controller können Sie jedoch möglicherweise die Einhaltung Ihrer Lizenzvereinbarung verschließen. Sie müssen daher nach Abschluss des Upgrades den neuen Lizenzschlüssel oder die neuen Schlüssel für den neuen Controller installieren.

Alle Lizenzschlüssel sind 28 Groß-alphabetische Zeichen lang. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken, wo Sie neue 28-stellige Lizenzschlüssel für ONTAP 9.7 erhalten. Oder früher. Die Schlüssel sind im Abschnitt „*My Support*“ unter „*Software licenses*“ verfügbar. Falls auf der Website keine Lizenzschlüssel vorhanden ist, wenden Sie sich an Ihren NetApp Ansprechpartner.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Storage-Verschlüsselung

Die ursprünglichen oder die neuen Nodes sind möglicherweise für die Storage-Verschlüsselung aktiviert. In diesem Fall müssen Sie in diesem Verfahren weitere Schritte durchführen, um zu überprüfen, ob die Speicherverschlüsselung ordnungsgemäß eingerichtet ist.

Falls Sie Storage Encryption verwenden möchten, müssen alle dem Node zugeordneten Festplattenlaufwerke über Self-Encrypting Drives verfügen.

2-Node-Cluster ohne Switches

Wenn Sie Nodes in einem 2-Node-Cluster ohne Switches aktualisieren, können Sie die Nodes im Cluster ohne Switches während des Upgrades belassen. Sie müssen sie nicht in ein Switch-Cluster konvertieren.

Fehlerbehebung

Dieses Verfahren enthält Vorschläge zur Fehlerbehebung.

Falls beim Upgrade der Controller Probleme auftreten, finden Sie weitere Informationen im "Fehlerbehebung" Abschnitt am Ende des Verfahrens für weitere Informationen und mögliche Lösungen.

Wenn Sie keine Lösung für das Problem finden, wenden Sie sich an den technischen Support.

Die erforderlichen Tools und Dokumentationen

Sie müssen über spezielle Tools verfügen, um die neue Hardware zu installieren, und Sie müssen während des Upgrade-Prozesses andere Dokumente referenzieren. Sie müssen außerdem die für das Controller-Upgrade wichtigen Informationen aufzeichnen. Zum Aufzeichnen von Informationen wird ein Arbeitsblatt bereitgestellt.

Für die Durchführung des Upgrades benötigen Sie die folgenden Tools:

- Erdungsband
- #2 Kreuzschlitzschraubendreher

Wechseln Sie zum "Quellen" Abschnitt für den Zugriff auf die Liste der für dieses Upgrade erforderlichen Referenzdokumente.

Worksheet: Zu erfassend vor und während des Controller-Upgrades

Sie sollten bestimmte Informationen sammeln, um das Upgrade der ursprünglichen Nodes zu unterstützen. Diese Informationen umfassen Node-IDs, Port- und LIF-Details, Lizenzschlüssel und IP-Adressen.

Sie können das folgende Arbeitsblatt verwenden, um die Informationen für eine spätere Verwendung im Verfahren aufzuzeichnen:

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
Modell, System-ID, Seriennummer der ursprünglichen Nodes	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Phase 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4* Stufe 6: *Decommission das alte System*	
Shelf- und Festplatteninformationen, Flash Storage-Details, Arbeitsspeicher, NVRAM und Adapterkarten auf den ursprünglichen Nodes	Phase 1: *Vorbereiten der Knoten für das Upgrade*	Während des gesamten Verfahrens	
Online-Aggregate und Volumes auf den ursprünglichen Nodes	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Während des gesamten Verfahrens zur Überprüfung, ob Aggregate und Volumes online bleiben, außer bei kurzen Standortverlagerungen	
Ausgabe von Befehlen `network port vlan show` Und `network port ifgrp show`	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 3: *Map Ports von node1 nach node3* Stufe 5: *Map Ports von node2 nach node4*	

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
(Nur SAN-Umgebungen) Standardkonfiguration von FC-Ports	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Beim Konfigurieren von FC-Ports auf den neuen Nodes	
(Systeme der V-Series oder Systeme mit FlexArray-Virtualisierungssoftware) Topologie für V-Series Systeme oder Systeme mit FlexArray Virtualisierungssoftware	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4*	
IP-Adresse der SPs	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 6: *Bestätigen Sie, dass die neuen Controller korrekt eingerichtet sind*	
Lizenzschlüssel	Phase 1: *Die Nodes für das Upgrade vorbereiten*	Stufe 6: *Bestätigen Sie, dass die neuen Controller korrekt eingerichtet sind*	
IP-Adresse für den externen Schlüsselverwaltungsserver	Phase 1: *Rekey Disks für Speicherverschlüsselung*	Phase 6: *Storage Encryption auf den neuen Nodes einrichten*	
Name und Pfad des per Web zugänglichen Verzeichnisses, bei dem Sie Dateien auf die Nodes als Netzboot herunterladen	Stufe 1: *Netzboot vorbereiten*	Stufe 3: *Installieren und Booten node3* Stufe 5: *Installieren und Booten von node4*	
LIFs für nicht-SAN-Daten im Besitz von Node1	Phase 2: *Verschieben Sie nicht-SAN-logische Datenschnittstellen von node1 auf node2*	Später im Abschnitt	
Cluster, Intercluster, Node-Management, Cluster-Management und physische Ports	Phase 2: *Node1-Informationen aufzeichnen*	Stufe 3: *Installieren und Booten node3* Stufe 3: *Kartenanschlüsse von node1 nach node3*	
Ports auf neuen Nodes	Phase 3: *Map Ports von node1 nach node3*	Später im Abschnitt und im Abschnitt *Kartenanschlüsse von node2 nach node4*	
Verfügbare Ports und Broadcast-Domänen auf Knoten 3	Phase 3: *Map Ports von node1 nach node3*	Später im Abschnitt	

Erforderliche Informationen	Wenn erfasst	Wenn verwendet	Erfassten Informationen Fertigzustellen
Logische Schnittstellen (Non-SAN) sind nicht im Besitz von node2	*Verschieben von LIFs für nicht-SAN-Daten, die zu node1 von node2 zu node3 gehören und SAN-LIFs auf node3* überprüfen	Später im Abschnitt	
LIFs für nicht-SAN-Daten im Besitz von node2	Phase 3: *Verschieben Sie nicht-SAN-logische Datenschnittstellen von node2 auf node3*	Später im Abschnitt	
Cluster, Intercluster, Node-Management, Cluster-Management und physische Ports	Stufe 4: *Node2-Informationen aufzeichnen*	Stufe 5: *Installation und Booten von node4* Stufe 5:_ Kartenanschlüsse von node2 nach node4_	
Cluster-Netzwerk-Ports auf node4	Stufe 5: *Map Ports von node2 nach node4*	Später im Abschnitt	
Verfügbare Ports und Broadcast-Domänen auf node4	Stufe 5: *Map Ports von node2 nach node4*	Später im Abschnitt	
Private und öffentliche SSL-Zertifikate für das Storage-System und private SSL-Zertifikate für jeden Schlüsselmanagementserver	Phase 6: *Storage Encryption auf den neuen Nodes einrichten*	Später im Abschnitt	

Konfigurieren Sie das FC-Switch-Layout für ONTAP 9.1 oder höher neu

Konfigurieren Sie das FC-Switch-Layout für ONTAP 9.1 oder höher neu

Wenn das vorhandene FC-Switch-Layout vor ONTAP 9.1 konfiguriert wurde, müssen Sie das Port-Layout neu konfigurieren und die neuesten RCFs (Reference Configuration Files) anwenden. Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen.

Bevor Sie beginnen

Sie müssen die in der Fabric-Domäne vorhandenen FC-Switches identifizieren.

Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

Über diese Aufgabe

Sie müssen diese Aufgabe ausführen, wenn Ihr vorhandenes FC Switch-Layout vor ONTAP 9.1 konfiguriert wurde und Sie ein Upgrade auf ein in ONTAP 9.1 oder höher unterstütztes Plattformmodell durchführen. Dies ist *nicht* erforderlich, wenn Sie ein Upgrade von einem vorhandenen Switch-Layout durchführen, das für ONTAP 9.1 oder höher konfiguriert wurde.

Dieser Vorgang läuft unterbrechungsfrei ab und dauert etwa vier Stunden (außer Rack und Stack), wenn Festplatten gelöscht werden.

Schritte

1. "Senden Sie vor der Neukonfiguration der Switches eine benutzerdefinierte AutoSupport Meldung"
2. "Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration"
3. "Prüfen Sie auf MetroCluster-Konfigurationsfehler"
4. "Deaktivieren Sie die Switches dauerhaft"
5. "Bestimmen Sie das neue Verkabelungslayout"
6. "Wenden Sie RCF-Dateien an und stellen Sie die Schalter wieder ein"
7. "Die Switches dauerhaft aktivieren"
8. "Überprüfung von UmschalttaFunktionen, Healing und Switchback"

Senden Sie vor der Neukonfiguration der Switches eine benutzerdefinierte AutoSupport Meldung

Bevor Sie Ihre Switches neu konfigurieren, müssen Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über laufende Wartungsarbeiten 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` Wert 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.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Sie sollten den Systemzustand der MetroCluster-Konfiguration überprüfen, um den korrekten Betrieb zu überprüfen.

Schritte

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

   `metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2017 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.
```

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

   ```
   system health alert show
   ```

Prüfen Sie auf MetroCluster-Konfigurationsfehler

Sie können das Active IQ Config Advisor Tool auf der NetApp Support-Website verwenden, um häufige Konfigurationsfehler zu überprüfen.

Wenn Sie keine MetroCluster-Konfiguration haben, können Sie diesen Abschnitt überspringen.

Über diese Aufgabe

Active IQ 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.

1. Laden Sie die herunter "Active IQ Config Advisor" Werkzeug.
2. Führen Sie Active IQ Config Advisor aus, überprüfen Sie die Ausgabe und folgen Sie seinen Empfehlungen, um eventuelle Probleme zu beheben.

Die Schalter werden persistenz deaktiviert

Sie müssen die Switches in der Fabric dauerhaft deaktivieren, damit Sie seine Konfiguration ändern können.

Über diese Aufgabe

Sie deaktivieren die Switches, indem Sie die Befehle in der Switch-Befehlszeile ausführen. Die dafür

verwendeten Befehle sind keine ONTAP-Befehle.

Schritt

Deaktivieren Sie den Switch dauerhaft:

- Verwenden Sie für Brocade-Switches den `switchCfgPersistentDisable` Befehl.
- Verwenden Sie für Cisco Switches das `suspend` Befehl.

Mit dem folgenden Befehl wird ein Brocade Switch dauerhaft deaktiviert:

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

Mit dem folgenden Befehl wird ein Cisco-Switch deaktiviert:

```
vsan [vsna #] suspend
```

Bestimmen Sie das neue Verkabelungslayout

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.

Schritt

Ermitteln Sie mithilfe des Inhalts *Fabric-Attached MetroCluster Installation and Configuration* das Verkabelungslayout für Ihren Switch-Typ. Verwenden Sie dabei die Portnutzung für eine MetroCluster-Konfiguration mit acht Nodes. Die Nutzung des FC-Switch-Ports muss der in dem Inhalt beschriebenen Nutzung entsprechen, sodass die Referenzkonfigurationsdateien (RCFs) verwendet werden können.

Gehen Sie zu "Quellen" Zum Verlinken auf den Content *Fabric-Attached MetroCluster Installation and Configuration*.

> Wenn Ihre Umgebung nicht so verkabelt werden kann, wie RCFs verwendet werden können, wenden Sie sich an den technischen Support. Verwenden Sie dieses Verfahren nicht, wenn die Verkabelung keine RCFs verwenden kann.

Wenden Sie RCF-Dateien an und stellen Sie die Schalter wieder ein

Sie müssen die entsprechenden Referenzkonfigurationsdateien (RCfs) anwenden, um Ihre Switches neu zu konfigurieren, damit sie die neuen Nodes aufnehmen können. Nachdem Sie die RCFs angewendet haben, können Sie die Schalter umschalten.

Bevor Sie beginnen

Die Verwendung des FC-Switch-Ports muss mit der in der Installation and Configuration_-Inhaltsanweisung *Fabric-Attached MetroCluster beschriebenen Nutzung übereinstimmen, damit die RCFs verwendet werden können. Gehen Sie zu "Quellen" Zum Verlinken auf den Content _Fabric-Attached MetroCluster Installation and Configuration*.

Schritte

1. Wechseln Sie zum "MetroCluster RCF-Downloads" Wählen Sie die RCFs für Ihre Switch-Konfiguration aus.

   Sie müssen die RCFs verwenden, die zu Ihren Switch-Modellen passen.

2. Installieren Sie die FC-Switch-RCFs, indem Sie das Verfahren auswählen, das Ihren Switch-Modellen entspricht, und befolgen Sie die Installationsanweisungen:
   - "Installieren Sie einen Brocade FC-Switch RCF"
   - "Installieren Sie einen Cisco FC-Switch RCF"
3. Vergewissern Sie sich, dass die Switch-Konfiguration gespeichert ist.
4. Verkabeln Sie beide FC-to-SAS-Bridges mithilfe des in erstellten Verkabelungslayouts zu den FC-Switches "Bestimmen Sie das neue Verkabelungslayout".
5. Vergewissern Sie sich, dass die Ports online sind:
   - Verwenden Sie für Brocade-Switches den `switchshow` Befehl.
   - Verwenden Sie für Cisco-Switches die Show `interface brief` Befehl.
6. Verkabeln Sie die FC-VI-Ports von den Controllern mit den Switches.
7. Vergewissern Sie sich von den vorhandenen Nodes, dass die FC-VI-Ports online sind:

   ```
   metrocluster interconnect adapter show

   metrocluster interconnect mirror show
   ```

Die Switches dauerhaft aktivieren

Sie müssen die Switches im Fabric dauerhaft aktivieren.

Schritt

Dauerhaft aktivieren Sie den Switch:

- Verwenden Sie für Brocade-Switches den `switchCfgPersistentenable` Befehl.

  ```
  FC_switch_A_1:admin> switchCfgPersistentenable
  ```

- Verwenden Sie für Cisco Switches das `no suspend` Befehl.

  ```
  vsan [vsna #]no suspend
  ```

Überprüfung von UmschalttaFunktionen, Healing und Switchback

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

Schritt

Siehe "Quellen" Verbinden mit Inhalten für *MetroCluster Management and Disaster Recovery* und Befolgen der Verfahren für ausgehandelte Umschaltung, Heilung und Umschalten.

Stufe 1: Upgrade vorbereiten

Phase 1 – Übersicht

In Phase 1 bestätigen Sie, dass interne Festplatten keine Root-Aggregate oder Datenaggregate enthalten, die Nodes für das Upgrade vorbereiten und mehrere Vorabprüfungen durchführen. Unter Umständen müssen Sie auch Festplatten für die Storage-Verschlüsselung rekeysen und die neuen Controller als Netzboot vorbereiten.

Schritte

1. "Ermitteln Sie, ob der Controller über Aggregate auf internen Festplatten verfügt"
2. "Bereiten Sie die Knoten für ein Upgrade vor"
3. "Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager"
4. "SnapMirror Beziehungen stilllegen"
5. "Vorbereitungen für den Netzboot"

Ermitteln Sie, ob der Controller über Aggregate auf internen Festplatten verfügt

Wenn Sie Controller mit internen Festplatten aktualisieren, müssen Sie mehrere Befehle ausführen und deren Ausgabe überprüfen, um zu bestätigen, dass keines der internen Festplatten Root-Aggregate oder Datenaggregate enthält.

Über diese Aufgabe

Wenn Sie Controller nicht mit Aggregaten auf internen Festplatten aktualisieren, lassen Sie diesen Abschnitt überspringen und fahren Sie mit dem Abschnitt fort "Bereiten Sie die Knoten für ein Upgrade vor".

Schritte

1. Geben Sie die nodeshell, einmal für jeden der ursprünglichen Knoten.

   ```
   system node run -node node_name
   ```

2. Anzeigen der internen Laufwerke:

   ```
   sysconfig -av
   ```

   Das System zeigt ausführliche Informationen über die Konfiguration des Node, einschließlich Storage, an. Diese Informationen werden in der im folgenden Beispiel gezeigten Teilausgabe angezeigt:

```
node> sysconfig -av
slot 0: SAS Host Adapter 0a (PMC-Sierra PM8001 rev. C, SAS, UP)
                Firmware rev: 01.11.06.00
                 Base WWN: 5:00a098:0008a3b:b0
                 Phy State: [0] Enabled, 6.0 Gb/s
                            [1] Enabled, 6.0 Gb/s
                            [2] Enabled, 6.0 Gb/s
                            [3] Enabled, 6.0 Gb/s
                ID Vendor Model FW Size
                00.0 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.1 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.2 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.3 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.4 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.5 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.6 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.7 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.8 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.9 : NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.10: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
                00.11: NETAPP X306_HMARK02TSSM NA04 1695.4GB (3907029168
512B/sect)
...
```

3. Untersuchen Sie die Speicherausgabe des `sysconfig -av` Befehl, um die internen Festplattenlaufwerke zu identifizieren, und notieren Sie dann die Informationen.

   Interne Laufwerke haben "00." zu Beginn ihrer ID. „00.“ gibt ein internes Festplatten-Shelf an, und die Zahl nach dem Dezimalpunkt gibt das einzelne Festplattenlaufwerk an.

4. Geben Sie auf beiden Controllern den folgenden Befehl ein:

   `aggr status -r`

   Das System zeigt den Aggregatstatus des Node an, wie in der Teilausgabe im folgenden Beispiel dargestellt:

```
node> aggr status -r
Aggregate aggr2 (online, raid_dp, parity uninit'd!) (block checksums)
Plex /aggr2/plex0 (online, normal, active)
RAID group /aggr2/plex0/rg0 (normal, block checksums)

RAID Disk Device    HA SHELF BAY CHAN Pool Type RPM  Used (MB/blks)
Phys (MB/blks)
--------- --------- -- ----- --- ---- ---- ---- ---- ------------------
------------------
dparity   0a.00.1   0a   0    1  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
parity    0a.00.3   0a   0    3  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
data      0a.00.9   0a   0    9  SA:B  0   BSAS 7200 1695466/3472315904
1695759/3472914816
...
```

Das Gerät, das zum Erstellen des Aggregats verwendet wird, ist möglicherweise keine physische Festplatte, sondern möglicherweise eine Partition.

5. Überprüfen Sie die Ausgabe des `aggr status -r` Befehl, um die Aggregate mithilfe interner Festplatten zu identifizieren und dann die Informationen aufzuzeichnen.

   Im Beispiel im vorherigen Schritt verwendet „aggr2“ interne Laufwerke, wie durch die Shelf-ID von „0“ angegeben.

6. Geben Sie bei beiden Controllern den folgenden Befehl ein:

   ```
   aggr status -y
   ```

   Das System zeigt Informationen zu den Volumes auf dem Aggregat an, wie in der teilweise Ausgabe im folgenden Beispiel dargestellt:

```
node> aggr status -v
...
 aggr2   online   raid_dp, aggr    nosnap=off, raidtype=raid_dp,
raidsize=14,
                  64-bit           raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off, resyncsnaptime=60,
                                   fs_size_fixed=off,
lost_write_protect=on,
                                   ha_policy=cfo, hybrid_enabled=off,
percent_snapshot_space=0%,
                                   free_space_realloc=off, raid_cv=on,
thorough_scrub=off
         Volumes: vol6, vol5, vol14
...
 aggr0   online   raid_dp, aggr    root, diskroot, nosnap=off,
raidtype=raid_dp,
                  64-bit           raidsize=14, raid_lost_write=on,
ignore_inconsistent=off,
                  rlw_on           snapmirrored=off,  resyncsnaptime=60,
fs_size_fixed=off,
                                   lost_write_protect=on, ha_policy=cfo,
hybrid_enabled=off,
                                   percent_snapshot_space=0%,
free_space_realloc=off, raid_cv=on
         Volumes: vol0
```

Basierend auf der Ausgabe in Schritt 4 Schritt 6 verwendet aggr2 drei interne Laufwerke – „0a.00.1“, „0a.00.3“ und „0a.00.9“ – und die Volumes auf „aggr2“ sind „vol6“, „vol5“ und „vol14“. Auch in der Ausgabe von Schritt 6 enthält die Auslesung für „aggr0“ das Wort „root“ am Anfang der Information für das Aggregat. Das bedeutet, dass es ein Root-Volume enthält.

7. Überprüfen Sie die Ausgabe des `aggr status -v` Befehl zur Ermittlung der Volumes, die zu beliebigen Aggregaten gehören, die sich auf einem internen Laufwerk befinden und ob eines dieser Volumes ein Root-Volume enthalten soll
8. Beenden Sie den nodeshell, indem Sie auf jedem Controller den folgenden Befehl eingeben:

   `exit`

9. Führen Sie eine der folgenden Aktionen durch:

Wenn die Controller	Dann…
Enthalten keine Aggregate auf internen Festplatten	Fahren Sie mit diesem Verfahren fort.

Wenn die Controller	Dann…
Enthalten Aggregate, aber keine Volumes auf den internen Festplattenlaufwerken	Fahren Sie mit diesem Verfahren fort. Bevor Sie fortfahren, müssen Sie die Aggregate offline setzen und dann die Aggregate auf den internen Festplattenlaufwerken zerstören. Siehe "Quellen" Verbinden mit *Disk und Aggregatmanagement mit CLI* Inhalt für Informationen über das Managen von Aggregaten.
Enthalten nicht-Root-Volumes auf den internen Laufwerken	Fahren Sie mit diesem Verfahren fort. Bevor Sie fortfahren, müssen Sie die Volumes zu einem externen Festplatten-Shelf verschieben, die Aggregate offline platzieren und dann die Aggregate auf den internen Festplattenlaufwerken zerstören. Siehe "Quellen" Informationen über das Verschieben von Volumes erhalten Sie unter Verweis auf das Management von *Festplatte und Aggregaten mit dem CLI* Inhalt.
Enthalten Root-Volumes auf den internen Laufwerken	Fahren Sie mit diesem Verfahren nicht fort. Sie können ein Upgrade der Controller durchführen, indem Sie auf verweisen "Quellen" Zum Verlinken auf die *NetApp Support Site* und das Verfahren *Aktualisieren der Controller Hardware auf einem Node-Paar, auf dem Clustered Data ONTAP durch Verschieben von Volumes* ausgeführt wird.
Enthalten nicht-Root-Volumes auf den internen Laufwerken und Sie können die Volumes nicht in einen externen Speicher verschieben	Fahren Sie mit diesem Verfahren nicht fort. Sie können die Controller mithilfe des Verfahrens *aktualisieren Sie die Controller-Hardware auf einem Node-Paar, auf dem Clustered Data ONTAP ausgeführt wird, indem Sie Volumes* verschieben. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken, auf die Sie Zugriff haben.

Bereiten Sie die Knoten für ein Upgrade vor

Bevor Sie die ursprünglichen Nodes ersetzen können, müssen Sie bestätigen, dass sich die Nodes in einem HA-Paar befinden, dass keine fehlenden oder ausgefallenen Festplatten vorhanden sind, auf den Storage der jeweils anderen Nodes zugreifen können und keine Daten-LIFs besitzen, die den anderen Nodes im Cluster zugewiesen sind. Sie müssen auch Informationen über die ursprünglichen Nodes sammeln und bestätigen, dass alle Knoten im Cluster Quorum sind, wenn sich der Cluster in einer SAN-Umgebung befindet.

Schritte

1. Vergewissern Sie sich, dass jeder der ursprünglichen Nodes über ausreichende Ressourcen verfügt, um den Workload beider Nodes im Übernahmemodus angemessen zu unterstützen.

Siehe "Quellen" Um zu *High Availability Management* zu verlinken und im Abschnitt „ Best Practices für HA-Paare_“ zu folgen. Keine der ursprünglichen Nodes sollte mit einer Auslastung von über 50 % laufen. Wenn ein Node eine Auslastung von unter 50 % aufweist, kann er die Lasten für beide Nodes während des Controller-Upgrades verarbeiten.

2. Führen Sie die folgenden Teilschritte durch, um eine Performance-Baseline für die ursprünglichen Nodes zu erstellen:
   a. Stellen Sie sicher, dass das Benutzerkonto für den Diagnosebenutzer entsperrt ist.

      Das diagnostische Benutzerkonto ist nur für diagnostische Zwecke auf niedriger Ebene gedacht und sollte nur unter Anleitung durch den technischen Support verwendet werden.

      Informationen zum Entsperren der Benutzerkonten finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

   b. Siehe "Quellen" Wenn Sie einen Link zur NetApp Support-Website_ erhalten möchten, können Sie den Performance and Statistics Collector (Perfstat Converged) herunterladen.

      Mit dem konvergenten Perfstat Tool können Sie eine Performance-Baseline für den Vergleich nach dem Upgrade erstellen.

   c. Erstellen Sie eine Performance-Baseline gemäß den Anweisungen auf der NetApp Support Site.
3. Siehe "Quellen" Einen Link zur NetApp Support Site_ öffnen und einen Support-Case auf der NetApp Support Site eröffnen.

   Sie können den Fall verwenden, um eventuelle Probleme während des Upgrades zu melden.

4. Überprüfen Sie, ob NVMEM oder NVRAM-Batterien der Node3 und node4 geladen sind, und laden Sie sie, falls nicht, auf.

   Sie müssen Node 3 und node4 physisch überprüfen, um zu ermitteln, ob die NVMEM- oder NVRAM-Batterien geladen sind. Informationen zu den LEDs für das Modell node3 und node4 finden Sie unter "Quellen" Zum Verknüpfen mit der *Hardware Universe*.

   Achtung Versuchen Sie nicht, den NVRAM-Inhalt zu löschen. Wenn der Inhalt des NVRAM gelöscht werden muss, wenden Sie sich an den technischen Support von NetApp.

5. Überprüfen Sie die Version von ONTAP auf node3 und node4.

   Die neuen Knoten müssen auf ihren ursprünglichen Knoten dieselbe Version von ONTAP 9.x installiert sein. Wenn die neuen Nodes über eine andere Version der ONTAP installiert sind, müssen Sie die neuen Controller nach der Installation neu laden. Anweisungen zum Upgrade von ONTAP finden Sie unter "Quellen" Link zu *Upgrade ONTAP*.

   Informationen über die Version von ONTAP auf node3 und node4 sollten in den Versandkartons enthalten sein. Die ONTAP-Version wird angezeigt, wenn der Node hochgefahren wird oder Sie können den Node im Wartungsmodus booten und den Befehl ausführen:

   ```
   version
   ```

6. Überprüfen Sie, ob Sie zwei oder vier Cluster LIFs auf node1 und node2 haben:

```
network interface show -role cluster
```

Das System zeigt alle Cluster-LIFs an, wie im folgenden Beispiel gezeigt:

```
cluster::> network interface show -role cluster
        Logical    Status     Network          Current  Current Is
Vserver Interface  Admin/Oper Address/Mask     Node     Port    Home
------- ---------- ---------- ---------------- -------- ------- ----
node1
        clus1      up/up      172.17.177.2/24  node1    e0c     true
        clus2      up/up      172.17.177.6/24  node1    e0e     true
node2
        clus1      up/up      172.17.177.3/24  node2    e0c     true
        clus2      up/up      172.17.177.7/24  node2    e0e     true
```

7. Wenn Sie zwei oder vier Cluster LIFs auf node1 oder node2 haben, stellen Sie sicher, dass Sie beide Cluster LIFs über alle verfügbaren Pfade pingen können, indem Sie die folgenden Unterschritte ausführen:

   a. Geben Sie die erweiterte Berechtigungsebene ein:

      ```
      set -privilege advanced
      ```

      Vom System wird die folgende Meldung angezeigt:

      ```
      Warning: These advanced commands are potentially dangerous; use them
      only when directed to do so by NetApp personnel.
      Do you wish to continue? (y or n):
      ```

   b. Eingabe `y`.

   c. Pingen der Knoten und Testen der Konnektivität:

      ```
      cluster ping-cluster -node node_name
      ```

      Vom System wird eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::*> cluster ping-cluster -node node1
Host is node1
Getting addresses from network interface table...
Local = 10.254.231.102 10.254.91.42
Remote = 10.254.42.25 10.254.16.228
Ping status:
...
Basic connectivity succeeds on 4 path(s) Basic connectivity fails on 0
path(s)
................
Detected 1500 byte MTU on 4 path(s):
Local 10.254.231.102 to Remote 10.254.16.228
Local 10.254.231.102 to Remote 10.254.42.25
Local 10.254.91.42 to Remote 10.254.16.228
Local 10.254.91.42 to Remote 10.254.42.25
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

+
Wenn der Node zwei Cluster Ports verwendet, sollten Sie sehen, dass er in vier Pfaden kommunizieren kann, wie im Beispiel dargestellt.

a. Zurück zur Berechtigung auf Administratorebene:

   ```
   set -privilege admin
   ```

8. Vergewissern Sie sich, dass sich node1 und node2 in einem HA-Paar befinden und überprüfen Sie, dass die Knoten miteinander verbunden sind und dass Übernahme möglich ist:

   ```
   storage failover show
   ```

   Das folgende Beispiel zeigt die Ausgabe, wenn die Nodes miteinander verbunden sind und Takeover möglich ist:

   ```
   cluster::> storage failover show
                                Takeover
   Node           Partner        Possible State Description
   -------------- -------------- -------- -------------------------------
   node1          node2          true     Connected to node2
   node2          node1          true     Connected to node1
   ```

   Beide Nodes sollten sich im partiellen Giveback enthalten. Das folgende Beispiel zeigt, dass sich node1 teilweise im Giveback befindet:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -------------------------------
node1          node2          true     Connected to node2, Partial
giveback
node2          node1          true     Connected to node1
```

Wenn einer der beiden Nodes sich als Teil des Giveback befindet, verwenden Sie den `storage failover giveback` Führen Sie den Befehl zum Giveback durch, und verwenden Sie dann den `storage failover show-giveback` Befehl um sicherzustellen, dass noch keine Aggregate zurückgegeben werden müssen. Ausführliche Informationen zu den Befehlen finden Sie unter "Quellen" Link zu *High Availability Management*.

9. Bestätigen Sie, dass weder node1 noch node2 die Aggregate besitzen, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

   `storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state`

   Wenn weder node1 noch node2 besitzt Aggregate, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer), gibt das System eine Meldung ähnlich dem folgenden Beispiel zurück:

```
cluster::> storage aggregate show -node node2 -is-home false -fields
owner-name,homename,state
There are no entries matching your query.
```

   Im folgenden Beispiel wird die Ausgabe des Befehls für einen Node mit dem Namen node2 angezeigt, der der Home-Inhaber, jedoch nicht der aktuelle Eigentümer von vier Aggregaten ist:

```
cluster::> storage aggregate show -node node2 -is-home false
              -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node2        online
aggr2         node1        node2        online
aggr3         node1        node2        online
aggr4         node1        node2        online

4 entries were displayed.
```

10. Führen Sie eine der folgenden Aktionen durch:

Wenn der Befehl in ausgeführt wird Schritt 9…	Dann…
Leere Ausgabe	Überspringen Sie Schritt 11, und fahren Sie mit fort Schritt 12.
Hatte eine Ausgabe	Gehen Sie zu Schritt 11.

11. [[man_prepare_Nodes_step11] Wenn node1 oder node2 Aggregate besitzt, für die es der aktuelle Eigentümer, aber nicht der Besitzer des Hauses ist, führen Sie die folgenden Teilschritte durch:

    a. Gibt die Aggregate zurück, die derzeit dem Partner-Node gehören, an den Home-Owner-Node:

    ```
    storage failover giveback -ofnode home_node_name
    ```

    b. Überprüfen Sie, dass weder node1 noch node2 noch Eigentümer von Aggregaten ist, für die es der aktuelle Eigentümer ist (aber nicht der Hausbesitzer):

    ```
    storage aggregate show -nodes node_name -is-home false -fields owner-name,
    home-name, state
    ```

    Das folgende Beispiel zeigt die Ausgabe des Befehls, wenn ein Node sowohl der aktuelle Eigentümer als auch der Home-Inhaber von Aggregaten ist:

```
cluster::> storage aggregate show -nodes node1
          -is-home true -fields owner-name,home-name,state

aggregate     home-name    owner-name   state
------------- ------------ ------------ ------
aggr1         node1        node1        online
aggr2         node1        node1        online
aggr3         node1        node1        online
aggr4         node1        node1        online

4 entries were displayed.
```

12. Bestätigen, dass node1 und node2 auf den Speicher des anderen zugreifen können und überprüfen, dass keine Festplatten fehlen:

    ```
    storage failover show -fields local-missing-disks,partner-missing-disks
    ```

    Im folgenden Beispiel wird die Ausgabe angezeigt, wenn keine Festplatten fehlen:

```
cluster::> storage failover show -fields local-missing-disks,partner-
missing-disks

node     local-missing-disks partner-missing-disks
-------- ------------------- ---------------------
node1    None                None
node2    None                None
```

Wenn Festplatten fehlen, lesen Sie "Quellen" Verbinden mit *Disk- und Aggregatmanagement mit CLI*, *logischem Storage-Management mit CLI* und *High Availability Management*, um Storage für das HA-Paar zu konfigurieren.

13. Vergewissern Sie sich, dass node1 und node2 gesund sind und am Cluster teilnehmen können:

    `cluster show`

    Das folgende Beispiel zeigt die Ausgabe, wenn beide Nodes qualifiziert und ordnungsgemäß sind:

```
cluster::> cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
```

14. Legen Sie die Berechtigungsebene auf erweitert fest:

    `set -privilege advanced`

15. Bestätigen Sie, dass node1 und node2 dieselbe ONTAP-Version ausführen:

    `system node image show -node *node1,node2* -iscurrent true`

    Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt:

```
cluster::*> system node image show -node node1,node2 -iscurrent true

                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node1
         image1   true    true    9.1         2/7/2017 20:22:06
node2
         image1   true    true    9.1         2/7/2017 20:20:48

2 entries were displayed.
```

16. Vergewissern Sie sich, dass weder node1 noch node2 Eigentümer sämtlicher Daten-LIFs sind, die zu anderen Nodes im Cluster gehören, und überprüfen Sie die `Current Node` Und `Is Home` Spalten in der Ausgabe:

    `network interface show -role data -is-home false -curr-node` *`node_name`*

    Das folgende Beispiel zeigt die Ausgabe, wenn node1 keine LIFs besitzt, die im Besitz anderer Nodes im Cluster sind:

    ```
    cluster::> network interface show -role data -is-home false -curr-node
    node1
     There are no entries matching your query.
    ```

    Das folgende Beispiel zeigt die Ausgabe, wenn Node1 dem anderen Node gehören wird, der Eigentümer von Daten-LIFs:

    ```
    cluster::> network interface show -role data -is-home false -curr-node
    node1

                Logical    Status     Network            Current
    Current Is
    Vserver     Interface  Admin/Oper Address/Mask       Node          Port
    Home
    ----------- ---------- ---------- ------------------ -------------
    ------- ----
    vs0
                data1      up/up      172.18.103.137/24  node1         e0d
    false
                data2      up/up      172.18.103.143/24  node1         e0f
    false

    2 entries were displayed.
    ```

17. Wenn die Ausgabe in Schritt 15 Zeigt, dass Node1 oder node2 Eigentümer beliebiger Daten-LIFs sind, die sich im Besitz anderer Nodes im Cluster befinden. Migrieren Sie die Daten-LIFs von node1 oder node2:

    ```
    network interface revert -vserver * -lif *
    ```

    Ausführliche Informationen zum `network interface revert` Befehl, siehe "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

18. Überprüfen Sie, ob node1 oder node2 ausgefallene Festplatten besitzt:

    ```
    storage disk show -nodelist node1,node2 -broken
    ```

    Wenn eine der Festplatten ausgefallen ist, entfernen Sie sie gemäß den Anweisungen in *Disk und Aggregat-Management mit der CLI*. (Siehe "Quellen" Verbinden mit *Disk und Aggregatmanagement mit CLI*.)

19. Sammeln Sie Informationen über node1 und node2, indem Sie die folgenden Unterschritte ausführen und die Ausgabe jedes Befehls aufzeichnen:

    Diese Informationen werden Sie später im Verfahren verwenden.

    a. Notieren Sie das Modell, die System-ID und die Seriennummer beider Nodes:

       ```
       system node show -node node1,node2 -instance
       ```

       Sie verwenden die Informationen, um Festplatten neu zuzuweisen und die ursprünglichen Nodes außer Betrieb zu nehmen.

    b. Geben Sie in node1 und node2 den folgenden Befehl ein und notieren Sie Informationen über die Shelfs, die Anzahl der Festplatten in jedem Shelf, die Flash Storage-Details, den Arbeitsspeicher, NVRAM und die Netzwerkkarten aus der Ausgabe:

       ```
       run -node node_name sysconfig
       ```

       Sie können die Informationen verwenden, um Teile oder Zubehör zu identifizieren, die Sie auf node3 oder node4 übertragen möchten. Wenn Sie nicht wissen, ob die Nodes V-Series Systeme sind oder über FlexArray-Virtualisierungssoftware verfügen, können Sie das auch aus der Ausgabe lernen.

    c. Geben Sie sowohl bei node1 als auch bei node2 den folgenden Befehl ein und notieren Sie die Aggregate, die auf beiden Nodes online sind:

       ```
       storage aggregate show -node node_name -state online
       ```

       Mithilfe dieser Informationen und der Informationen im folgenden Unterschritt können Sie überprüfen, ob die Aggregate und Volumes während des gesamten Verfahrens online bleiben, mit Ausnahme des kurzen Zeitraums, in dem sie während der Verschiebung offline sind.

    d. Geben Sie sowohl für node1 als auch für node2 den folgenden Befehl ein und notieren Sie die Volumes, die auf beiden Knoten offline sind:

```
volume show -node node_name -state offline
```

Nach dem Upgrade führen Sie den Befehl erneut aus und vergleichen die Ausgabe mit der Ausgabe in diesem Schritt, um zu sehen, ob andere Volumes offline gegangen sind.

20. Geben Sie die folgenden Befehle ein, um zu ermitteln, ob Schnittstellengruppen oder VLANs auf node1 oder node2 konfiguriert sind:

    ```
    network port ifgrp show

    network port vlan show
    ```

    Beachten Sie, ob Schnittstellengruppen oder VLANs auf node1 oder node2 konfiguriert sind. Diese Informationen benötigen Sie im nächsten Schritt und später im Verfahren.

21. Führen Sie die folgenden Teilschritte sowohl bei node1 als auch bei node2 durch, um zu bestätigen, dass die physischen Ports im weiteren Verlauf des Verfahrens korrekt zugeordnet werden können:

    a. Geben Sie den folgenden Befehl ein, um zu ermitteln, ob außer den Failover-Gruppen auf dem Node Failover-Gruppen vorhanden sind `clusterwide`:

    ```
    network interface failover-groups show
    ```

    Failover-Gruppen sind Gruppen von Netzwerk-Ports, die sich im System befinden. Da durch ein Upgrade der Controller-Hardware der Standort physischer Ports geändert werden kann, können Failover-Gruppen während des Upgrades unbeabsichtigt geändert werden.

    Das System zeigt Failover-Gruppen auf dem Node an, wie im folgenden Beispiel dargestellt:

    ```
    cluster::> network interface failover-groups show

    Vserver              Group              Targets
    -------------------- ------------------ ----------
    Cluster              Cluster            node1:e0a, node1:e0b
                                            node2:e0a, node2:e0b

    fg_6210_e0c          Default            node1:e0c, node1:e0d
                                            node1:e0e, node2:e0c
                                            node2:e0d, node2:e0e

    2 entries were displayed.
    ```

    b. Wenn es andere Failover-Gruppen als gibt `clusterwide`Notieren Sie die Namen der Failover-Gruppen und die Ports, die zu den Failover-Gruppen gehören.

    c. Geben Sie den folgenden Befehl ein, um zu ermitteln, ob auf dem Node konfigurierte VLANs vorhanden sind:

    ```
    network port vlan show -node node_name
    ```

    VLANs werden über physische Ports konfiguriert. Wenn sich die physischen Ports ändern, müssen die

VLANs später im Verfahren neu erstellt werden.

Das System zeigt VLANs an, die auf dem Knoten konfiguriert sind, wie im folgenden Beispiel dargestellt:

```
cluster::> network port vlan show

Network Network
Node    VLAN Name Port    VLAN ID MAC Address
------  --------- ------- ------- ------------------
node1   e1b-70    e1b     70      00:15:17:76:7b:69
```

a. Wenn auf dem Node VLANs konfiguriert sind, notieren Sie sich jeden Netzwerkport und die Verbindung zwischen VLAN-ID.

22. Führen Sie eine der folgenden Aktionen durch:

Wenn Interface Groups oder VLANS…	**Dann…**
Auf node1 oder node2	Vollständig Schritt 23 Und Schritt 24.
Nicht auf node1 oder node2	Gehen Sie zu Schritt 24.

23. [[man_prepare_Nodes_step23] Wenn Sie nicht wissen, ob sich node1 und node2 in einer SAN- oder nicht-SAN-Umgebung befinden, geben Sie den folgenden Befehl ein und überprüfen die Ausgabe:

`network interface show -vserver` *`vserver_name`* `-data-protocol iscsi|fcp`

Wenn iSCSI oder FC für die SVM konfiguriert ist, wird mit dem Befehl eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::> network interface show -vserver Vserver8970 -data-protocol
iscsi|fcp
There are no entries matching your query.
```

Sie können bestätigen, dass sich der Knoten in einer NAS-Umgebung befindet, indem Sie den verwenden `network interface show` Befehl mit dem `-data-protocol nfs|cifs` Parameter.

Wenn iSCSI oder FC für die SVM konfiguriert ist, wird mit dem Befehl eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::> network interface show -vserver vs1 -data-protocol iscsi|fcp

         Logical    Status     Network            Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask       Node     Port    Home
-------- ---------- ---------- ------------------ -------- ------- ----
vs1      vs1_lif1   up/down    172.17.176.20/24   node1    0d      true
```

24. Stellen Sie sicher, dass alle Knoten im Cluster Quorum sind, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie die erweiterte Berechtigungsebene ein:

    ```
    set -privilege advanced
    ```

    Vom System wird die folgende Meldung angezeigt:

    ```
    Warning: These advanced commands are potentially dangerous; use them
    only when directed to do so by NetApp personnel.
    Do you wish to continue? (y or n):
    ```

    b. Eingabe `y`.

    c. Überprüfen Sie einmal für jeden Node den Cluster-Service-Status im Kernel:

    ```
    cluster kernel-service show
    ```

    Vom System wird eine Meldung wie das folgende Beispiel angezeigt:

```
cluster::*> cluster kernel-service show

Master        Cluster       Quorum        Availability  Operational
Node          Node          Status        Status        Status
------------- ------------- ------------- ------------- -------------
node1         node1         in-quorum     true          operational
              node2         in-quorum     true          operational

2 entries were displayed.
```

+
Nodes in einem Cluster sind Quorum, wenn eine einfache Mehrheit der Nodes in einem ordnungsgemäßen Zustand ist und miteinander kommunizieren kann. Weitere Informationen finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

    a. Zurück zur Administratorberechtigungsebene:

    ```
    set -privilege admin
    ```

25. Führen Sie eine der folgenden Aktionen durch:

Wenn der Cluster…	**Dann…**
Ist SAN konfiguriert	Gehen Sie zu Schritt 26.
Hat kein SAN konfiguriert	Gehen Sie zu Schritt 29.

26. Stellen Sie sicher, dass SAN LIFs auf node1 und node2 für jede SVM sind, bei der entweder SAN iSCSI oder FC Service aktiviert ist, indem Sie den folgenden Befehl eingeben und seine Ausgabe prüfen:

```
network interface show -data-protocol iscsi|fcp -home-node node_name
```

Der Befehl zeigt SAN LIF-Informationen für node1 und node2 an. Die folgenden Beispiele zeigen den Status in der Spalte Status Admin/Oper nach oben/oben und geben an, dass SAN-iSCSI- und FC-Service aktiviert sind:

```
cluster::> network interface show -data-protocol iscsi|fcp
            Logical    Status     Network                  Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask             Node
Port    Home
----------- ---------- ---------- ------------------       ---------
------- ----
a_vs_iscsi  data1      up/up      10.228.32.190/21         node1     e0a
true
            data2      up/up      10.228.32.192/21         node2     e0a
true

b_vs_fcp    data1      up/up      20:09:00:a0:98:19:9f:b0  node1     0c
true
            data2      up/up      20:0a:00:a0:98:19:9f:b0  node2     0c
true

c_vs_iscsi_fcp data1   up/up      20:0d:00:a0:98:19:9f:b0  node2     0c
true
            data2      up/up      20:0e:00:a0:98:19:9f:b0  node2     0c
true
            data3      up/up      10.228.34.190/21         node2     e0b
true
            data4      up/up      10.228.34.192/21         node2     e0b
true
```

Alternativ können Sie ausführlichere LIF-Informationen anzeigen, indem Sie den folgenden Befehl eingeben:

```
network interface show -instance -data-protocol iscsi|fcp
```

27. Erfassen Sie die Standardkonfiguration aller FC-Ports an den ursprünglichen Nodes, indem Sie den folgenden Befehl eingeben und die Ausgabe für Ihre Systeme aufzeichnen:

```
ucadmin show
```

Der Befehl zeigt Informationen zu allen FC-Ports im Cluster an, wie im folgenden Beispiel dargestellt:

```
cluster::> ucadmin show

                Current Current   Pending Pending   Admin
Node    Adapter Mode    Type      Mode    Type      Status
------- ------- ------- --------- ------- --------- -----------
node1   0a      fc      initiator -       -         online
node1   0b      fc      initiator -       -         online
node1   0c      fc      initiator -       -         online
node1   0d      fc      initiator -       -         online
node2   0a      fc      initiator -       -         online
node2   0b      fc      initiator -       -         online
node2   0c      fc      initiator -       -         online
node2   0d      fc      initiator -       -         online
8 entries were displayed.
```

Sie können die Informationen nach dem Upgrade verwenden, um die Konfiguration von FC-Ports auf den neuen Nodes einzustellen.

28. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware aktualisieren, erfassen Sie Informationen über die Topologie der Original-Nodes, indem Sie den folgenden Befehl eingeben und die Ausgabe aufzeichnen:

    `storage array config show -switch`

    Das System zeigt Topologieinformationen wie im folgenden Beispiel dargestellt an:

```
cluster::> storage array config show -switch

      LUN LUN                                    Target Side Initiator
Side Initi-
Node  Grp Cnt Array Name    Array Target Port  Switch Port Switch Port
ator
----- --- --- ------------- ------------------ -----------
-------------- ------
node1 0   50  I_1818FAStT_1
                            205700a0b84772da   vgbr6510a:5
vgbr6510s164:3  0d
                            206700a0b84772da   vgbr6510a:6
vgbr6510s164:4  2b
                            207600a0b84772da   vgbr6510b:6
vgbr6510s163:1  0c
node2 0   50  I_1818FAStT_1
                            205700a0b84772da   vgbr6510a:5
vgbr6510s164:1  0d
                            206700a0b84772da   vgbr6510a:6
vgbr6510s164:2  2b
                            207600a0b84772da   vgbr6510b:6
vgbr6510s163:3  0c
                            208600a0b84772da   vgbr6510b:5
vgbr6510s163:4  2a
7 entries were displayed.
```

29. die folgenden Teilschritte ausführen:

    a. Geben Sie an einem der Original-Nodes den folgenden Befehl ein und notieren Sie die Ausgabe:

       `service-processor show -node * -instance`

    Das System zeigt auf beiden Nodes detaillierte Informationen zum SP an.

    a. Vergewissern Sie sich, dass der SP-Status lautet `online`.
    b. Vergewissern Sie sich, dass das SP-Netzwerk konfiguriert ist.
    c. Notieren Sie die IP-Adresse und andere Informationen zum SP.

       Möglicherweise möchten Sie die Netzwerkparameter der Remote-Verwaltungsgeräte, in diesem Fall die SPs, vom ursprünglichen System für die SPs auf den neuen Knoten wieder verwenden. Ausführliche Informationen zum SP finden Sie unter "Quellen" Link zu den Befehlen *Systemadministration Reference* und *ONTAP 9: Manual Page Reference*.

30. Wenn die neuen Nodes dieselben lizenzierten Funktionen wie die ursprünglichen Knoten haben sollen, geben Sie den folgenden Befehl ein, um die Clusterlizenzen auf dem ursprünglichen System anzuzeigen:

    `system license show -owner *`

Das folgende Beispiel zeigt die Websitelizenzen für Cluster1:

```
system license show -owner *
Serial Number: 1-80-000013
Owner: cluster1

Package           Type    Description           Expiration
----------------- ------- --------------------- -----------
Base              site    Cluster Base License  -
NFS               site    NFS License           -
CIFS              site    CIFS License          -
SnapMirror        site    SnapMirror License    -
FlexClone         site    FlexClone License     -
SnapVault         site    SnapVault License     -
6 entries were displayed.
```

31. Beschaffung neuer Lizenzschlüssel für die neuen Nodes auf der *NetApp Support Site*. Siehe "Quellen" Zum Link zu *NetApp Support Site*.

    Falls auf der Website keine Lizenzschlüssel vorhanden ist, wenden Sie sich an Ihren NetApp Ansprechpartner.

32. Überprüfen Sie, ob im Original-System AutoSupport aktiviert ist, indem Sie auf jedem Node den folgenden Befehl eingeben und seine Ausgabe überprüfen:

    `system node autosupport show -node node1,node2`

    Die Befehlsausgabe gibt an, ob AutoSupport aktiviert ist. Wie im folgenden Beispiel gezeigt:

```
cluster::> system node autosupport show -node node1,node2

Node              State     From          To                Mail Hosts
----------------- --------- ------------- ----------------  ----------
node1             enable    Postmaster    admin@netapp.com  mailhost

node2             enable    Postmaster    -                 mailhost
2 entries were displayed.
```

33. Führen Sie eine der folgenden Aktionen durch:

Wenn das ursprüngliche System…	Dann…
Hat AutoSupport aktiviert…	Gehen Sie zu Schritt 34.

Wenn das ursprüngliche System…	Dann…
AutoSupport ist nicht aktiviert…	Aktivieren Sie AutoSupport, indem Sie den Anweisungen in der Systemverwaltungsreferenz_ folgen. (Siehe "Quellen" Zum Verknüpfen mit der Referenz *Systemadministration*.) **Hinweis:** AutoSupport ist standardmäßig aktiviert, wenn Sie Ihr Speichersystem zum ersten Mal konfigurieren. Sie können AutoSupport zwar jederzeit deaktivieren, jedoch sollten Sie sie aktiviert lassen. Wenn Sie AutoSupport aktivieren, können Sie erheblich dabei helfen, Probleme und Lösungen zu identifizieren, sollten bei Ihrem Storage-System Probleme auftreten.

34. Überprüfen Sie, ob AutoSupport mit den korrekten E-Mail-IDs für den Mailhost konfiguriert ist, indem Sie auf beiden Originalknoten den folgenden Befehl eingeben und die Ausgabe prüfen:

    `system node autosupport show -node node_name -instance`

    Ausführliche Informationen zu AutoSupport finden Sie unter "Quellen" Link zu den Befehlen *Systemadministration Reference* und *ONTAP 9: Manual Page Reference*.

35. Senden Sie eine AutoSupport-Nachricht für node1 an NetApp, indem Sie den folgenden Befehl eingeben:

    `system node autosupport invoke -node node1 -type all -message "Upgrading node1 from platform_old to platform_new"`

    Senden Sie jetzt keine AutoSupport Nachricht für node2 an NetApp. Sie gehen das später im Verfahren vor.

36. Überprüfen Sie, ob die AutoSupport-Meldung gesendet wurde, indem Sie den folgenden Befehl eingeben und die Ausgabe prüfen:

    `system node autosupport show -node *node1* -instance`

    Felder `Last Subject Sent:` Und `Last Time Sent:` Enthält den Nachrichtentitel der letzten gesendeten Nachricht und den Zeitpunkt, zu dem die Nachricht gesendet wurde.

37. Wenn Ihr System Self-Encrypting Drives verwendet, lesen Sie den Artikel der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der Self-Encrypting Drives, die auf dem HA-Paar verwendet werden, das Sie aktualisieren. ONTAP unterstützt zwei Arten von Self-Encrypting Drives:

    - FIPS-zertifizierte NetApp Storage Encryption (NSE) SAS- oder NVMe-Laufwerke
    - Self-Encrypting-NVMe-Laufwerke (SED) ohne FIPS

    FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

    SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

"Weitere Informationen zu unterstützten Self-Encrypting Drives".

Verwaltung von Authentifizierungsschlüssel mit dem Onboard Key Manager

Sie können den Onboard Key Manager (OKM) zur Verwaltung von Authentifizierungsschlüsseln verwenden. Wenn Sie das OKM eingerichtet haben, müssen Sie die Passphrase und das Sicherungsmaterial aufzeichnen, bevor Sie mit dem Upgrade beginnen.

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

   Dies ist die Passphrase, die eingegeben wurde, als das OKM mit der CLI oder REST-API konfiguriert oder aktualisiert wurde.

2. Sichern Sie die Key-Manager-Informationen, indem Sie den ausführen `security key-manager onboard show-backup` Befehl.

SnapMirror Beziehungen stilllegen

Bevor Sie das System mit dem Netzboot booten, müssen Sie sicherstellen, dass alle SnapMirror Beziehungen stillgelegt werden. Wenn eine SnapMirror Beziehung stillgelegt wird, bleibt es bei einem Neustart und einem Failover stillgelegt.

Schritte

1. Überprüfen Sie den SnapMirror Beziehungsstatus auf dem Ziel-Cluster:

   ```
   snapmirror show
   ```

   ⓘ Wenn der Status lautet `Transferring`, Sie müssen diese Transfers abbrechen: `snapmirror abort -destination-vserver vserver name`

   Der Abbruch schlägt fehl, wenn die SnapMirror-Beziehung sich nicht im befindet `Transferring` Bundesland.

2. Alle Beziehungen zwischen dem Cluster stilllegen:

   ```
   snapmirror quiesce -destination-vserver *
   ```

Vorbereitungen für den Netzboot

Nachdem Sie später noch Node3 und node4 physisch gerast haben, müssen Sie sie eventuell als Netzboot Netboot eingesetzt werden. Der Begriff *boots* bedeutet, dass Sie von einem 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.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.

- Siehe "Quellen" Um eine Verknüpfung zur NetApp Support-Website zu erhalten und die erforderlichen Systemdateien für Ihre Plattform und die richtige Version von ONTAP herunterzuladen.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert 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.

Sie müssen die Controller jedoch nicht per Netzboot fahren, wenn auf den Original-Controllern die gleiche Version von ONTAP 9 installiert ist. Wenn ja, können Sie diesen Abschnitt überspringen und mit fortfahren "Phase 3: Installieren und booten node3".

Schritte

1. auf der NetApp Support-Website können Sie die Dateien herunterladen, die zum Ausführen des Netzboots des Systems verwendet werden.
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. 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 FAS/AFF8000 Serie	Extrahieren Sie den Inhalt des `<ontap_version>_image.tgz` Datei zum Zielverzeichnis:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz`HINWEIS: Sie müssen den Inhalt des nicht extrahieren `<ontap_version>_image.tgz` Datei:

Sie verwenden Informationen in den Verzeichnissen in "Phase 3".

Stufe 2: Knoten1 verschieben und ausmustern

Phase-2-Übersicht

Während Phase 2 verschieben Sie Aggregate ohne Root-Root-Fehler von Knoten1 auf

Knoten2 und verschieben Daten-LIFs, die nicht-SAN-Daten-LIFs gehören, die sich im Besitz von node1 befinden, auf Knoten 2, einschließlich fehlgeschlagener oder Vetos. Sie notieren auch die notwendigen Node1-Informationen, die Sie später im Verfahren verwenden können, und setzen dann node1 aus.

Schritte

1. "Verlagerung von Aggregaten außerhalb der Root-Ebene und NAS-Daten-LIFs, die sich im Besitz von node1 auf node2 befinden"
2. "Das Verschieben von NAS-Daten-LIFs von node1 auf node2"
3. "Node1-Informationen werden aufgezeichnet"
4. "Node1 ausmustern"

Verschiebung von nicht-Root-Aggregaten von node1 auf node2

Bevor Sie node1 durch node3 ersetzen können, müssen Sie die nicht-Root-Aggregate von node1 auf node2 verschieben, indem Sie den Befehl Storage Aggregate Relocation verwenden und dann die Verschiebung überprüfen.

Schritte

1. Verschieben der nicht-Root-Aggregate durch Ausfüllen der folgenden Teilschritte:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      ```
      set -privilege advanced
      ```

   b. Geben Sie den folgenden Befehl ein:

      ```
      storage aggregate relocation start -node node1 -destination node2 -aggregate
      -list * -ndo-controller-upgrade true
      ```

   c. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge werden im Hintergrund stattfinden. Um ein Aggregat verschieben zu können, dauerte der Vorgang einige Sekunden oder Minuten. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

   d. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:

      ```
      set -privilege admin
      ```

2. Überprüfen Sie den Versetzungsstatus, indem Sie auf node1 den folgenden Befehl eingeben:

   ```
   storage aggregate relocation show -node node1
   ```

   Die Ausgabe wird angezeigt `Done` Für ein Aggregat, nachdem es verlegt wurde.

   > Warten Sie, bis alle nicht-Root-Aggregate im Besitz von node1 in node2 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

3. Führen Sie eine der folgenden Aktionen durch:

Wenn Umzug…	Dann…
Von allen Aggregaten ist erfolgreich	Gehen Sie zu Schritt 4.
Fällt ein Aggregate aus oder kommt ein Vetos vor	a. Überprüfen Sie die EMS-Protokolle auf Korrekturmaßnahmen. b. Führen Sie die Korrekturmaßnahme durch. c. Verschiebung ausgefallener oder Vetos von Aggregaten: `storage aggregate relocation start -node node1 - destination node2 -aggregate-list * -ndo -controller-upgrade true` d. Geben Sie bei der entsprechenden Aufforderung ein `y`. e. Zurück zur Administratorebene: `set -privilege admin`Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen: ◦ Veto-Prüfungen überschreiben: `storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade` ◦ Zielprüfungen überschreiben: `storage aggregate relocation start -override -destination-checks true -ndo-controller -upgrade` Siehe "Quellen" Link zum *Disk- und Aggregatmanagement mit dem CLI* Inhalt und den *ONTAP 9 Befehlen: Manual Page Reference* Weitere Informationen zu den Befehlen zum Verlegen von Speicheraggregaten.

4. Überprüfen Sie, ob alle nicht-Root-Aggregate online sind und ihren Status auf node2:

   `storage aggregate show -node node2 -state online -root false`

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node2 online sind:

```
cluster::> storage aggregate show -node node2 state online -root false
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr_1
           744.9GB 744.8GB      0% online       5 node2
raid_dp,

normal
aggr_2     825.0GB 825.0GB      0% online       1 node2
raid_dp,

normal
2 entries were displayed.
```

Wenn die Aggregate offline gegangen sind oder in node2 fremd geworden sind, bringen Sie sie mit dem folgenden Befehl auf node2, einmal für jedes Aggregat online:

`storage aggregate online -aggregate` *`aggr_name`*

5. Überprüfen Sie, ob alle Volumes auf node2 online sind, indem Sie den folgenden Befehl auf node2 eingeben und seine Ausgabe prüfen:

   `volume show -node` *`node2`* `-state offline`

   Wenn ein Volume auf node2 offline ist, bringen Sie sie mit dem folgenden Befehl auf node2 für jedes Volume online:

   `volume online -vserver` *`vserver-name`* `-volume` *`volume-name`*

   Der `vserver-name` Die Verwendung mit diesem Befehl ist in der Ausgabe des vorherigen gefunden `volume show` Befehl.

6. Geben Sie auf node2 den folgenden Befehl ein:

   `storage failover show -node` *`node2`*

   Die Ausgabe sollte die folgende Meldung anzeigen:

   ```
   Node owns partner's aggregates as part of the nondisruptive controller
   upgrade procedure.
   ```

7. Vergewissern Sie sich, dass node1 keine im Besitz von nicht-Root-Aggregaten ist, die online sind:

   `storage aggregate show -owner-name` *`node1`* `-ha-policy sfo -state online`

   Die Ausgabe sollte keine online nicht-Root-Aggregate anzeigen, die bereits in node2 verschoben wurden.

Verschieben Sie NAS-Daten-LIFs von node1 auf node2

Bevor Sie node1 durch node3 ersetzen können, müssen Sie die NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf node2 verschieben, wenn Sie ein Cluster mit zwei Nodes haben, oder auf einen dritten Node, wenn Ihr Cluster mehr als zwei Nodes hat. Die von Ihnen verwendete Methode hängt davon ab, ob das Cluster für NAS oder SAN konfiguriert ist.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. Sie müssen überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Führen Sie alle auf node1 gehosteten NAS-Daten-LIFs auf, indem Sie den folgenden Befehl eingeben und die Ausgabe erfassen:

   `network interface show -data-protocol nfs|cifs -curr-node` *`node1`*

   Das System zeigt die NAS-Daten-LIFs auf node1 an, wie im folgenden Beispiel dargestellt:

```
 cluster::> network interface show -data-protocol nfs|cifs -curr-node
node1

          Logical     Status      Network             Current   Current
Is
 Vserver  Interface   Admin/Oper  Address/Mask        Node      Port
Home
 -------- ----------  ----------  ------------------  --------- -------
----
 vs0
          a0a         up/down     10.63.0.53/24       node1     a0a
true
          data1       up/up       10.63.0.50/18       node1     e0c
true
          rads1       up/up       10.63.0.51/18       node1     e1a
true
          rads2       up/down     10.63.0.52/24       node1     e1b
true
 vs1
          lif1        up/up       192.17.176.120/24   node1     e0c
true
          lif2        up/up       172.17.176.121/24   node1     e1a
true
```

2. Führen Sie eine der folgenden Aktionen durch:

Falls Knoten 1…	Dann…
Sind Schnittstellengruppen mit VLANs konfiguriert	Gehen Sie zu Schritt 3.
Schnittstellengruppen oder VLANs sind nicht konfiguriert	Überspringen Sie Schritt 3, und fahren Sie mit fort Schritt 4.

Verwenden Sie die `network port vlan show` Befehl zum Anzeigen von Informationen über die mit VLANs verbundenen Netzwerk-Ports, und verwenden Sie den `network port ifgrp show` Befehl zum Anzeigen von Informationen über die Port-Schnittstellengruppen.

3. Nehmen Sie die folgenden Schritte durch, um alle auf Schnittstellengruppen und VLANs gehosteten NAS-Daten-LIFs auf node1 zu migrieren:

   a. Migrieren Sie die LIFs, die auf beliebigen Schnittstellengruppen gehostet werden, und die VLANs auf node1 zu einem Port auf node2, der in der Lage ist, LIFs auf demselben Netzwerk wie die der Schnittstellengruppen zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

   `network interface migrate -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node2`* `–destination-port` *`netport|ifgrp`*

   b. Ändern Sie den Home-Port und den Home-Node der LIFs und VLANs in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

   `network interface modify -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node2`* `- home-port` *`netport|ifgrp`*

4. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 5 Bis Schritt 8.
San	Deaktivieren Sie alle SAN-LIFs auf dem Node, um sie für das Upgrade herunterzufahren: `network interface modify -vserver *Vserver-name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport`

5. Migrieren Sie NAS-Daten-LIFs von node1 nach node2, indem Sie den folgenden Befehl eingeben, einmal für jede Daten-LIF:

   `network interface migrate -vserver` *`Vserver-name`* `-lif` *`LIF_name`* `-destination -node` *`node2`* `-destination-port` *`data_port`*

6. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs an die richtigen Ports verschoben wurden und dass die LIFs den Status von „up“ aufweisen. Geben Sie dazu den folgenden Befehl an einem der beiden Nodes ein und überprüfen Sie die Ausgabe:

   `network interface show -curr-node` *`node2`* `-data-protocol nfs|cifs`

7. Geben Sie den folgenden Befehl ein, um den Home-Node der migrierten LIFs zu ändern:

```
network interface modify -vserver Vserver-name -lif LIF_name -home-node node2
-home-port port_name
```

8. Überprüfen Sie, ob die LIF den Port als ihren Home- oder aktuellen Port verwendet. Wenn der Port nicht zu Hause oder der aktuelle Port ist, fahren Sie mit fort Schritt 9:

```
network interface show -home-node node2 -home-port port_name
```

```
network interface show -curr-node node_name -curr-port port_name
```

9. Wenn die LIFs den Port als Home-Port oder aktuellen Port verwenden, ändern Sie die LIF und verwenden Sie einen anderen Port:

```
network interface migrate -vserver Vserver-name -lif LIF_name
-destination-node node_name -destination-port port_name
```

```
network interface modify -vserver Vserver-name -lif LIF_name -home-node
node_name -home-port port_name
```

10. Wenn die Ports, die derzeit Daten-LIFs hosten, nicht auf der neuen Hardware vorhanden sein werden, entfernen Sie sie jetzt aus der Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace Default -broadcast-domain
Default -ports node:port
```

11. Wenn eine der LIFs ausgefallen sind, setzen Sie den Administrationsstatus der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface modify -vserver Vserver-name -lif LIF_name -home-node
nodename -status-admin up
```

> Bei MetroCluster Konfigurationen können Sie die Broadcast-Domäne eines Ports möglicherweise nicht ändern, da dieser einem Port zugewiesen ist, der die LIF einer Ziel-Storage Virtual Machine (SVM) hostet. Geben Sie den folgenden Befehl von der entsprechenden Quell-SVM auf dem Remote-Standort ein, um die Ziel-LIF einem entsprechenden Port zuzuweisen:
> `metrocluster vserver resync -vserver Vserver_name`

12. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu überprüfen, ob auf node1 keine Daten-LIFs mehr vorhanden sind:

```
network interface show -curr-node node1 -role data
```

13. Wenn Schnittstellengruppen oder VLANs konfiguriert sind, führen Sie die folgenden Teilschritte aus:

    a. Entfernen Sie die VLANs aus den Schnittstellengruppen, indem Sie den folgenden Befehl eingeben:

    ```
    network port vlan delete -node nodename -port ifgrp_name -vlan-id VLAN_ID
    ```

    b. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu sehen, ob Schnittstellengruppen auf dem Node konfiguriert sind:

    ```
    network port ifgrp show -node nodename -ifgrp ifgrp_name -instance
    ```

Das System zeigt Schnittstellengruppeninformationen für den Node an, wie im folgenden Beispiel gezeigt:

```
cluster::> network port ifgrp show -node node1 -ifgrp a0a -instance
                  Node: node1
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: 02:a0:98:17:dc:d4
   Port Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

a. Wenn Schnittstellengruppen auf dem Node konfiguriert sind, notieren Sie die Namen dieser Gruppen und der ihnen zugewiesenen Ports. Löschen Sie dann die Ports, indem Sie den folgenden Befehl eingeben, und zwar einmal für jeden Port:

   `network port ifgrp remove-port -node` *`nodename`* `-ifgrp` *`ifgrp_name`* `-port` *`netport`*

Node1-Informationen aufzeichnen

Bevor Sie node1 herunterfahren und außer Betrieb nehmen können, müssen Sie Informationen über das Cluster-Netzwerk, die Management- und FC-Ports sowie seine NVRAM-System-ID aufzeichnen. Sie benötigen diese Informationen später im Verfahren, wenn Sie node1 Node3 zuordnen und Festplatten neu zuweisen.

Schritte

1. Geben Sie den folgenden Befehl ein, und erfassen Sie die Ausgabe:

   `network route show`

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
cluster::> network route show

Vserver         Destination    Gateway      Metric
 -------------- -------------- ----------- -------
 iscsi vserver  0.0.0.0/0       10.10.50.1  20
 node1          0.0.0.0/0       10.10.20.1  10
 ....
 node2          0.0.0.0/0       192.169.1.1 20
```

2. Geben Sie den folgenden Befehl ein und erfassen Sie die Ausgabe:

```
vserver services name-service dns show
```

Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
 cluster::> vserver services name-service dns show
                                                                    Name
 Vserver        State     Domains                                   Servers
 -------------- --------- ------------------------------------
---------------
 node 1 2       enabled   alpha.beta.gamma.netapp.com
10.10.60.10,

10.10.60.20
 vs_base1       enabled   alpha.beta.gamma.netapp.com,
10.10.60.10,
                          beta.gamma.netapp.com,
10.10.60.20
 ...
 ...
 vs peer1        enabled  alpha.beta.gamma.netapp.com,
10.10.60.10,
                          gamma.netapp.com
10.10.60.20
```

3. Suchen Sie die Cluster-Netzwerk- und Node-Management-Ports auf node1, indem Sie auf einem der Controller den folgenden Befehl eingeben:

   ```
   network interface show -curr-node node1 -role cluster,intercluster,node-
   mgmt,cluster-mgmt
   ```

   Das System zeigt die LIFs für das Cluster, das Intercluster, das Node-Management und das Cluster-Management für den Node im Cluster an, wie im folgenden Beispiel dargestellt:

```
 cluster::> network interface show -curr-node <node1>
            -role cluster,intercluster,node-mgmt,cluster-mgmt

              Logical       Status     Network            Current
Current Is
  Vserver     Interface     Admin/Oper Address/Mask       Node     Port
Home
  ----------- ------------- ---------- ------------------ --------
------- ----
  vserver1
              cluster mgmt   up/up     192.168.x.xxx/24   node1    e0c
true
  node1
              intercluster   up/up     192.168.x.xxx/24   node1    e0e
true
              clus1          up/up     169.254.xx.xx/24   node1    e0a
true
              clus2          up/up     169.254.xx.xx/24   node1    e0b
true
              mgmt1          up/up     192.168.x.xxx/24   node1    e0c
true
 5 entries were displayed.
```

Das System verfügt möglicherweise über keine Intercluster-LIFs.

4. Erfassen Sie die Informationen in der Ausgabe des Befehls in Schritt 3 Zur Verwendung im Abschnitt "Ports von node1 nach node3 zuordnen".

   Die Ausgabeinformationen sind erforderlich, um die neuen Controller-Ports den alten Controller-Ports zuzuordnen.

5. Geben Sie den folgenden Befehl für node1 ein:

   `network port show -node node1 -type physical`

   Das System zeigt die physischen Ports auf dem Node an, wie im folgenden Beispiel dargestellt:

```
 sti8080mcc-htp-008::> network port show -node sti8080mcc-htp-008 -type
physical

 Node: sti8080mcc-htp-008

                                                                        Ignore
                                                  Speed(Mbps)  Health   Health
 Port   IPspace  Broadcast Domain Link MTU   Admin/Oper   Status   Status
 ----   -------  ---------------- ---- ----  -----------  -------
-------
 e0M    Default  Mgmt             up   1500  auto/1000    healthy  false
 e0a    Default  Default          up   9000  auto/10000   healthy  false
 e0b    Default  -                up   9000  auto/10000   healthy  false
 e0c    Default  -                down 9000  auto/-       -        false
 e0d    Default  -                down 9000  auto/-       -        false
 e0e    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0f    Default  -                up   9000  auto/10000   healthy  false
 e0g    Cluster  Cluster          up   9000  auto/10000   healthy  false
 e0h    Default  Default          up   9000  auto/10000   healthy  false
 9 entries were displayed.
```

6. Notieren Sie die Ports und ihre Broadcast-Domänen.

   Die Broadcast-Domänen müssen später im Verfahren den neuen Ports auf dem neuen Controller zugeordnet werden.

7. Geben Sie den folgenden Befehl für node1 ein:

   `network fcp adapter show -node *node1*`

   Das System zeigt die FC-Ports auf dem Node an, wie im folgenden Beispiel dargestellt:

```
 cluster::> fcp adapter show -node <node1>
                      Connection  Host
 Node         Adapter Established Port Address
 ------------ ------- ----------- ------------
 node1
               0a     ptp         11400
 node1
               0c     ptp         11700
 node1
               6a     loop        0
 node1
               6b     loop        0
 4 entries were displayed.
```

8. Notieren Sie die Ports.

   Die Ausgabeinformationen sind erforderlich, um die neuen FC-Ports auf dem neuen Controller später im Verfahren zuzuordnen.

9. Falls Sie dies zuvor nicht getan haben, überprüfen Sie, ob auf node1 Schnittstellengruppen oder VLANs konfiguriert sind, indem Sie die folgenden Befehle eingeben:

   ```
   network port ifgrp show
   ```

   ```
   network port vlan show
   ```

   Sie verwenden die Informationen im Abschnitt "Ports von node1 nach node3 zuordnen".

10. Führen Sie eine der folgenden Aktionen durch:

Sie suchen…	Dann…
Die NVRAM-System-ID-Nummer im Abschnitt wurde aufgezeichnet "Bereiten Sie die Knoten auf das Upgrade vor".	Weiter mit dem nächsten Abschnitt "Node1 ausmustern".
Die NVRAM-System-ID-Nummer wurde nicht in den Abschnitt aufgezeichnet "Bereiten Sie die Knoten auf das Upgrade vor"	Vollständig Schritt 11 Und Schritt 12 Und dann weiter zu "Node1 ausmustern".

11. Geben Sie den folgenden Befehl auf einem der Controller ein:

    ```
    system node show -instance -node node1
    ```

    Das System zeigt Informationen über node1 an, wie im folgenden Beispiel dargestellt:

    ```
    cluster::> system node show -instance -node <node1>
                                Node: node1
                               Owner:
                            Location: GDl
                               Model: FAS6240
                       Serial Number: 700000484678
                           Asset Tag: -
                              Uptime: 20 days 00:07
                     NVRAM System ID: 1873757983
                           System ID: 1873757983
                              Vendor: NetApp
                              Health: true
                         Eligibility: true
    ```

12. notieren Sie die im Abschnitt zu verwendende NVRAM-System-ID "Installieren und booten Sie node3".

Node1 ausmustern

Um node1 außer Betrieb zu nehmen, müssen Sie das HA-Paar mit node2 deaktivieren, Node1 richtig herunterfahren und aus dem Rack oder Chassis entfernen.

Schritte

1. Überprüfen Sie die Anzahl der Nodes im Cluster:

   ```
   cluster show
   ```

   Das System zeigt die Nodes im Cluster an, wie im folgenden Beispiel dargestellt:

   ```
   cluster::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node1                 true    true
   node2                 true    true
   2 entries were displayed.
   ```

2. Speicherausfallschutz nach Bedarf deaktivieren:

Falls das Cluster…	Dann…

Eines Clusters mit zwei Nodes	a. Deaktivieren Sie die Hochverfügbarkeit des Clusters, indem Sie auf einem der Nodes den folgenden Befehl eingeben:
	`cluster ha modify -configured false`
	a. Deaktivier Speicher-Failover:
	`storage failover modify -node node1 -enabled false`

Ein Cluster mit mehr als zwei Nodes	Deaktivier Speicher-Failover: `storage failover modify -node node1 -enabled false`

   Wenn Sie Storage-Failover nicht deaktivieren, kann es zu einem Ausfall des Controller-Upgrades kommen, der den Datenzugriff unterbrechen und zu Datenverlusten führen kann.

3. Überprüfen Sie, ob der Storage-Failover deaktiviert wurde:

   ```
   storage failover show
   ```

   Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl, wenn Storage-Failover für einen Node deaktiviert wurde:

```
 cluster::> storage failover show
                                 Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node1          node2          false    Connected to node2, Takeover
                                        is not possible: Storage
failover is
                                        disabled

 node2          node1          false    Node owns partner's aggregates
as part
                                        of the nondisruptive controller
upgrade
                                        procedure. Takeover is not
possible:
                                        Storage failover is disabled
 2 entries were displayed.
```

4. Überprüfen Sie den Daten-LIF-Status:

   `network interface show -role data -curr-node node2 -home-node node1`

   Sehen Sie in der Spalte **Status Admin/Oper** nach, ob LIFs nicht verfügbar sind. Wenn LIFs ausgefallen sind, lesen Sie das "Troublehsoot" Abschnitt.

5. Führen Sie eine der folgenden Aktionen durch:

Falls das Cluster…	Dann…
Eines Clusters mit zwei Nodes	Gehen Sie zu Schritt 6.
Ein Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 8.

6. Zugriff auf die erweiterte Berechtigungsebene auf beiden Knoten:

   `set -privilege advanced`

7. Überprüfen Sie, ob die Cluster-HA deaktiviert wurde:

   `cluster ha show`

   Vom System wird die folgende Meldung angezeigt:

```
High Availability Configured: false
```

   Wenn Cluster HA nicht deaktiviert wurde, wiederholen Sie den Vorgang Schritt 2.

8. Prüfen Sie, ob node1 aktuell epsilon hält:

   `cluster show`

   Da in einem Cluster mit einer geraden Anzahl von Nodes eine Krawatte möglich ist, verfügt ein Node über eine zusätzliche fraktionale Abstimmungsgewichtung namens epsilon. Siehe "Quellen" Um weitere Informationen zur *System Administration Reference* zu erhalten.

   > Wenn Sie ein Cluster mit vier Nodes haben, liegt das Epsilon auf einem Node in einem anderen HA-Paar im Cluster.
   >
   > Wenn Sie ein HA-Paar in einem Cluster mit mehreren HA-Paaren aktualisieren, müssen Sie Epsilon auf den Node eines HA-Paars verschieben, ohne ein Controller-Upgrade durchführen zu müssen. Wenn Sie beispielsweise nodeA/nodeB in einem Cluster mit der HA-Paar-Konfiguration nodeA/nodeB und nodeC/nodded aktualisieren, müssen Sie Epsilon auf nodeC oder nodded verschieben.

   Das folgende Beispiel zeigt, dass bei node1 Epsilon gehalten wird:

   ```
   cluster::*> cluster show

   Node                  Health  Eligibility  Epsilon
   --------------------- ------- ------------ ------------
   node1                 true    true         true
   node2                 true    true         false
   ```

9. Wenn node1 das Epsilon hält, markieren Sie das Epsilon `false` Auf dem Knoten, so dass er auf die node2 übertragen werden kann:

   `cluster modify -node *node1* -epsilon false`

10. Übertragen Sie das Epsilon auf node2, indem Sie epsilon markieren `true` Auf Knoten 2:

    `cluster modify -node *node2* -epsilon true`

11. Vergewissern Sie sich, dass die Änderung in node2 aufgetreten ist:

    `cluster show`

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

    Das Epsilon für node2 sollte nun wahr sein und das Epsilon für node1 sollte falsch sein.

12. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show

Enable Switchless Cluster: false/true
```

Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

13. Zurück zur Administratorebene:

```
set -privilege admin
```

14. Stop node1 von der Eingabeaufforderung node1:

```
system node halt -node node1
```

> **Achtung**: Wenn sich Node1 im selben Gehäuse wie node2 befindet, schalten Sie das Gehäuse nicht über den Netzschalter oder durch Ziehen des Netzkabels aus. Wenn Sie das tun, wird node2, der Daten bereitstellt, ausfallen.

15. Wenn Sie vom System aufgefordert werden, zu bestätigen, dass Sie das System anhalten möchten, geben Sie ein `y`.

    Der Node wird an der Eingabeaufforderung der Boot-Umgebung angehalten.

16. Wenn in node1 die Eingabeaufforderung für die Boot-Umgebung angezeigt wird, entfernen Sie sie aus dem Chassis oder dem Rack.

    Sie können Node1 nach Abschluss des Upgrades außer Betrieb nehmen. Siehe "Ausmustern des alten Systems".

Phase 3: Installieren und booten Sie node3

Phase-3-Übersicht

In Phase 3 installieren und booten Sie Node3, ordnen Sie die Cluster- und Node-Management-Ports von node1 zu node3 zu, überprüfen die Installation und verschieben Daten-LIFs und SAN-LIFs, die zu node1 gehören, von node2 auf node3. Außerdem werden alle Aggregate von node2 auf node3 verschoben und die Daten-LIFs und SAN-LIFs von node2 auf node3 verschoben.

Schritte

1. "Installieren und booten Sie node3"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest"
3. "Ports von node1 nach node3 zuordnen"
4. "Überprüfen Sie die Installation von node3"
5. "Verschieben Sie die NAS-Daten-LIFs von node1 auf node2 und überprüfen Sie SAN LIFs auf node3"

6. "Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3"
7. "Verschieben Sie die NAS-Daten-LIFs von node2 auf node3"

Installieren und booten Sie node3

Sie müssen node3 im Rack installieren, Verbindungen von node1 zu node3, Boot node3 übertragen und ONTAP installieren. Sie müssen auch jede der freien Festplatten von node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate, die nicht früher auf node2 verschoben wurden, neu zuweisen.

Über diese Aufgabe

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten. Siehe "Vorbereitungen für den Netzboot".

Sie müssen jedoch nicht als Netzboot auf Node3 setzen, wenn es die gleiche oder eine höhere Version von ONTAP 9 hat, die auf node1 installiert ist.

> Wenn Sie ein mit Storage-Arrays verbundenes V-Series System oder ein System mit FlexArray-Virtualisierungssoftware aktualisieren, die mit Storage Arrays verbunden ist, sind die vollständigen Anforderungen unbedingt zu beachten Schritt 1 Bis Schritt 5, Lassen Sie diesen Abschnitt bei Schritt 6 Und befolgen Sie die Anweisungen unter "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren" Geben Sie nach Bedarf Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und mit fortfahren Schritt 7.
>
> Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und anschließend mit fortfahren "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

   Wenn sich Node1 und Node2 in einem separaten Chassis befanden, können Sie Node3 in denselben Rack-Standort wie node1 platzieren. Wenn sich jedoch node1 mit node2 im selben Chassis befand, müssen Sie node3 in seinen eigenen Rack-Platz legen, vorzugsweise in der Nähe der Position von node1.

2. Installieren Sie Node3 im Rack gemäß der *Installations- und Setup-Anleitung* für Ihr Node-Modell.

   > Wenn Sie ein Upgrade auf ein System mit beiden Nodes im selben Chassis durchführen, installieren sie node4 sowohl im Chassis als auch in node3. Wenn Sie dies nicht tun, verhält sich der Node, wenn Sie node3 booten, wie in einer Dual-Chassis-Konfiguration. Und wenn Sie node4 booten, wird der Interconnect zwischen den Nodes nicht gestartet.

3. Kabelnode3, Verschieben der Verbindungen von node1 zu node3.

   Die folgenden Referenzen helfen Ihnen dabei, geeignete Kabelverbindungen zu machen. Gehen Sie zu "Quellen" Um eine Verbindung zu ihnen zu machen.

   - *Installations- und Setup-Anleitung* oder *Installationsanforderungen für die FlexArray-Virtualisierung und*

Referenz für die node3-Plattform

- Das entsprechende Verfahren für das Festplatten-Shelf
- Die Dokumentation *High Availability Management*

Folgende Anschlüsse verkabeln:

- Konsole (Remote-Management-Port)
- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Möglicherweise müssen Sie die Interconnect-Karte oder die Cluster Interconnect-Kabelverbindung von node1 zu node3 nicht verschieben, da die meisten Plattform-Modelle über ein einzigartiges Interconnect-Kartenmodell verfügen. Für die MetroCluster-Konfiguration müssen Sie die FC-VI-Kabelverbindungen von node1 zu node3 verschieben. Wenn der neue Host keine FC-VI-Karte besitzt, müssen Sie möglicherweise die FC-VI-Karte verschieben.

4. Einschalten Sie die Stromversorgung auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

   Wenn Sie ein Upgrade auf ein System mit beiden Nodes im gleichen Chassis durchführen, wird node4 auch neu gebootet. Allerdings kann man den node4-Stiefel bis später ignorieren.

   > Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

   ```
   WARNING: The battery is unfit to retain data during a power outage. This
   is likely because the battery is discharged but could be due to other
   temporary conditions.
   When the battery is ready, the boot process will complete and services
   will be engaged.
   To override this delay, press 'c' followed by 'Enter'
   ```

5. Wenn die Warnmeldung in angezeigt wird Schritt 4, Nehmen Sie die folgenden Aktionen:

   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.

   b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.

      > **Achtung**: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden kann, kann dies zu einem Datenverlust führen.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Überspringen Sie Schritt 7 bis Schritt 12, und fahren Sie mit fort Schritt 13.
Ist ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware, die mit Storage-Arrays verbunden ist	a. Gehen Sie zu "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest" Und vervollständigen Sie die Unterabschnitte "Konfigurieren Sie FC-Ports auf node3" Und "UTA/UTA2-Ports in node3 prüfen und konfigurieren", Je nach Ihrem System. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 7. Sie müssen die integrierten FC-Ports, die integrierten CNA-Ports und CNA-Karten neu konfigurieren, bevor Sie ONTAP auf der V-Series oder dem System mit FlexArray Virtualisierungssoftware booten.

7. Fügen Sie die FC-Initiator-Ports des neuen Knotens zu den Switch-Zonen hinzu.

   Wenn Ihr System über ein Tape-SAN verfügt, müssen Sie das Zoning für die Initiatoren benötigen. Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

8. Fügen Sie die FC-Initiator-Ports zum Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

   Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

9. Ändern Sie die WWPN-Werte (World Wide Port Name) in den Host- oder Volume-Gruppen, die mit Array LUNs auf dem Speicher-Array verknüpft sind.

   Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

10. Wenn Ihre Konfiguration ein Switch-basiertes Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
11. Überprüfen Sie, ob die Array-LUNs jetzt für node3 sichtbar sind:

    ```
    sysconfig -v
    ```

    Das System zeigt alle Array-LUNs an, die für jeden FC-Initiator-Port sichtbar sind. Wenn die Array-LUNs nicht sichtbar sind, können Sie Festplatten von node1 zu node3 später in diesem Abschnitt nicht neu zuweisen.

12. Drücken Sie Strg-C, um das Boot-Menü anzuzeigen und den Wartungsmodus auszuwählen.
13. Geben Sie in der Eingabeaufforderung für den Wartungsmodus den folgenden Befehl ein:

    ```
    halt
    ```

    Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

14. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, auf das Sie aktualisieren, in einem ist…	Dann…
Dual-Chassis-Konfiguration (mit Controllern in anderem Chassis)	Gehen Sie zu Schritt 15.
Einzel-Chassis-Konfiguration (mit Controllern im selben Chassis)	a. Schalten Sie das Konsolenkabel von node3 auf node4 um. b. Schalten Sie node4 ein, und unterbrechen Sie den Bootvorgang, indem Sie am Konsolenterminal Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen. Die Stromversorgung sollte bereits eingeschaltet sein, wenn sich beide Controller im gleichen Chassis befinden. verlassen sie node4 an der Boot-Umgebung Eingabeaufforderung; Sie kehren nach node4 in zurück "installieren und booten sie node4". c. Wenn die Warnmeldung in angezeigt wird Schritt 4, Folgen Sie den Anweisungen in Schritt 5 d. Schalten Sie das Konsolenkabel von node4 nach node3 zurück. e. Gehen Sie zu Schritt 15.

15. node3 für ONTAP konfigurieren:

```
set-defaults
```

16. Wenn Sie NetApp Storage Encryption (NSE)-Laufwerke installiert haben, führen Sie die folgenden Schritte aus.

Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Wenden Sie sich an den NetApp Support, um Hilfe beim Wiederherstellen der integrierten Schlüsselmanagementinformationen zu erhalten.

17. [[man_install3_step17] Wenn die auf node3 installierte ONTAP-Version dieselbe oder höher als die auf node1 installierte Version von ONTAP 9 ist, führen Sie die Liste auf und weisen Sie Festplatten der neuen node3 neu zu:

```
boot_ontap
```

> Wenn dieser neue Node jemals in einem anderen Cluster oder HA-Paar verwendet wurde, müssen Sie ausgeführt werden `wipeconfig` Bevor Sie fortfahren. Andernfalls kann es zu Serviceausfällen oder Datenverlusten kommen. Wenden Sie sich an den technischen Support, wenn der Ersatz-Controller zuvor verwendet wurde, insbesondere dann, wenn auf den Controllern ONTAP im 7-Mode ausgeführt wurde.

18. Drücken Sie STRG-C, um das Startmenü anzuzeigen.
19. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	**Dann…**
Hat *Not* die richtige oder aktuelle ONTAP-Version auf node3	Gehen Sie zu Schritt 20.
Verfügt über die richtige oder aktuelle Version von ONTAP auf node3	Gehen Sie zu Schritt 25.

20. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie müssen den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder sonst kann während des Upgrades ein Datenausfall auftreten.

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

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

21. Netzboot auf node3 ausführen:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip>/<path_to_webaccessible_directory>/<ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Führt zu der Stelle, an der Sie das heruntergeladen haben `<ontap_version>_image.tgz` In "Schritt 1" Im Abschnitt *Vorbereiten für Netzboot*.

Unterbrechen Sie den Startvorgang nicht.

22. Wählen Sie im Startmenü die Option **(7) Neue Software installieren** zuerst.

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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.

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 Versionen von ONTAP. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt die Startmedien und platziert dieselbe ONTAP-Version-ONTAP auf beiden Bildpartitionen.

23. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie dazu aufgefordert werden, das Paket einzugeben, geben Sie die folgende URL ein:

    `http://<web_server_ip>/<path_to_web-accessible_directory>/<ontap_version_image>.tgz`

24. führen Sie die folgenden Teilschritte durch:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

25. Wählen Sie **(5) Boot im Wartungsmodus** aus, indem Sie eingeben `5`, Und geben Sie dann ein `y` Wenn Sie dazu aufgefordert werden, den Startvorgang fortzusetzen.

26. bevor Sie fortfahren, fahren Sie mit fort "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest" Um alle erforderlichen Änderungen an den FC- oder UTA/UTA2-Ports auf dem Node vorzunehmen.

    Nehmen Sie die in diesen Abschnitten empfohlenen Änderungen vor, booten Sie den Node neu und wechseln Sie in den Wartungsmodus.

27. Suche nach der System-ID von node3:

    `disk show -a`

    Das System zeigt die System-ID des Node sowie Informationen über seine Festplatten an, wie im folgenden Beispiel dargestellt:

```
 *> disk show -a
 Local System ID: 536881109
 DISK     OWNER                    POOL   SERIAL    HOME          DR
 HOME                                     NUMBER
 -------- -------------            -----  -------- -------------
-------------
 0b.02.23 nst-fas2520-2(536880939) Pool0  KPG2RK6F nst-fas2520-
2(536880939)
 0b.02.13 nst-fas2520-2(536880939) Pool0  KPG3DE4F nst-fas2520-
2(536880939)
 0b.01.13 nst-fas2520-2(536880939) Pool0  PPG4KLAA nst-fas2520-
2(536880939)
 ......
 0a.00.0               (536881109) Pool0  YFKSX6JG
(536881109)
 ......
```

Möglicherweise wird die Meldung angezeigt `disk show: No disks match option -a.` Nach Eingabe des Befehls. Dies ist keine Fehlermeldung, sodass Sie mit dem Verfahren fortfahren können.

28. Spares des Rasign node1, alle Festplatten, die zum Root gehören, und alle nicht-Root-Aggregate, die früher in node2 verschoben wurden "Verschiebung von nicht-Root-Aggregaten von node1 auf node2".

Geben Sie das entsprechende Formular des ein `disk reassign` Befehl basierend auf der Frage, ob Ihr System freigegebene Festplatten hat:

Wenn Sie auf Ihrem System freigegebene Festplatten, Hybrid-Aggregate oder beides haben, müssen Sie die korrekte verwenden `disk reassign` Befehl aus der folgenden Tabelle.

Wenn Disk-Typ…	Führen Sie dann den Befehl aus…
Mit gemeinsamen Festplatten	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`* `-p` *`node2_sysid`*
Ohne gemeinsame Festplatten	`disk reassign -s` *`node1_sysid`* `-d` *`node3_sysid`*

Für das *`node1_sysid`* Wert: Verwenden Sie die in erfassten Informationen "Node1-Informationen aufzeichnen". Um den Wert für zu erhalten *`node3_sysid`*, Verwenden Sie die `sysconfig` Befehl.

Der `-p` Die Option ist nur im Wartungsmodus erforderlich, wenn freigegebene Festplatten vorhanden sind.

Der `disk reassign` Befehl gibt nur die Festplatten wieder, für die *`node1_sysid`* Ist der aktuelle Eigentümer.

Vom System wird die folgende Meldung angezeigt:

```
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)?
```

29. Geben Sie ein `n`.

Vom System wird die folgende Meldung angezeigt:

```
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)?
```

30. Geben Sie ein `y`

Vom System wird die folgende Meldung angezeigt:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)?
```

31. Geben Sie ein `y`.

32. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (zum Beispiel AFF A800 Systeme), setzen Sie das node1-Aggregat als root ein, um zu bestätigen, dass node3 aus dem Root-Aggregat von node1 startet.

Warnung: Sie müssen die folgenden Teilschritte in der angegebenen Reihenfolge durchführen; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.

Im folgenden Verfahren wird node3 vom Root-Aggregat von node1 gestartet:

a. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node1 Aggregat:

```
aggr status -r
```

b. Überprüfen Sie den Status des node1-Aggregats:

```
aggr status
```

c. Bringen Sie das node1 Aggregat ggf. online:

```
aggr_online root_aggr_from_node1
```

d. Verhindern Sie, dass das node3 vom ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node3
```

e. Legen Sie das node1-Root-Aggregat als das neue Root-Aggregat für node3 fest:

```
aggr options aggr_from_node1 root
```

f. Überprüfen Sie, ob das Root-Aggregat von node3 offline ist und das Root-Aggregat für die von node1 hergebrachten Festplatten online ist und in den Root-Status eingestellt ist:

```
aggr status
```

> Wenn der vorherige Unterschritt nicht ausgeführt wird, kann node3 vom internen Root-Aggregat booten, oder es kann dazu führen, dass das System eine neue Cluster-Konfiguration übernimmt oder Sie aufgefordert werden, eine zu identifizieren.

Im Folgenden wird ein Beispiel für die Befehlsausgabe angezeigt:

```
-------------------------------------------------------------------
     Aggr State               Status          Options
aggr0_nst_fas8080_15 online   raid_dp, aggr   root, nosnap=on
                              fast zeroed
                              64-bit

  aggr0 offline               raid_dp, aggr   diskroot
                              fast zeroed
                              64-bit
-------------------------------------------------------------------
```

33. Überprüfen Sie, ob Controller und Chassis als konfiguriert sind `ha`:

```
ha-config show
```

Im folgenden Beispiel wird die Ausgabe des Befehls ha-config show angezeigt:

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

Systeme zeichnen sich in einem programmierbaren ROM (PROM) auf, unabhängig davon, ob sie sich in einem HA-Paar oder einer eigenständigen Konfiguration befinden. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

Wenn der Controller und das Chassis nicht als „ha“ konfiguriert wurden, korrigieren Sie die Konfiguration mit den folgenden Befehlen:

```
ha-config modify controller ha

ha-config modify chassis ha
```

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um den Controller und das Chassis zu ändern:

```
ha-config modify controller mcc

ha-config modify chassis mcc
```

34. zerstören Sie die Mailboxen auf node3:

```
mailbox destroy local
```

Über die Konsole wird die folgende Meldung angezeigt:

```
Destroying mailboxes forces a node to create new empty mailboxes, which
clears any takeover state, removes all knowledge of out-of-date plexes
of mirrored volumes, and will prevent management services from going
online in 2-node cluster HA configurations. Are you sure you want to
destroy the local mailboxes?
```

35. Geben Sie ein `y` Bestätigen Sie an der Eingabeaufforderung, dass Sie die lokalen Mailboxen zerstören möchten.
36. Wartungsmodus beenden:

```
halt
```

Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

37. auf node2 überprüfen Sie Datum, Uhrzeit und Zeitzone des Systems:

```
date
```

38. auf node3 prüfen Sie das Datum an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

39. Ggf. Das Datum auf node3 einstellen:

```
set date mm/dd/yyyy
```

40. in node3 überprüfen Sie die Zeit an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

41. Ggf. Die Zeit auf node3 einstellen:

```
set time hh:mm:ss
```

42. Überprüfen Sie, ob die Partner-System-ID korrekt festgelegt ist, wie in angegeben Schritt 28 Schalter unter -p:

```
printenv partner-sysid
```

43. Ggf. Setzen Sie die Partner-System-ID auf node3:

    `setenv partner-sysid node2_sysid`

    Einstellungen speichern:

    `saveenv`

44. Öffnen Sie das Boot-Menü an der Eingabeaufforderung der Boot-Umgebung:

    `boot_ontap menu`

45. Wählen Sie im Boot-Menü die Option **(6) Flash aus Backup config** aktualisieren, indem Sie eingeben `6` An der Eingabeaufforderung.

    Vom System wird die folgende Meldung angezeigt:

    ```
    This will replace all flash-based configuration with the last backup to
    disks. Are you sure you want to continue?:
    ```

46. Geben Sie ein `y` An der Eingabeaufforderung.

    Der Startvorgang läuft normal weiter, und das System fordert Sie dann auf, die Unstimmigkeit der System-ID zu bestätigen.

    > Das System wird möglicherweise zweimal neu gestartet, bevor die Warnmeldung zur Nichtübereinstimmung angezeigt wird.

47. Bestätigen Sie die Diskrepanz, wie im folgenden Beispiel gezeigt:

    ```
    WARNING: System id mismatch. This usually occurs when replacing CF or
    NVRAM cards!
    Override system id (y|n) ? [n] y
    ```

    Der Node kann vor dem normalen Booten eine Runde des Neubootens durchlaufen.

48. Einloggen in node3.

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node3 fest

Wenn node3 integrierte FC-Ports, Onboard Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschluss abschließen Konfigurieren Sie FC-Ports auf node3, Oder UTA/UTA2-Ports in node3 prüfen und konfigurieren, Oder beide Abschnitte.

Für das NetApp Marketingmaterial wird möglicherweise der Begriff „UTA2“ verwendet, um CNA-Adapter und Ports zu beziehen. Die CLI verwendet jedoch den Begriff „CNA“.

- Wenn node3 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie zur springen "Ports von node1 nach node3 zuordnen".
- Wenn Sie jedoch ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware mit Storage-Arrays haben und node3 keine integrierten FC-Ports, Onboard UTA/UTA-Ports oder eine UTA/UTA2-Karte haben, kehren Sie zurück zu *Install and Boot node3* und fahren Sie fort "Schritt 22".

Optionen:

- Konfigurieren Sie FC-Ports auf node3
- UTA/UTA2-Ports in node3 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node3

Wenn node3 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in Betrieb nehmen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node1 haben, die Sie in gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder eine UTA/UTA2-Karte verfügt, konfigurieren Sie sie in UTA/UTA2-Ports in node3 prüfen und konfigurieren.

Wenn Ihr System über Speicherfestplatten verfügt, geben Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle ein. Wenn Sie über ein V-Series System oder über FlexArray-Virtualisierungssoftware verfügen und mit Storage-Arrays verbunden sind, geben Sie im Wartungsmodus in diesem Abschnitt Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Gehen Sie zu Schritt 5
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 2

2. Boot node3 und Zugriff auf Wartungsmodus:

```
boot_ontap maint
```

3. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Geben Sie den folgenden Befehl ein: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden.	Geben Sie den folgenden Befehl ein `ucadmin show`

Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

4. Vergleichen Sie die FC-Einstellungen von node3 mit den Einstellungen, die Sie zuvor aus node1 erfasst haben.
5. Nehmen Sie eine der folgenden Aktionen:

Wenn die FC-Standardeinstellungen auf den neuen Nodes sind…	Dann…
Das gleiche wie jene, die ihr auf Node1 gefangen habt	Gehen Sie zu Schritt 11.
Anders als jene, die du auf Node1 gefangen hast	Gehen Sie zu Schritt 6.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node3 nach Bedarf, indem Sie einen der folgenden Befehle eingeben: • So programmieren Sie Zielanschlüsse: `system node hardware unified-connect modify -type
-t target -adapter *port_name*` ** So programmieren Sie Initiator-Ports: `system node hardware unified-connect modify -type	-t initiator -adapter *port_name*`  `-t` Ist der FC4-Typ: Target oder Initiator.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node3 nach Bedarf, indem Sie den folgenden Befehl eingeben: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

7. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `ucadmin show`

8. Beenden des Wartungsmodus durch Eingabe des folgenden Befehls:

```
halt
```

9. nach Eingabe des Befehls warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
10. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder verfügt FlexArray Virtualisierungssoftware mit Clustered Data ONTAP 8.3	Boot Node3 und Wartung an der Eingabeaufforderung für die Boot-Umgebung: `boot_ontap maint`
Ist kein V-Series System oder verfügt über keine FlexArray Virtualisierungssoftware	Boot node3 an der Eingabeaufforderung Boot-Umgebung: `boot_ontap`

11. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Wenn node3 eine UTA/UTA2-Karte oder Onboard-Ports zu UTA/UTA2 hat, gehen Sie zu UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn node3 keine UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2 hat, überspringen UTA/UTA2-Ports in node3 prüfen und konfigurieren Und gehen Sie zu "Ports von node1 nach node3 zuordnen".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Wenn kein Knoten 3 über eine Karte oder Onboard-Ports verfügt, gehen Sie zu UTA/UTA2-Ports in node3 prüfen und konfigurieren. • Wenn kein Karten- oder Onboard-Port für node3 vorhanden ist, überspringen Sie UTA/UTA2-Ports in node3 prüfen und konfigurieren, Und zurück zu *Install und Boot node3* und wieder bei "Schritt 7".

UTA/UTA2-Ports in node3 prüfen und konfigurieren

Wenn node3 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie möglicherweise neu konfigurieren, je nachdem, wie Sie das aktualisierte System verwenden möchten.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

Wenn Sie einen Unified Target Adapter (UTA/UTA2)-Port für FC verwenden möchten, müssen Sie zuerst überprüfen, wie der Port konfiguriert ist.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

Sie können das verwenden `ucadmin show` Befehl zum Überprüfen der aktuellen Portkonfiguration:

```
*> ucadmin show
          Current  Current    Pending  Pending    Admin
 Adapter  Mode     Type       Mode     Type       Status
 -------  -------  ---------  -------  ---------  -----------
 0e       fc       target     -        initiator  offline
 0f       fc       target     -        initiator  offline
 0g       fc       target     -        initiator  offline
 0h       fc       target     -        initiator  offline
 1a       fc       target     -        -          online
 1b       fc       target     -        -          online
6 entries were displayed.
```

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht gleichzeitige NIC- und FCoE-Traffic über die gleiche 10-GbE-SFP+-Schnittstelle und unterstützt FC-Ziele.

UTA/UTA2-Ports befinden sich möglicherweise auf einem Adapter oder auf dem Controller und verfügen über die folgenden Konfigurationen. Sie sollten jedoch die Konfiguration der UTA/UTA2-Ports auf der node3 überprüfen und gegebenenfalls ändern:

- UTA-/UTA2-Karten, die bestellt werden, werden vor dem Versand konfiguriert, um die von Ihnen geforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden vor dem Versand konfiguriert, um die Persönlichkeit zu erhalten, die Sie anfordern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, müssen Sie an der Eingabeaufforderung des Clusters die Befehle in diesem Abschnitt eingeben, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein VSeries-System verfügen oder über FlexArray-Virtualisierungssoftware verfügen und mit Speicherarrays verbunden sind, müssen Sie in diesem Abschnitt Befehle in der Eingabeaufforderung für den Wartungsmodus eingeben. Sie müssen sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit konfiguriert sind, und geben Sie auf node3 die folgenden Befehle ein:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt eine Ausgabe an, die den folgenden Beispielen entspricht:

```
cluster1::> system node hardware unified-connect show

                 Current  Current    Pending  Pending  Admin
Node  Adapter    Mode     Type       Mode     Type     Status
----  -------    -------  ---------  -------  -------  ------
f-a   0e         fc       initiator  -        -        online
f-a   0f         fc       initiator  -        -        online
f-a   0g         cna      target     -        -        online
f-a   0h         cna      target     -        -        online
f-b   0e         fc       initiator  -        -        online
f-b   0f         fc       initiator  -        -        online
f-b   0g         cna      target     -        -        online
f-b   0h         cna      target     -        -        online
12 entries were displayed.
```

```
*> ucadmin show
          Current  Current    Pending  Pending  Admin
Adapter   Mode     Type       Mode     Type     Status
-------   -------  ---------  -------  -------  ------
0e        fc       initiator  -        -        online
0f        fc       initiator  -        -        online
0g        cna      target     -        -        online
0h        cna      target     -        -        online
0e        fc       initiator  -        -        online
0f        fc       initiator  -        -        online
0g        cna      target     -        -        online
0h        cna      target     -        -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Untersuchung der Ausgabe des `system node hardware unified-connect show` Oder `ucadmin show` Befehl zum Bestimmen, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.

4. Nehmen Sie eine der folgenden Aktionen:

Wenn die UTA/UTA2-Ports…	**Dann…**
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Es gibt Storage-Festplatten, auf denen Clustered Data ONTAP 8.3 ausgeführt wird	Boot-Knoten3 und wechseln in den Wartungsmodus: `boot_ontap maint`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 6. Sie sollten sich bereits im Wartungsmodus befinden.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7.
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

7. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

   `storage disable adapter` *`adapter_name`*

   Adapter im Ziel-Modus sind im Wartungsmodus automatisch offline.

8. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, ändern Sie die Konfiguration nach Bedarf:

   `ucadmin modify -m fc|cna -t initiator|target` *`adapter_name`*

   - `-m` Ist der Persönlichkeitsmodus, `fc` Oder `cna`.
   - `-t` Ist der Typ FC4, `target` Oder `initiator`.

   > Sie müssen FC Initiator für Tape-Laufwerke, FlexArray Virtualisierungssysteme und MetroCluster Konfigurationen verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

9. Überprüfen Sie die Einstellungen:

   `ucadmin show`

10. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…

Festplatten sind vorhanden	a. Anhalten des Systems:
	`halt`
	Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.
	b. Geben Sie den folgenden Befehl ein:
	`boot_ontap`

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Neubooten in den Wartungsmodus: `boot_netapp maint`

11. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist eine V-Series oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`:

```
cluster1::> system node hardware unified-connect show

                Current  Current    Pending  Pending      Admin
Node  Adapter  Mode     Type       Mode     Type         Status
----  -------  -------  ---------  -------  -----------  ------
f-a   1a       fc       initiator  -        -            online
f-a   1b       fc       target     -        initiator    online
f-a   2a       fc       target     cna      -            online
f-a   2b       fc       target     cna      -            online

4 entries were displayed.
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  ------
1a       fc       initiator  -        -          online
1b       fc       target     -        initiator  online
2a       fc       target     cna      -          online
2b       fc       target     cna      -          online
*>
```

12. Platzieren Sie alle Zielports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

13. Anschluss verkabeln.
14. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Ports von node1 nach node3 zuordnen".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zu *Install and Boot node3* zurück und fahren Sie bei fort "Schritt 7".

Ports von node1 nach node3 zuordnen

Sie müssen sicherstellen, dass die physischen Ports auf node1 den physischen Ports auf node3 korrekt zugeordnet werden. Somit kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Bevor Sie beginnen

Sie müssen von *Hardware Universe* bereits über die Ports auf den neuen Nodes verfügen. (Gehen Sie zu "Quellen" Zum Verknüpfen mit dem *Hardware Universe*). Sie verwenden die Informationen später in diesem Abschnitt und in "Weisen Sie Ports von node2 nach node4 zu".

Die Softwarekonfiguration von node3 muss mit der physischen Konnektivität von node3 übereinstimmen. Die IP-Konnektivität muss wiederhergestellt werden, bevor Sie mit dem Upgrade fortfahren.

Über diese Aufgabe

Die Port-Einstellungen können je nach Modell der Nodes variieren.

Sie müssen den Port des ursprünglichen Node und die LIF-Konfiguration mit dem kompatibel machen, was Sie planen, die Konfiguration des neuen Node zu verwenden. Dies liegt daran, dass der neue Node beim Booten der gleichen Konfiguration wiedergibt. Dies bedeutet, dass ONTAP beim Booten von node3 versuchen wird, LIFs auf den gleichen Ports zu hosten, die in node1 verwendet wurden.

Wenn also die physischen Ports auf node1 nicht direkt den physischen Ports auf node3 zugeordnet werden, sind daher Änderungen der Software-Konfiguration erforderlich, um nach dem Booten die Cluster-, Management- und Netzwerkkonnektivität wiederherzustellen. Wenn die Cluster-Ports auf node1 zudem nicht direkt den Cluster-Ports auf node3 zugeordnet werden, wird node3 möglicherweise nicht automatisch dem Quorum beitreten, wenn es neu gestartet wird, bis eine Software-Konfiguration geändert wird, um die Cluster LIFs auf den korrekten physischen Ports zu hosten.

Schritte

1. in der folgenden Tabelle alle Kabelinformationen node1 für node1, die Ports, Broadcast-Domänen und IPspaces erfassen:

LIF	Anzahl an Knoten1-Ports	Node1-IPspaces	Node1 Broadcast-Domäne	Node3-Ports	Node3-Ports	Node3 Broadcast-Domänen
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Cluster 5						
Cluster 6						
Node-Management						
Cluster-Management						
Daten 1						
Daten 2						
Daten 3						
Daten 4						
San						
Intercluster-Port						

   Siehe "Node1-Informationen aufzeichnen" Für die Schritte zum Einerhalten dieser Informationen.

2. Alle Verkabelungsinformationen für node3, die Ports, Broadcast-Domänen und IPspaces in der vorherigen Tabelle mit demselben Verfahren in erfassen "Node1-Informationen aufzeichnen".
3. Überprüfen Sie anhand der folgenden Schritte, ob es sich bei dem Setup um ein Cluster mit zwei Nodes ohne Switches handelt:

a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
cluster::> set -privilege advanced
```

b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
network options switchless-cluster show
```

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

+
Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

a. Zurück zur Administratorberechtigungsebene:

```
cluster::*> set -privilege admin
cluster::>
```

4. Holen Sie sich Node3 in Quorum, indem Sie die folgenden Schritte durchführen:

a. Boot-Knoten 3. Siehe "Installieren und booten Sie node3" Um den Node zu booten, wenn Sie dies noch nicht getan haben.

b. Vergewissern Sie sich, dass sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden:

```
network port show -node node-name -port port-name -fields broadcast-domain
```

Das folgende Beispiel zeigt, dass Port „e0a“ sich in der „Cluster“-Domäne auf node3 befindet:

```
 cluster::> network port show -node node3 -port e0a -fields
broadcast-domain

 node       port broadcast-domain
 ---------- ---- ----------------
 node3      e1a  Cluster
```

c. Fügen Sie die korrekten Ports zur Cluster Broadcast-Domäne hinzu:

```
network port modify -node node-name -port port-name -ipspace Cluster -mtu
9000
```

Dieses Beispiel fügt Cluster-Port „e1b“ auf Knoten3 hinzu:

```
network port modify -node node3 -port e1b -ipspace Cluster -mtu 9000
```

Bei einer MetroCluster-Konfiguration können Sie die Broadcast-Domäne unter einem Port möglicherweise nicht ändern, da dieser mit einem Port verknüpft ist, der die LIF einer synchronen-Ziel-SVM hostet. Außerdem werden Fehler angezeigt, die ähnlich sind, jedoch nicht auf die folgende Meldung beschränkt sind`:

```
command failed: This operation is not permitted on a Vserver that is
configured as the destination of a MetroCluster Vserver relationship.
```

Geben Sie den folgenden Befehl von der entsprechenden Quell-SVM auf dem Remote-Standort ein, um die synchrone Ziel-LIF einem entsprechenden Port zuzuweisen:

```
metrocluster vserver resync -vserver Vserver-name
```

d. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

```
network interface migrate -vserver Cluster -lif LIF-name -source-node node3
-destination-node node3 -destination-port port-name
```

e. Ändern Sie den Startport der Cluster-LIFs:

```
network interface modify -vserver Cluster -lif LIF-name –home-port port-name
```

f. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domain befinden, fügen Sie sie hinzu:

```
network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain
Cluster -ports node:port
```

g. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne:

```
network port broadcast-domain remove-ports
```

Im folgenden Beispiel wird der Port „e0d“ auf node3 entfernt:

```
network port broadcast-domain remove-ports -ipspace Cluster -broadcast
-domain Cluster -ports <node3:e0d>
```

a. Vergewissern Sie sich, dass node3 erneut dem Quorum beigetreten ist:

```
cluster show -node node3 -fields health
```

5. passen Sie die Broadcast-Domänen an, die Ihre Cluster-LIFs hosten, sowie LIFs für Node-Management und/oder Cluster-Management. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie die LIFs möglicherweise wie folgt migrieren und ändern müssen:

a. Zeigen Sie den Startport einer logischen Schnittstelle an:

```
network interface show -fields home-node,home-port
```

b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:

```
network port broadcast-domain add-ports
```

```
network port broadcast-domain remove-ports
```

a. Ändern Sie den Home-Port eines LIF:

```
network interface modify -vserver Vserver-name -lif LIF-name –home-port
port-name
```

6. passen Sie die Intercluster-Broadcast-Domänen an und migrieren Sie die LIFs, falls erforderlich, mithilfe derselben Befehle wie in dargestellt Schritt 5.
7. passen Sie alle anderen Broadcast-Domänen an und migrieren Sie die Daten-LIFs, falls erforderlich, mit denselben Befehlen in Schritt 5.
8. Wenn auf node1 keine Ports mehr vorhanden sind, gehen Sie wie folgt vor, um sie zu löschen:

a. Zugriff auf die erweiterte Berechtigungsebene auf beiden Nodes:

```
set -privilege advanced
```

b. Löschen Sie die Ports:

```
network port delete -node node-name -port port-name
```

c. Zurück zur Administratorebene:

```
set -privilege admin
```

9. Anpassen aller LIF Failover-Gruppen:

```
network interface modify -failover-group failover-group -failover-policy
failover-policy
```

Im folgenden Beispiel wird die Failover-Richtlinie auf „Broadcast-Domain-wide“ gesetzt und verwendet die Ports in Failover-Gruppe „fg1“ als Failover-Ziele für LIF „data1“ auf „node3“:

```
network interface modify -vserver node3 -lif data1 failover-policy
broadcast-domainwide -failover-group fg1
```

Gehen Sie zu "Quellen" Link zu *Netzwerkverwaltung* oder den Befehlen *ONTAP 9: Manual Page Reference* für weitere Informationen.

10. Überprüfen Sie die Änderungen auf node3:

```
network port show -node node3
```

11. Jedes Cluster-LIF muss an Port 7700 zuhören. Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören:

```
::> network connections listening show -vserver Cluster
```

Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

```
::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
int modify -vserver Cluster -lif cluster-lif -status-admin up
```

Wiederholen Sie Schritt 11, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

Überprüfen Sie die Installation von node3

Nach der Installation und dem Booten von node3 müssen Sie überprüfen, ob er korrekt installiert ist, dass er Teil des Clusters ist und mit node2 kommunizieren kann.

Schritte

1. an der Systemaufforderung melden Sie sich bei node3 an. Überprüfen Sie dann, ob node3 Teil desselben Clusters ist wie node2 und sich in einem ordnungsgemäßen Zustand:

```
cluster show
```

2.] überprüft, ob node3 mit node2 kommunizieren kann und dass alle LIFs aktiv sind:

```
network interface show -curr-node node3
```

3. Nehmen Sie eine der folgenden Aktionen:

Falls das Cluster…	Dann…
In einer SAN-Umgebung erfolgreich positionieren	Vollständig Schritt 4 Und gehen Sie dann zum Abschnitt "Das Verschieben von NAS-Daten-LIFs von node1 von node2 auf node3 und die Überprüfung von SAN-LIFs auf node3".
Nicht in einer SAN-Umgebung	Überspringen Sie Schritt 4, und fahren Sie mit fort "Das Verschieben von NAS-Daten-LIFs von node1 von node2 auf node3 und die Überprüfung von SAN-LIFs auf node3".

4. Überprüfen Sie, dass node2 und node3 im Quorum sind, indem Sie auf einem der Knoten den folgenden Befehl eingeben und dessen Ausgabe prüfen:

   `event log show -messagename scsiblade.*`

   Das folgende Beispiel zeigt die Ausgabe, wenn sich die Nodes im Cluster im Quorum befinden:

```
cluster::> event log show -messagename scsiblade.*
Time                Node   Severity      Event
------------------- ------ ------------- -------------------------
8/13/2012 14:03:51  node1  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:51  node2  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:48  node3  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:43  node4  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
```

Verschieben Sie die NAS-Daten-LIFs von node1 auf node2 und überprüfen Sie SAN LIFs auf node3

Nachdem Sie die Installation node3 überprüft haben und bevor Sie Aggregate von node2 auf node3 verschieben, müssen Sie die NAS-Daten-LIFs von node1 verschieben, die sich derzeit in node2 von node2 auf node3 befinden. Sie müssen außerdem die SAN-LIFs auf node3 überprüfen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

Schritte

1. Listen Sie alle NAS-Daten-LIFs auf, die nicht im Besitz von node2 sind, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe erfassen:

   `network interface show -role data -curr-node` *`node2`* `-is-home false -home-node` *`node3`*

2. Wenn das Cluster für SAN-LIFs konfiguriert ist, notieren Sie die SAN-LIFs `adapter` Und `switch-port` Konfigurationsinformationen in diesem "Arbeitsblatt" Zur späteren Verwendung im Verfahren.

   a. Führen Sie die SAN-LIFs auf node2 auf und untersuchen Sie die Ausgabe:

      `network interface show -data-protocol fc*`

      Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> net int show -data-protocol fc*
  (network interface show)
            Logical     Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node
Port    Home
----------- ----------  ---------- ------------------ -------------
------- ----
svm2_cluster1
            lif_svm2_cluster1_340
                        up/up      20:02:00:50:56:b0:39:99
                                                      cluster1-01
1b      true
            lif_svm2_cluster1_398
                        up/up      20:03:00:50:56:b0:39:99
                                                      cluster1-02
1a      true
            lif_svm2_cluster1_691
                        up/up      20:01:00:50:56:b0:39:99
                                                      cluster1-01
1a      true
            lif_svm2_cluster1_925
                        up/up      20:04:00:50:56:b0:39:99
                                                      cluster1-02
1b      true
4 entries were displayed.
```

b. Führen Sie die vorhandenen Konfigurationen auf und untersuchen Sie die Ausgabe:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Nehmen Sie eine der folgenden Aktionen:

Falls Knoten 1…	Dann…
Schnittstellengruppen oder VLANs wurden konfiguriert	Gehen Sie zu Schritt 4.
Schnittstellengruppen oder VLANs waren nicht konfiguriert	Überspringen Sie Schritt 4, und fahren Sie mit fort Schritt 5.

4. führen Sie die folgenden Teilschritte durch, um alle auf Schnittstellengruppen und VLANs gehosteten NAS-Daten-LIFs zu migrieren, die sich ursprünglich auf node1 von node2 auf node3 befanden:

   a. Migrieren Sie alle auf node2 gehosteten Daten-LIFs, die zuvor zu node1 auf einer Schnittstellengruppe gehörten, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

   ```
   network interface migrate -vserver vserver_name -lif LIF_name -destination
   -node node3 -destination-port netport|ifgrp
   ```

   b. Ändern Sie den Home-Port und den Home-Node der LIF in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node3 -home-port netport|ifgrp
   ```

   c. Migrieren Sie alle auf node2 gehosteten Daten-LIFs, die zuvor zu node1 auf einem VLAN-Port gehörten, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem

Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node3 -home-port netport|ifgrp
```

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 6 Und Schritt 7, überspringen Sie Schritt 8, und abgeschlossen Schritt 9 Bis Schritt 12.
San	Deaktivieren Sie alle SAN-LIFs auf dem Node, um sie für das Upgrade herunterzufahren: `network interface modify -vserver *vserver_name* -lif *LIF_name* -home-node *node_to_upgrade* -home-port _netport

6. Wenn Datenports auf Ihren Plattformen nicht identisch sind, fügen Sie die Ports zur Broadcast-Domäne hinzu:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „6280-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain „Management“ im IPspace „Standard“ hinzu:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrieren Sie jede NAS-Daten-LIF auf node3, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

8. stellen Sie sicher, dass die Datenmigration persistent ist:

```
network interface modify -vserver vserver_name -lif LIF_name-home-port
netport|ifgrp -home-node node3
```

9. Bestätigen, dass sich die SAN-LIFs auf den richtigen Ports auf node3 befinden:

a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

```
network interface show -data-protocol iscsi|fcp -home-node node3
```

Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster::> net int show -data-protocol iscsi|fcp -home-node node3
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node
Port     Home
 -----------  ----------  ----------  ------------------
-------------  -------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node3
a0a      true
              data1       up/up       10.63.0.50/18       node3
e0c      true
              rads1       up/up       10.63.0.51/18       node3
e1a      true
              rads2       up/down     10.63.0.52/24       node3
e1b      true
 vs1
              lif1        up/up       172.17.176.120/24   node3
e0c      true
              lif2        up/up       172.17.176.121/24   node3
e1a      true
```

b. Überprüfen Sie das neue und `adapter` Und `switch-port` Die Konfigurationen sind korrekt, indem die Ausgabe von dem verglichen wird `fcp adapter show` Befehl mit den Konfigurationsinformationen, die Sie im Arbeitsblatt in aufgezeichnet haben Schritt 2.

Liste der neuen SAN LIF-Konfigurationen auf Knoten3:

```
fcp adapter show -fields switch-port,fc-wwpn
```

Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter fc-wwpn                 switch-port
------------ ------- ----------------------- -------------
cluster1-01 0a      50:0a:09:82:9c:13:38:00 ACME Switch:0
cluster1-01 0b      50:0a:09:82:9c:13:38:01 ACME Switch:1
cluster1-01 0c      50:0a:09:82:9c:13:38:02 ACME Switch:2
cluster1-01 0d      50:0a:09:82:9c:13:38:03 ACME Switch:3
cluster1-01 0e      50:0a:09:82:9c:13:38:04 ACME Switch:4
cluster1-01 0f      50:0a:09:82:9c:13:38:05 ACME Switch:5
cluster1-01 1a      50:0a:09:82:9c:13:38:06 ACME Switch:6
cluster1-01 1b      50:0a:09:82:9c:13:38:07 ACME Switch:7
cluster1-02 0a      50:0a:09:82:9c:6c:36:00 ACME Switch:0
cluster1-02 0b      50:0a:09:82:9c:6c:36:01 ACME Switch:1
cluster1-02 0c      50:0a:09:82:9c:6c:36:02 ACME Switch:2
cluster1-02 0d      50:0a:09:82:9c:6c:36:03 ACME Switch:3
cluster1-02 0e      50:0a:09:82:9c:6c:36:04 ACME Switch:4
cluster1-02 0f      50:0a:09:82:9c:6c:36:05 ACME Switch:5
cluster1-02 1a      50:0a:09:82:9c:6c:36:06 ACME Switch:6
cluster1-02 1b      50:0a:09:82:9c:6c:36:07 ACME Switch:7
16 entries were displayed
```

Wenn sich ein SAN LIF in der neuen Konfiguration nicht auf einem Adapter befindet, der noch an denselben angeschlossen ist `switch-port`, Es kann zu einem Systemausfall führen, wenn Sie den Node neu booten.

c. Wenn node3 irgendwelche SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der nicht in node1 vorhanden war oder einem anderen Port zugeordnet werden muss, verschieben Sie sie zu einem geeigneten Port auf node3, indem Sie die folgenden Teilschritte ausführen:

   i. Legen Sie den LIF-Status auf „down“ fest:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status -admin down`

   ii. Entfernen Sie das LIF aus dem Portsatz:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Geben Sie einen der folgenden Befehle ein:

      - Verschieben eines einzelnen LIF:

        `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home -port` *`new_home_port`*

      - Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen

neuen Port:

```
network interface modify {-home-port port_on_node1 -home-node node1
-role data} -home-port new_home_port_on_node3
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

> Sie müssen SAN-LIFs zu einem Port verschieben, der die gleiche Verbindungsgeschwindigkeit wie der ursprüngliche Port hat.

10. Ändern Sie den Status aller LIFs auf „up“, damit die LIFs den Datenverkehr auf dem Node akzeptieren und senden können:

```
network interface modify -home-port port_name -home-node node3 -lif data
-status-admin up
```

11. Geben Sie an jedem Node den folgenden Befehl ein, und überprüfen Sie seine Ausgabe, um zu überprüfen, ob LIFs an die richtigen Ports verschoben wurden und ob die LIFs den Status von „up“ aufweisen. Geben Sie dazu den folgenden Befehl an einem der Nodes ein und überprüfen Sie die Ausgabe:

```
network interface show -home-node node3 -role data
```

12. Wenn eine der LIFs nicht verfügbar ist, setzen Sie den Administrationsstatus der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

13. Senden Sie eine AutoSupport Nachricht nach dem Upgrade an NetApp für den Knoten1:

```
system node autosupport invoke -node node3 -type all -message "node1
successfully upgraded from platform_old to platform_new"
```

Arbeitsblatt: Informationen, die aufgezeichnet werden sollen, bevor NAS-Daten-LIFs in node3 verschoben werden

Um zu überprüfen, ob Sie die richtige Konfiguration haben, nachdem Sie SAN LIFs von node2 auf node3 verschoben haben, können Sie das folgende Arbeitsblatt verwenden, um die aufzuzeichnen `adapter` Und `switch-port` Informationen für jedes LIF.

Notieren Sie das LIF `adapter` Informationen aus dem `network interface show -data-protocol fc*` Befehlsausgabe und das `switch-port` Informationen aus dem `fcp adapter show -fields switch-port,fc-wwpn` Befehlsausgabe für node2.

Notieren Sie nach Abschluss der Migration zu node3 die LIF `adapter` Und `switch-port` Informationen für die LIFs auf Knoten 3 und überprüfen Sie, dass jede LIF noch mit derselben verbunden ist `switch-port`.

Knoten 2			Node3		
LIF	adapter	switch-port	LIF	adapter	switch-port

Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3

Bevor Sie node2 durch node4 ersetzen können, müssen Sie eine AutoSupport-Nachricht für node2 senden und dann die nicht-Root-Aggregate verschieben, die im Besitz von node2 sind, in node3.

Schritte

1. Senden Sie eine AutoSupport-Nachricht an NetApp für node2:

   `system node autosupport invoke -node` *`node2`* `-type all -message "Upgrading` *`node2`* `from` *`platform_old`* `to` *`platform_new`*`"`

2. Überprüfen Sie, ob die AutoSupport Meldung gesendet wurde:

   `system node autosupport show -node` *`node2`* `-instance`

   Die Felder „Letzter Betreff gesendet:“ und „Letzter Zeitpunkt gesendet:“ enthalten den Nachrichtentitel der letzten gesendeten Nachricht und den Zeitpunkt, zu dem die Nachricht gesendet wurde.

3. Verschiebung der nicht-Root-Aggregate:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

   b. Listen Sie die Aggregate auf, die Eigentum von node2 sind:

      `storage aggregate show -owner-name` *`node2`*

   c. Starten Sie die Aggregatverschiebung:

      `storage aggregate relocation start -node` *`node2`* `-destination` *`node3`* `-aggregate -list * -ndo-controller-upgrade true`

      Der Befehl sucht nur Aggregate außerhalb des Root-Bereichs.

   a. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge finden im Hintergrund statt. Für die Verschiebung eines Aggregats kann dieser Zeitraum von

wenigen Sekunden bis hin zu einigen Minuten dauern. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

4. Überprüfen Sie den Versetzungsstatus von node2:

```
storage aggregate relocation show -node node2
```

Die Ausgabe zeigt „Fertig“ für ein Aggregat an, nachdem es verschoben wurde.

Sie müssen warten, bis alle Aggregate, die sich im Besitz von node2 befinden, in node3 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

5. Führen Sie eine der folgenden Aktionen durch:

Bei Umzug von…	Dann…
Alle Aggregate waren erfolgreich	Gehen Sie zu Schritt 6.

Bei Umzug von…	Dann…

Aggregate sind ausgefallen oder sie wurden Vetos	a. Detaillierte Statusmeldung anzeigen:
	`storage aggregate show -instance`
	Sie können auch die EMS-Protokolle überprüfen, um die erforderlichen Korrekturmaßnahmen anzuzeigen.
	Der `event log show` Befehl listet alle Fehler auf, die aufgetreten sind.
	b. Führen Sie die Korrekturmaßnahme durch.
	c. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	d. Verschiebung ausgefallener oder Vetos von Aggregaten:
	`storage aggregate relocation start -node node2 -destination node3 -aggregate-list * -ndo -controllerupgrade true`
	e. Geben Sie bei der entsprechenden Aufforderung ein `y`.
	f. Zurück zur Administratorberechtigungsebene:
	`set -privilege admin`
	Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen:
	• Durch Überschreiben von Veto-Prüfungen:
	`storage aggregate relocation start -override -vetoes true -ndo-controller-upgrade`
	• Durch Überschreiben von Zielprüfungen:
	`storage aggregate relocation start -override -destination-checks true -ndocontroller-upgrade`
	Weitere Informationen zu den Befehlen für die Verschiebung des Storage-Aggregats finden Sie unter "Quellen" Verbinden mit *Disk und Aggregat-Management mit den Befehlen CLI* und *ONTAP 9: Manual Page Reference*.

6. Stellen Sie sicher, dass alle nicht-Root-Aggregate online sind auf node3:

`storage aggregate show -node node3 -state offline -root false`

Wenn irgendwelche Aggregate offline gegangen sind oder fremd geworden sind, müssen Sie sie online

bringen, einmal für jedes Aggregat:

`storage aggregate online -aggregate aggr_name`

7. Vergewissern Sie sich, dass alle Volumes auf node3 online sind:

   `volume show -node node3 -state offline`

   Wenn Volumes auf Knoten3 offline sind, müssen Sie sie einmal für jedes Volume online bringen:

   `volume online -vserver Vserver-name -volume volume-name`

8. Vergewissern Sie sich, dass node2 keine Online-Aggregate besitzt, die nicht im Root-Modus sind:

   `storage aggregate show -owner-name node2 -ha-policy sfo -state online`

   Die Befehlsausgabe sollte nicht online nicht-Root-Aggregate anzeigen, da alle nicht-Root-Online-Aggregate bereits in node3 verschoben wurden.

Verschieben Sie die NAS-Daten-LIFs von node2 auf node3

Nachdem Sie die Aggregate von node2 auf node3 verschoben haben, müssen Sie die NAS-Daten-LIFs von node2 auf node3 verschieben.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie müssen überprüfen, ob die LIFs sich in den entsprechenden Ports befinden, nachdem Sie die LIFs von node3 nach node4 verschoben und node4 in den Online-Modus versetzt haben.

Schritte

1. Listen Sie alle NAS-Daten-LIFs auf, die sich im Besitz von node2 befinden, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe erfassen:

   `network interface show -data-protocol nfs|cifs -home-node node2`

   Im folgenden Beispiel wird die Befehlsausgabe für „node2“ gezeigt:

```
cluster::> network interface show -data-protocol nfs|cifs -home-node
node2
              Logical     Status      Network             Current
Current  Is
 Vserver      Interface   Admin/Oper  Address/Mask        Node     Port
Home
 -----------  ----------  ----------  ------------------  -------
-------  ----
 vs0
              a0a         up/down     10.63.0.53/24       node2    a0a
true
              data1       up/up       10.63.0.50/18       node2    e0c
true
              rads1       up/up       10.63.0.51/18       node2    e1a
true
              rads2       up/down     10.63.0.52/24       node2    e1b
true
 vs1
              lif1        up/up       172.17.176.120/24   node2    e0c
true
              lif2        up/up       172.17.176.121/24   node2    e1a
true
```

2. Nehmen Sie eine der folgenden Aktionen:

Falls Knoten 2…	Dann…
Schnittstellengruppen oder VLANs sind konfiguriert	Gehen Sie zu Schritt 3.
Schnittstellengruppen oder VLANs sind nicht konfiguriert	Überspringen Sie Schritt 3, und fahren Sie mit fort Schritt 4.

3. Nehmen Sie die folgenden Schritte durch, um die auf Schnittstellengruppen und VLANs auf node2 gehosteten NAS-Daten-LIFs zu migrieren:

   a. Migrieren Sie alle Daten-LIFs, die auf einer Schnittstellengruppe auf node2 gehostet werden, zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

      `network interface migrate -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-destination -node` *`node3`* `-destination-port` *`netport|ifgrp`*

   b. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt A Um den Port und Node, der derzeit die LIFs hostet, geben Sie einmal für jeden Node den folgenden Befehl ein:

      `network interface modify -vserver` *`Vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node3`* `-homeport` *`netport|ifgrp`*

c. Migrieren Sie alle auf VLANs gehosteten LIFs auf node2 zu einem Port auf node3, der in der Lage ist, LIFs auf demselben Netzwerk wie die des VLANs zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -home-node
node3 -homeport netport|ifgrp
```

4. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 5 Bis Schritt 8.
San	Überspringen Sie Schritt 5 bis Schritt 8 und schließen Sie dann ab Schritt 9.
Sowohl NAS als auch SAN	Vollständig Schritt 5 Bis Schritt 9.

5. Wenn auf Ihren Plattformen nicht dieselben Daten-Ports vorhanden sind, fügen Sie die Ports der Broadcast-Domäne hinzu:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt -ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „6280-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain „Management“ im IPspace „Standard“ hinzu:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
           -broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

6. Migrieren Sie jede NAS-Daten-LIF auf node3 durch Eingabe des folgenden Befehls, einmal für jede LIF:

```
network interface migrate -vserver Vserver_name -lif LIF_name -destination
-node node3 -destination-port netport|ifgrp
```

7. Überprüfen Sie, ob NAS-LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von „up“ haben, indem Sie auf einem der beiden Knoten den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network interface show -curr-node node3 -data-protocol cifs|nfs
```

8. Wenn eine der LIFs nicht verfügbar ist, setzen Sie den administrativen Status der LIFs auf „up“, indem Sie den folgenden Befehl eingeben, einmal für jede LIF:

```
network interface modify -vserver Vserver_name -lif LIF_name -status-admin up
```

9. Wenn Schnittstellengruppen oder VLANs konfiguriert sind, führen Sie die folgenden Teilschritte aus:

   a. Entfernen Sie die VLANs aus den Schnittstellengruppen:

      `network port vlan delete -node node_name -port ifgrp -vlan-id VLAN_ID`

   b. Geben Sie den folgenden Befehl ein und überprüfen Sie seine Ausgabe, um zu ermitteln, ob Schnittstellengruppen auf dem Node konfiguriert sind:

      `network port ifgrp show -node node_name -ifgrp ifgrp_name -instance`

      Das System zeigt Schnittstellengruppeninformationen für den Node an, wie im folgenden Beispiel gezeigt:

```
cluster::> network port ifgrp show -node node2 -ifgrp a0a -instance
                  Node: node2
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode_lacp
          MAC Address: MAC_address
    ort Participation: partial
        Network Ports: e2c, e2d
             Up Ports: e2c
           Down Ports: e2d
```

   a. Wenn auf dem Node Schnittstellengruppen konfiguriert sind, notieren Sie die Namen der Interface Groups und der ihnen zugewiesenen Ports. Löschen Sie dann die Ports, indem Sie den folgenden Befehl eingeben, jeweils ein für jeden Port:

      `network port ifgrp remove-port -node node_name -ifgrp ifgrp_name -port port_name`

Phase 4: Notieren Sie Informationen und entfernen Sie node2

Phase-4-Übersicht

Während der Phase 4 notieren Sie node2 Informationen, die später im Verfahren verwendet werden sollen, und setzen dann node2 aus.

Schritte

1. "Node2-Informationen aufzeichnen"
2. "Node2 ausmustern"

Node2-Informationen aufzeichnen

Bevor Sie node2 herunterfahren und außer Betrieb nehmen können, müssen Sie Informationen über das Cluster-Netzwerk, die Management- und FC-Ports sowie seine NVRAM-System-ID aufzeichnen. Sie benötigen diese Informationen später im Verfahren,

wenn Sie node2 node4 zuordnen und Festplatten neu zuweisen.

Schritte

1. Ermitteln Sie die Cluster-Netzwerk-, Node-Management-, Cluster- und Cluster-Management-Ports auf node2:

   `network interface show -curr-node node_name -role cluster,intercluster,nodemgmt,cluster-mgmt`

   Das System zeigt die LIFs für diesen Node und andere Nodes im Cluster an, wie im folgenden Beispiel dargestellt:

```
cluster::> network interface show -curr-node node2 -role
cluster,intercluster,node-mgmt,cluster-mgmt
         Logical     Status     Network            Current     Current
Is
Vserver  Interface   Admin/Oper Address/Mask       Node        Port
Home
-------- ----------  ---------- ------------------ ----------  -------
----
node2
         intercluster up/up     192.168.1.202/24   node2       e0e
true
         clus1        up/up     169.254.xx.xx/24   node2       e0a
true
         clus2        up/up     169.254.xx.xx/24   node2       e0b
true
         mgmt1        up/up     192.168.0.xxx/24   node2       e0c
true
4 entries were displayed.
```

   > Das System verfügt möglicherweise über keine Intercluster-LIFs. Sie erhalten eine Cluster-Management-LIF nur auf einem Node eines Node-Paars. Eine LIF zum Cluster-Management wird in der Beispielausgabe von angezeigt "Schritt 1" In *Port-Informationen für Node1 aufzeichnen*.

2. Erfassen Sie die Informationen in der Ausgabe, die im Abschnitt verwendet werden sollen "Weisen Sie Ports von node2 nach node4 zu".

   Die Ausgabeinformationen sind erforderlich, um die neuen Controller-Ports den alten Controller-Ports zuzuordnen.

3. Physische Ports auf node2 bestimmen:

   `network port show -node node_name -type physical +`

   node_name Ist der Node, der migriert wird.

   Das System zeigt die physischen Ports auf node2 an, wie im folgenden Beispiel dargestellt:

```
cluster::> network port show -node node2 -type physical

                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node2
       e0M       Default      IP_address       up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

4. Notieren Sie die Ports und ihre Broadcast-Domänen.

   Die Broadcast-Domänen müssen später im Verfahren den Ports auf dem neuen Controller zugeordnet werden.

5. Bestimmen Sie die FC-Ports auf node2:

   `network fcp adapter show`

   Das System zeigt die FC-Ports auf dem node2 an, wie im folgenden Beispiel dargestellt:

```
cluster::> network fcp adapter show -node node2
                     Connection  Host
Node         Adapter Established Port Address
------------ ------- ----------- ------------
node2
             0a      ptp         11400
node2
             0c      ptp         11700
node2
             6a      loop        0
node2
             6b      loop        0
4 entries were displayed.
```

6. Notieren Sie die Ports.

   Die Ausgabeinformationen sind erforderlich, um die neuen FC-Ports auf dem neuen Controller später im Verfahren zuzuordnen.

7. Falls Sie dies zuvor noch nicht getan haben, überprüfen Sie, ob auf node2 Schnittstellengruppen oder VLANs konfiguriert sind:

```
ifgrp show

vlan show
```

Sie verwenden die Informationen im Abschnitt "Weisen Sie Ports von node2 nach node4 zu".

8. Führen Sie eine der folgenden Aktionen durch:

Sie suchen…	Dann…
Die NVRAM-System-ID-Nummer in wurde aufgezeichnet "Bereiten Sie die Knoten für ein Upgrade vor"	Gehen Sie zu "Node2 ausmustern".
Die NVRAM-System-ID-Nummer in wurde nicht aufgezeichnet "Bereiten Sie die Knoten für ein Upgrade vor"	Vollständig Schritt 9 Und Schritt 10 Und fahren Sie dann mit dem nächsten Abschnitt fort, "Node2 ausmustern".

9. die Attribute von node2 anzeigen:

```
system node show -instance -node node2
```

```
cluster::> system node show -instance -node node2
                                ...
                    NVRAM System ID: system_ID
                                ...
```

10. notieren Sie die im Abschnitt zu verwendende NVRAM-System-ID "installieren und booten sie node4".

Node2 ausmustern

Um node2 auszumustern, müssen Sie node2 richtig abschalten und aus dem Rack oder Gehäuse entfernen. Wenn sich das Cluster in einer SAN-Umgebung befindet, müssen Sie auch die SAN-LIFs löschen.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Falls das Cluster…	Dann…
Eines Clusters mit zwei Nodes	Gehen Sie zu Schritt 2.
Ein Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 9.

2. Zugriff auf die erweiterte Berechtigungsebene durch Eingabe des folgenden Befehls auf einem der beiden Knoten:

```
set -privilege advanced
```

3. Überprüfen Sie, ob die Cluster-HA deaktiviert wurde, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

`cluster ha show`

Vom System wird die folgende Meldung angezeigt:

```
High Availability Configured: false
```

4. Überprüfen Sie, ob node2 aktuell epsilon hält, indem Sie den folgenden Befehl eingeben und die Ausgabe prüfen:

   `cluster show`

   Das folgende Beispiel zeigt, dass auf node2 Epsilon steht:

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

Warning: Cluster HA has not been configured. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

2 entries were displayed.
```

> Wenn Sie ein HA-Paar in einem Cluster mit mehreren HA-Paaren aktualisieren, müssen Sie Epsilon auf den Node eines HA-Paars verschieben, ohne ein Controller-Upgrade durchführen zu müssen. Wenn Sie beispielsweise nodeA/nodeB in einem Cluster mit der HA-Paar-Konfiguration nodeA/nodeB und nodeC/nodded aktualisieren, müssen Sie Epsilon auf nodeC oder nodded verschieben.

5. Wenn das Epsilon auf node2 hält, markieren Sie Epsilon als `false` Auf dem Node, sodass er auf node3 übertragen werden kann:

   `cluster modify -node *node2* -epsilon false`

6. Übertragen Sie das Epsilon auf node3, indem Sie epsilon markieren `true` Auf Knoten 3:

   `cluster modify -node *node3* -epsilon true`

7. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

   `network options switchless-cluster show`

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

8. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

   `network options switchless-cluster show`

   ```
   cluster::*> network options switchless-cluster show
   Enable Switchless Cluster: false/true
   ```

   Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

9. Zurück zur Administratorebene:

   `set -privilege admin`

10. Stoppen Sie node2, indem Sie auf beiden Controllern den folgenden Befehl eingeben:
    `system node halt -node node2`
11. Nachdem der Knoten 2 vollständig heruntergefahren wurde, entfernen Sie ihn aus dem Gehäuse oder Rack. Sie können nach Abschluss des Upgrades die Decommission node2 deaktivieren. Siehe "Ausmustern des alten Systems".

Phase 5: installieren und booten sie node4

Phase-5-Übersicht

In Phase 5 installieren und booten Sie node4, ordnen das Cluster und die Node-Management-Ports von node2 nach node4 zu, überprüfen die installation von node4 und verschieben Daten-LIFs und SAN-LIFs, die zu node2 gehören, von node3 auf node4. Außerdem werden node2-Aggregate von Node3 nach node4 verschoben.

Schritte

1. "installieren und booten sie node4"
2. "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest"
3. "Weisen Sie Ports von node2 nach node4 zu"
4. "Überprüfen Sie die installation von node4"
5. "Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4"
6. "Verschiebung von nicht-Root-Aggregaten node2 von Node3 in node4"

installieren und booten sie node4

sie müssen node4 im Rack installieren, Node2-Verbindungen zu node4 übertragen und

node4 booten. Sie müssen auch node2-Spares, alle Festplatten der Root-Partition und alle nicht-Root-Aggregate neu zuweisen, die nicht zu node3 früher verschoben wurden.

Über diese Aufgabe

Sie müssen node4 als Netzboot fahren, wenn nicht die gleiche Version von ONTAP 9 auf node2 installiert ist. Nachdem sie node4 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für den späteren Systemstart herunterladen, indem Sie den Anweisungen unter folgen "Vorbereitungen für den Netzboot"

Sie sind jedoch nicht verpflichtet, Netboot node4 zu starten, wenn es die gleiche oder eine höhere Version von ONTAP 9 hat, die auf node2 installiert ist.

- Wichtige Informationen:*
- Wenn Sie ein V-Series System oder ein System mit mit mit FlexArray Virtualisierungssoftware aktualisieren, die mit Storage-Arrays verbunden ist, müssen Sie diese vollständig ausführen Schritt 1 Bis Schritt 7, Lassen Sie diesen Abschnitt bei Schritt 8 Und befolgen Sie die Anweisungen unter "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Geben Sie bei Bedarf die Befehle im Wartungsmodus ein. Sie müssen dann zu diesem Abschnitt zurückkehren und den Vorgang unter fortsetzen Schritt 9.
- Wenn Sie jedoch ein System mit Speicherfestplatten aktualisieren, müssen Sie diesen gesamten Abschnitt abschließen und dann mit dem Abschnitt fortfahren "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest", Eingabe von Befehlen an der Cluster-Eingabeaufforderung.

Schritte

1. Nehmen Sie eine der folgenden Aktionen:

Wenn node4 wird in …	Dann…
Ein von Knoten 3 getrenntes Chassis	Gehen Sie zu Schritt 2.
Im gleichen Chassis mit Knoten3	Überspringen Sie die Schritte 2 und 3 und gehen Sie zu Schritt 4.

2. stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt.

   Wenn node4 sich in einem separaten Chassis von node3 befindet, können sie node4 an der gleichen Stelle wie node2 platzieren. Wenn sich Node3 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

3. installieren sie node4 im Rack gemäß den Anweisungen in der Anleitung *Installation and Setup Instructions* für das Node-Modell.
4. kabelnode4, die Verbindungen von node2 nach node4 verschieben.

   Die folgenden Referenzen helfen Ihnen dabei, geeignete Kabelverbindungen zu machen. Gehen Sie zu "Quellen" Um eine Verbindung zu ihnen zu machen.

   - *Installations- und Setup-Anleitung* oder *Installationsanforderungen für die FlexArray-Virtualisierung und Referenz* für die node4-Plattform
   - Das entsprechende Verfahren für das Festplatten-Shelf
   - Die Dokumentation *High Availability Management*

     Folgende Anschlüsse verkabeln:

- Konsole (Remote-Management-Port)
- Cluster-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Storage
- SAN-Konfigurationen: ISCSI Ethernet und FC Switch Ports

> Sie müssen die Interconnect-Karte/FC_VI-Karte oder den Interconnect/FC_VI-Kabelanschluss von node2 auf node4 nicht verschieben, da die meisten Plattformmodelle über einzigartige Interconnect-Kartenmodelle verfügen.

5. Führen Sie eine der folgenden Aktionen durch:

Wenn node4 in…	Dann…
Im gleichen Chassis wie bei Node3	Gehen Sie zu Schritt 8.
Ein von Knoten 3 getrenntes Chassis	Gehen Sie zu Schritt 6.

6. Schalten Sie die Stromversorgung zu node4 ein, und unterbrechen Sie dann den Start, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Startumgebung zuzugreifen.

> Wenn Sie node4 booten, wird möglicherweise die folgende Meldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power
         outage. This is likely because the battery is
         discharged but could be due to other temporary
         conditions.
         When the battery is ready, the boot process will
         complete and services will be engaged.
         To override this delay, press 'c' followed by 'Enter'
```

7. Wenn die Warnmeldung in Schritt 6 angezeigt wird, führen Sie die folgenden Schritte aus:
   a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.
   b. Lassen Sie den Akku laden und den Bootvorgang beenden.

> **Warnung: Die Verzögerung nicht außer Kraft setzen. Wenn der Akku nicht geladen werden kann, kann dies zu einem Datenverlust führen.**

8. Nehmen Sie eine der folgenden Aktionen:

Wenn Ihr System…	Dann…
Verfügt über Festplatten und keinen Back-End-Speicher	Überspringen Sie Schritt 9 bis Schritt 14, und fahren Sie mit fort Schritt 15.

Wenn Ihr System…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	a. Gehen Sie zum Abschnitt „ FC- oder UTA/UTA2-Konfiguration auf node4_“ und füllen Sie die Abschnitte aus "Konfigurieren Sie FC-Ports auf node4" Und "UTA/UTA2-Ports auf node4 prüfen und konfigurieren", Je nach Ihrem System. b. Kehren Sie zu diesem Abschnitt zurück, und führen Sie die verbleibenden Schritte aus. Beginnen Sie mit Schritt 9. Vor dem Booten von ONTAP auf dem V-Series System müssen Sie die integrierten FC-Ports, UTA/UTA2-Ports und UTA/UTA2-Karten neu konfigurieren.

9. Fügen Sie die FC-Initiator-Ports des neuen Node zu den Switch-Zonen hinzu.

   Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

10. Fügen Sie die FC-Initiator-Ports dem Speicher-Array als neue Hosts hinzu, und ordnen Sie die Array-LUNs den neuen Hosts zu.

    Anweisungen finden Sie in der Dokumentation für das Storage-Array und Zoning.

11. Ändern Sie die WWPN-Werte (World Wide Port Name) in den Host- oder Volume-Gruppen, die Array-LUNs auf dem Speicher-Array zugeordnet sind.

    Durch die Installation eines neuen Controller-Moduls werden die WWPN-Werte geändert, die den einzelnen integrierten FC-Ports zugeordnet sind.

12. Wenn die Konfiguration das Switch-basierte Zoning verwendet, passen Sie das Zoning an die neuen WWPN-Werte an.
13. Überprüfen Sie, ob die Array-LUNs nun für node4 sichtbar sind, indem Sie den folgenden Befehl eingeben und seine Ausgabe prüfen:

    ```
    sysconfig -v
    ```

    Das System zeigt alle Array-LUNs an, die für jeden FC-Initiator-Port sichtbar sind. Wenn die Array-LUNs nicht sichtbar sind, können Sie Festplatten von node2 nicht später in diesem Abschnitt neu zuweisen.

14. Drücken Sie Strg-C, um das Startmenü anzuzeigen, und wählen Sie Wartungsmodus aus.
15. Geben Sie in der Eingabeaufforderung für den Wartungsmodus den folgenden Befehl ein:

    ```
    halt
    ```

    Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

16. node4 für ONTAP konfigurieren:

    ```
    set-defaults
    ```

17. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.

Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base "Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist" Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden…	Dann…
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	`setenv bootarg.storageencryption.support` **`true`**
NetApp ohne FIPS SEDs	`setenv bootarg.storageencryption.support` **`false`**

FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.

SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

b. Wenden Sie sich an den NetApp Support, um Hilfe beim Wiederherstellen der integrierten Schlüsselmanagementinformationen zu erhalten.

18. Wenn die auf node4 installierte ONTAP-Version gleich oder höher als die auf node2 installierte Version von ONTAP 9 ist, geben Sie den folgenden Befehl ein:

```
boot_ontap menu
```

19. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Verfügt nicht über die richtige oder aktuelle ONTAP-Version unter node4	Gehen Sie zu Schritt 20.
Hat die richtige oder aktuelle Version von ONTAP auf node4	Gehen Sie zu Schritt 25.

20. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

Sie müssen den Management-Port und die IP-Adresse als Netzboot-Verbindung verwenden. Verwenden Sie keine LIF-IP-Adresse von Daten, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -auto`
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `ifconfig e0M -addr=filer_addr mask=netmask -gw=gateway dns=dns_addr domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Speichersystems (obligatorisch). *`netmask`* Ist die Netzwerkmaske des Storage-Systems (erforderlich). *`gateway`* Ist das Gateway für das Speichersystem (erforderlich). *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

21. Ausführen eines Netzboots auf node4:

Für…	Dann…
Systeme der FAS/AFF8000 Serie	`netboot http://<web_server_ip/path_to_webaccessible_directory>/netboot/kernel`
Alle anderen Systeme	`netboot http://<web_server_ip/path_to_webaccessible_directory/ontap_version>_image.tgz`

Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In "Schritt 1" Im Abschnitt *Vorbereiten für Netzboot*.

Unterbrechen Sie den Startvorgang nicht.

22. Wählen Sie im Startmenü die Option `option (7) Install new software first`.

Mit dieser Menüoption wird das neue Data 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
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der Data ONTAP und keine Upgrades von Controllern.

> 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 Versionen von ONTAP. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

23. [[man_install4_steep23] Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie y ein. Geben Sie dann die URL ein, wenn Sie nach dem Paket gefragt werden:

    ```
    http://<web_server_ip/path_to_web-
    accessible_directory/ontap_version>_image.tgz
    ```

24. Führen Sie die folgenden Teilschritte durch:

    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

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

    b. Starten Sie den Neustart durch Eingabe `y` Wenn die folgende Eingabeaufforderung angezeigt wird:

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

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

25. Wählen Sie den Wartungsmodus `5` Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
26. bevor Sie fortfahren, fahren Sie mit fort "Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest" Um alle erforderlichen Änderungen an den FC- oder UTA/UTA2-Ports auf dem Node vorzunehmen. Nehmen Sie die in diesen Abschnitten empfohlenen Änderungen vor, starten Sie den Node neu, und wechseln Sie in den Wartungsmodus.
27. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe, um die System-ID von node4 zu finden:

    ```
    disk show -a
    ```

    Das System zeigt die System-ID des Node sowie Informationen über seine Festplatten an, wie im folgenden Beispiel dargestellt:

```
*> disk show -a
Local System ID: 536881109
DISK         OWNER                      POOL   SERIAL NUMBER   HOME
------------ -------------              -----  -------------
-------------
0b.02.23     nst-fas2520-2(536880939)   Pool0  KPG2RK6F        nst-
fas2520-2(536880939)
0b.02.13     nst-fas2520-2(536880939)   Pool0  KPG3DE4F        nst-
fas2520-2(536880939)
0b.01.13     nst-fas2520-2(536880939)   Pool0  PPG4KLAA        nst-
fas2520-2(536880939)
......
0a.00.0                   (536881109)   Pool0  YFKSX6JG
(536881109)
......
```

28. Weisen Sie node2 Ersatzteile, Festplatten, die zur Root gehören, und alle nicht-Root-Aggregate erneut zu, die im Abschnitt früher nicht in node3 verschoben wurden "Verschieben Sie Aggregate ohne Root-Root-Fehler von node2 auf node3":

> Wenn Sie auf Ihrem System freigegebene Festplatten, Hybrid-Aggregate oder beides haben, müssen Sie die korrekte verwenden `disk reassign` Befehl aus der folgenden Tabelle.

Festplattentyp…	Führen Sie den Befehl aus…
Mit gemeinsamen Festplatten	`disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`* `-p` *`node3_sysid`*
Ohne Shared-Ressourcen	`disks disk reassign -s` *`node2_sysid`* `-d` *`node4_sysid`*

Für das `<node2_sysid>` Wert: Verwenden Sie die in erfassten Informationen "Schritt 10" Des Abschnitts *Record node2 information*. Für `*node4_sysid*`Verwenden Sie die Informationen, die in erfasst werden Schritt 23.

> Der `-p` Die Option ist nur im Wartungsmodus erforderlich, wenn freigegebene Festplatten vorhanden sind.

Der `disk reassign` Befehl weist nur die Festplatten zu, für die es erforderlich ist *`node2_sysid`* Ist der aktuelle Eigentümer.

Vom System wird die folgende Meldung angezeigt:

```
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
```

Eingabe `n` Wenn Sie aufgefordert werden, die Neuzuweisung der Festplatte abzubrechen.

Wenn Sie aufgefordert werden, die Neuzuweisung der Festplatte abzubrechen, müssen Sie eine Reihe von Eingabeaufforderungen beantworten, wie in den folgenden Schritten dargestellt:

a. Vom System wird die folgende Meldung angezeigt:

```
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
```

b. Eingabe `y` Um fortzufahren.

Vom System wird die folgende Meldung angezeigt:

```
Disk ownership will be updated on all disks previously belonging to
Filer with sysid <sysid>.
Do you want to continue (y/n)? y
```

a. Eingabe `y` Um die Aktualisierung der Festplatteneigentümer zu ermöglichen.

29. Wenn Sie ein Upgrade von einem System mit externen Festplatten auf ein System durchführen, das interne und externe Festplatten unterstützt (z. B. A800-Systeme), setzen sie node4 als root, um zu bestätigen, dass es aus dem Root-Aggregat von node2 startet.

> **Warnung: Sie müssen die folgenden Teilschritte in der angegebenen Reihenfolge durchführen; andernfalls kann es zu einem Ausfall oder sogar zu Datenverlust kommen.**

Mit dem folgenden Verfahren wird node4 vom Root-Aggregat von node2 gestartet:

a. Überprüfen Sie die RAID-, Plex- und Prüfsummeninformationen für das node2 Aggregat:

```
aggr status -r
```

b. Prüfen Sie den Gesamtstatus des node2-Aggregats:

```
aggr status
```

c. Bei Bedarf das node2 Aggregat online bringen:

```
aggr_online root_aggr_from_node2
```

d. Verhindern Sie, dass das node4 aus dem ursprünglichen Root-Aggregat gebootet wird:

```
aggr offline root_aggr_on_node4
```

e. Legen Sie das node2-Root-Aggregat als das neue Root-Aggregat für node4 fest:

```
aggr options aggr_from_node2 root
```

30. Vergewissern Sie sich, dass Controller und Chassis als konfiguriert sind `ha` Indem Sie den folgenden Befehl eingeben und die Ausgabe beobachten:

```
ha-config show
```

Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

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

Systeme zeichnen in EINEM PROM auf, ob sie in einem HA-Paar oder einer Standalone-Konfiguration sind. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

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

```
ha-config modify chassis ha.
```

Wenn Sie eine MetroCluster-Konfiguration haben, verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

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

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

31. Löschen Sie die Mailboxen auf node4:

```
mailbox destroy local
```

32. Beenden des Wartungsmodus:

```
halt
```

Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.

33. Überprüfen Sie in Knoten 3 das Systemdatum, die Uhrzeit und die Zeitzone:

```
date
```

34. Prüfen Sie am node4 das Datum an der Eingabeaufforderung für die Boot-Umgebung:

    `show date`

35. Legen Sie bei Bedarf das Datum auf node4 fest:

    `set date mm/dd/yyyy`

36. Prüfen Sie auf node4 die Zeit an der Eingabeaufforderung der Boot-Umgebung:

    `show time`

37. Stellen Sie bei Bedarf die Uhrzeit auf node4 ein:

    `set time hh:mm:ss`

38. Überprüfen Sie, ob die Partner-System-ID korrekt festgelegt ist, wie in beschrieben Schritt 26 Unter Option.

    `printenv partner-sysid`

39. Legen Sie bei Bedarf die Partner System-ID auf node4 fest:

    `setenv partner-sysid node3_sysid`

    a. Einstellungen speichern:

       `saveenv`

40. Rufen Sie das Boot-Menü an der Eingabeaufforderung der Boot-Umgebung auf:

    `boot_ontap menu`

41. Wählen Sie im Startmenü die Option **(6) Flash von Backup config** aktualisieren, indem Sie eingeben `6` An der Eingabeaufforderung.

    Vom System wird die folgende Meldung angezeigt:

    ```
    This will replace all flash-based configuration with the last backup to
    disks. Are you sure you want to continue?:
    ```

42. Eingabe `y` An der Eingabeaufforderung.

    Der Startvorgang läuft normal weiter, und das System fordert Sie auf, die Unstimmigkeit der System-ID zu bestätigen.

    > Das System wird möglicherweise zweimal neu gestartet, bevor die Warnmeldung zur Nichtübereinstimmung angezeigt wird.

43. Bestätigen Sie die Diskrepanz. Der Node kann vor dem normalen Booten eine Runde des Neubootens abschließen.
44. Melden Sie sich bei node4 an.

Legen Sie die FC- oder UTA/UTA2-Konfiguration auf node4 fest

Wenn node4 über integrierte FC-Ports, integrierte Unified Target Adapter (UTA/UTA2)-Ports oder eine UTA/UTA2-Karte verfügt, müssen Sie die Einstellungen konfigurieren, bevor Sie den Rest des Verfahrens abschließen.

Über diese Aufgabe

Möglicherweise müssen Sie den Abschluss abschließen Konfigurieren Sie FC-Ports auf node4, Das UTA/UTA2-Ports auf node4 prüfen und konfigurieren, Oder beide Abschnitte.

Wenn node4 keine integrierten FC-Ports, Onboard-UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat und Sie ein System mit Storage-Festplatten aktualisieren, können Sie weiter gehen "Weisen Sie Ports von node2 nach node4 zu".

Wenn Sie jedoch ein V-Series System oder FlexArray-Virtualisierungssoftware haben und mit Storage-Arrays verbunden sind und node4 keine integrierten FC-Ports, Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie zum Abschnitt *Installation and Boot node4* zurückkehren und wieder aufnehmen "Schritt 9". stellen Sie sicher, dass node4 über ausreichend Rack-Platz verfügt. Wenn node4 sich in einem separaten Chassis von node2 befindet, können sie node4 an der gleichen Stelle wie node3 platzieren. Wenn sich Node2 und node4 im selben Chassis befinden, befindet sich node4 bereits in der entsprechenden Rack-Position.

Wahlmöglichkeiten

- Konfigurieren Sie FC-Ports auf node4
- UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Konfigurieren Sie FC-Ports auf node4

Wenn node4 FC-Ports hat, entweder Onboard oder auf einem FC-Adapter, müssen Sie Port-Konfigurationen auf dem Node festlegen, bevor Sie ihn in den Dienst stellen, da die Ports nicht vorkonfiguriert sind. Wenn die Ports nicht konfiguriert sind, kann es zu einer Serviceunterbrechung kommen.

Bevor Sie beginnen

Sie müssen die Werte der FC-Port-Einstellungen von node2 haben, die Sie im Abschnitt gespeichert haben "Bereiten Sie die Knoten für ein Upgrade vor".

Über diese Aufgabe

Sie können diesen Abschnitt überspringen, wenn Ihr System über keine FC-Konfigurationen verfügt. Wenn Ihr System über integrierte UTA/UTA2-Ports oder einen UTA/UTA2-Adapter verfügt, konfigurieren Sie sie in UTA/UTA2-Ports auf node4 prüfen und konfigurieren.

> Wenn im System Storage-Festplatten vorhanden sind, müssen Sie an der Cluster-Eingabeaufforderung in diesem Abschnitt die Befehle eingeben. Wenn Sie ein V-Series System oder ein System mit FlexArray Virtualisierungssoftware haben, die mit Storage-Arrays verbunden sind, geben Sie in diesem Abschnitt im Wartungsmodus Befehle ein.

Schritte

1. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Gehen Sie zu Schritt 5.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 2.

2. Zugriff auf den Wartungsmodus:

```
boot_ontap maint
```

3. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

Das System zeigt Informationen zu allen FC- und konvergenten Netzwerkadaptern im System an.

4. Vergleichen Sie die FC-Einstellungen auf den neuen Nodes mit den Einstellungen, die Sie zuvor vom ursprünglichen Node erfasst haben.
5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Ändern Sie die FC-Ports auf node4 nach Bedarf: • So programmieren Sie Zielanschlüsse: `system node hardware unified-connect modify -type
-t target -adapter *port_name*` ** So programmieren Sie Initiator-Ports: `system node unified-connect modify type	-t initiator -adapter *port_name*` `-type` Ist der FC4-Typ, das Ziel oder der Initiator.

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Ändern Sie die FC-Ports auf node4 nach Bedarf: `ucadmin modify -m fc -t initiator -f adapter_port_name` `-t` Ist der FC4-Typ, das Ziel oder der Initiator. Die FC-Ports müssen als Initiatoren programmiert werden.

6. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `system node unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Überprüfen Sie die neuen Einstellungen, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen: `ucadmin show`

7. Führen Sie eine der folgenden Aktionen durch:

Wenn die FC-Standardeinstellungen auf den neuen Nodes sind…	Dann…
Das gleiche wie diejenigen, die Sie auf den ursprünglichen Knoten erfasst	Gehen Sie zu Schritt 11.
Anders als jene, die Sie auf den ursprünglichen Knoten erfasst haben	Gehen Sie zu Schritt 8.

8. Wartungsmodus beenden:

```
halt
```

9. Nachdem Sie den Befehl eingegeben haben, warten Sie, bis das System an der Eingabeaufforderung der Boot-Umgebung angehalten wird.
10. Führen Sie eine der folgenden Aktionen durch:

Wenn das System, das Sie aktualisieren…	Dann…
Ist ein V-Series System oder verfügt über FlexArray Virtualisierungssoftware mit Data ONTAP 8.3.0 oder höher	Greifen Sie auf den Wartungsmodus zu, indem Sie an der Eingabeaufforderung der Boot-Umgebung den folgenden Befehl eingeben: `boot_ontap maint`
Ist kein V-Series System und verfügt nicht über FlexArray Virtualisierungssoftware	Boot node4 durch Eingabe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung: `boot_ontap`

11. Nehmen Sie eine der folgenden Aktionen:

Wenn das System, das Sie aktualisieren…	Dann…
Festplatten sind vorhanden	• Gehen Sie zu UTA/UTA2-Ports auf node4 prüfen und konfigurieren Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt und gehen Sie zu "Weisen Sie Ports von node2 nach node4 zu" Wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat.
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	• Gehen Sie zu UTA/UTA2-Ports auf node4 prüfen und konfigurieren Bei node4 mit einer UTA/UTA2-Karte oder Onboard-Ports UTA/UTA2: • Überspringen Sie den Abschnitt *UTA/UTA2-Ports auf node4* überprüfen und konfigurieren, wenn node4 keine UTA/UTA2-Karte oder UTA/UTA2 Onboard-Ports hat, kehren Sie zum Abschnitt *Installieren und Booten von node4* zurück, und setzen Sie den Abschnitt unter fort "Schritt 9".

UTA/UTA2-Ports auf node4 prüfen und konfigurieren

Wenn node4 Onboard UTA/UTA2-Ports oder eine UTA/UTA2-Karte hat, müssen Sie die Konfiguration der Ports überprüfen und sie je nach Nutzung des aktualisierten Systems konfigurieren.

Bevor Sie beginnen

Sie müssen die richtigen SFP+ Module für die UTA/UTA2-Ports besitzen.

Über diese Aufgabe

DIE UTA2-Ports können im nativen FC-Modus oder im UTA/UTA2-Modus konfiguriert werden. Der FC-Modus unterstützt FC Initiator und FC Target. Der UTA-/UTA2-Modus ermöglicht es, gleichzeitig NIC- und FCoE-Datenverkehr auf die gleiche 10-GbE-SFP+-Schnittstelle zu übertragen und das FC-Ziel zu unterstützen.

Bei NetApp Marketingmaterialien wird möglicherweise der Begriff UTA2 verwendet, um sich auf CNA-Adapter und Ports zu beziehen. Allerdings verwendet die CLI den Begriff CNA.

UTA2-Ports können an einem Adapter oder auf dem Controller mit den folgenden Konfigurationen verwendet werden:

- UTA-/UTA2-Karten, die gleichzeitig mit dem Controller bestellt wurden, werden vor dem Versand konfiguriert, um die von Ihnen angeforderte Persönlichkeit zu erhalten.
- DIE UTA2-Karten, die separat vom Controller bestellt werden, werden mit der standardmäßigen FC-Zielgruppe ausgeliefert.
- Onboard UTA/UTA2-Ports auf neuen Controllern werden konfiguriert (vor dem Versand), um die von Ihnen angeforderte Persönlichkeit zu besitzen.

Sie können jedoch die Konfiguration der UTA/UTA2-Ports auf node4 überprüfen und sie gegebenenfalls ändern.

Achtung: Wenn Ihr System über Speicherfestplatten verfügt, geben Sie die Befehle in diesem Abschnitt an der Cluster-Eingabeaufforderung ein, sofern nicht dazu aufgefordert wird, in den Wartungsmodus zu wechseln. Wenn Sie über ein MetroCluster FC-System, ein V-Series System oder ein System mit FlexArray-Virtualisierungssoftware verfügen, die mit Storage-Arrays verbunden ist, müssen Sie sich im Wartungsmodus befinden, um UTA/UTA2-Ports zu konfigurieren.

Schritte

1. Überprüfen Sie, wie die Ports derzeit mit einem der folgenden Befehle auf node4 konfiguriert werden:

Wenn das System…	Dann…
Festplatten sind vorhanden	`system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`ucadmin show`

   Das System zeigt eine Ausgabe wie im folgenden Beispiel an:

```
*> ucadmin show
                Current  Current    Pending   Pending   Admin
Node   Adapter  Mode     Type       Mode      Type      Status
----   -------  ---      ---------  -------   --------  -------
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
f-a    0e       fc       initiator  -          -        online
f-a    0f       fc       initiator  -          -        online
f-a    0g       cna      target     -          -        online
f-a    0h       cna      target     -          -        online
*>
```

2. Wenn das aktuelle SFP+-Modul nicht mit der gewünschten Verwendung übereinstimmt, ersetzen Sie es durch das richtige SFP+-Modul.

   Wenden Sie sich an Ihren NetApp Ansprechpartner, um das richtige SFP+ Modul zu erhalten.

3. Überprüfen Sie die Ausgabe des `system node hardware unified-connect show` Oder `ucadmin`

`show` Führen Sie einen Befehl aus, und bestimmen Sie, ob die UTA/UTA2-Ports die gewünschte Persönlichkeit haben.

4. Führen Sie eine der folgenden Aktionen durch:

Wenn die CNA-Ports…	Dann…
Haben Sie nicht die Persönlichkeit, die Sie wollen	Gehen Sie zu Schritt 5.
Haben Sie die Persönlichkeit, die Sie wollen	Überspringen Sie Schritt 5 bis Schritt 12, und fahren Sie mit fort Schritt 13.

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das System…	Dann…
Verfügt über Speicherfestplatten und führt Data ONTAP 8.3 aus	Boot-node4 und wechseln in den Wartungsmodus: `boot_ontap maint`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Gehen Sie zu Schritt 6. Sie sollten sich bereits im Wartungsmodus befinden.

6. Nehmen Sie eine der folgenden Aktionen:

Wenn Sie konfigurieren…	Dann…
Ports auf einer UTA/UTA2-Karte	Gehen Sie zu Schritt 7.
Onboard UTA/UTA2-Ports	Überspringen Sie Schritt 7, und fahren Sie mit fort Schritt 8.

7. Wenn sich der Adapter im Initiator-Modus befindet und der UTA/UTA2-Port online ist, versetzen Sie den UTA/UTA2-Port in den Offline-Modus:

```
storage disable adapter adapter_name
```

Adapter im Zielmodus sind im Wartungsmodus automatisch offline.

8. Wenn die aktuelle Konfiguration nicht mit der gewünschten Verwendung übereinstimmt, geben Sie den folgenden Befehl ein, um die Konfiguration nach Bedarf zu ändern:

```
ucadmin modify -m fc|cna -t initiator|target adapter_name
```

- `-m` Ist der Personality Modus: FC oder 10GbE UTA.
- `-t` Ist der FC4-Typ: Target oder Initiator.

> Sie müssen FC Initiator für Tape-Laufwerke und FlexArray-Virtualisierungssysteme verwenden. Sie müssen das FC-Ziel für SAN-Clients verwenden.

9. Überprüfen Sie die Einstellungen, indem Sie den folgenden Befehl eingeben und seine Ausgabe überprüfen:

```
ucadmin show
```

10. Führen Sie eine der folgenden Aktionen aus:

Wenn das System…	Dann…

Festplatten sind vorhanden	a. Geben Sie den folgenden Befehl ein:
	`halt`
	Das System wird an der Eingabeaufforderung für die Boot-Umgebung angehalten.
	b. Geben Sie den folgenden Befehl ein:
	`boot_ontap`

Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden und läuft Data ONTAP 8.3	Neustart in Wartungsmodus: `boot_ontap maint`

11. Überprüfen Sie die Einstellungen:

Wenn das System…	Dann…
Festplatten sind vorhanden	Geben Sie den folgenden Befehl ein: `system node hardware unified-connect show`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Geben Sie den folgenden Befehl ein: `ucadmin show`

Die Ausgabe in den folgenden Beispielen zeigt, dass sich der Adaptertyp „1b“ in ändert `initiator` Und dass sich der Modus der Adapter „2a“ und „2b“ in ändert `cna`.

```
cluster1::> system node hardware unified-connect show
                Current  Current    Pending  Pending    Admin
Node  Adapter  Mode     Type       Mode     Type       Status
----  -------  -------  ---------  -------  -------    -----
f-a    1a      fc       initiator  -        -          online
f-a    1b      fc       target     -        initiator  online
f-a    2a      fc       target     cna      -          online
f-a    2b      fc       target     cna      -          online
4 entries were displayed.
```

```
*> ucadmin show
                Current Current    Pending  Pending    Admin
Node   Adapter  Mode    Type       Mode     Type       Status
----   -------  ------- ---------  -------  -------    -----
f-a     1a      fc      initiator  -        -          online
f-a     1b      fc      target     -        initiator  online
f-a     2a      fc      target     cna      -          online
f-a     2b      fc      target     cna      -          online
4 entries were displayed.
*>
```

12. Platzieren Sie alle Ziel-Ports online, indem Sie einen der folgenden Befehle eingeben, einmal für jeden Port:

Wenn das System…	Dann…
Festplatten sind vorhanden	`network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-state up`
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	`fcp config` *`adapter_name`* `up`

13. Anschluss verkabeln.
14. Führen Sie eine der folgenden Aktionen aus:

Wenn das System…	Dann…
Festplatten sind vorhanden	Gehen Sie zu "Weisen Sie Ports von node2 nach node4 zu".
Ist ein V-Series System oder hat FlexArray-Virtualisierungssoftware und ist mit Storage-Arrays verbunden	Kehren Sie zum Abschnitt *Installieren und Starten von node4* zurück, und setzen Sie den Abschnitt unter fort "Schritt 9".

Weisen Sie Ports von node2 nach node4 zu

Sie müssen sicherstellen, dass die physischen Ports auf node2 den physischen Ports auf node4 korrekt zugeordnet werden. damit kann node4 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

Bevor Sie beginnen

Sie müssen bereits über die Ports auf den neuen Nodes verfügen, um auf diese Informationen zuzugreifen, siehe "Quellen" Zum Verknüpfen mit der *Hardware Universe*. Die Informationen werden später in diesem Abschnitt verwendet.

die Softwarekonfiguration von node4 muss mit der physischen Konnektivität von node4 übereinstimmen. Die IP-Konnektivität muss wiederhergestellt werden, bevor Sie mit dem Upgrade fortfahren.

Über diese Aufgabe

Die Port-Einstellungen können je nach Modell der Nodes variieren. Sie müssen den Port des ursprünglichen Node und die LIF-Konfiguration mit dem kompatibel machen, was Sie planen, die Konfiguration des neuen Node zu verwenden. Dies liegt daran, dass der neue Node beim Booten die gleiche Konfiguration wiedergibt. Dies bedeutet, wenn Sie node4 booten, wird Data ONTAP versuchen, LIFs auf den gleichen Ports zu hosten, die in node2 verwendet wurden.

Wenn die physischen Ports auf node2 also nicht direkt den physischen Ports auf node4 zugeordnet werden, sind daher Änderungen der Software-Konfiguration erforderlich, um nach dem Booten die Cluster-, Management- und Netzwerkkonnektivität wiederherzustellen. Wenn die Cluster-Ports auf node2 nicht direkt den Cluster-Ports auf node4 zugeordnet werden, kann node4 das Quorum auch dann nicht automatisch erneut verbinden, wenn es neu gestartet wird, bis eine Softwarekonfiguration geändert wird, um die Cluster LIFs auf den korrekten physischen Ports zu hosten.

Schritte

1. Notieren Sie alle node2-Verkabelungsinformationen für node2, die Ports, Broadcast-Domänen und IPspaces in dieser Tabelle:

LIF	Anzahl an Knoten2-Ports	Node2-IPspaces	Node2 Broadcast-Domänen	Node4-Ports	Node4 IPspaces	Node4 Broadcast-Domänen
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Cluster 5						
Cluster 6						
Node-Management						
Cluster-Management						
Daten 1						
Daten 2						
Daten 3						
Daten 4						
San						
Intercluster-Port						

   Die Schritte, um diese Informationen zu erhalten, finden Sie im Abschnitt „Node2-Informationen aufzeichnen“.

2. Notieren Sie alle Kabelinformationen für node4, die Ports, Broadcast-Domänen und IPspaces in der vorherigen Tabelle unter Verwendung der gleichen Vorgehensweise im "Node2-Informationen aufzeichnen" Abschnitt für die Schritte, um diese Informationen zu erhalten.

3. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob es sich bei dem Setup um ein 2-Node-Cluster ohne Switches handelt:
   a. Legen Sie die Berechtigungsebene auf erweitert fest:
   b. Überprüfen Sie, ob es sich um ein 2-Node-Cluster ohne Switches handelt:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: false/true
```

   Der Wert dieses Befehls muss mit dem physischen Status des Systems übereinstimmen.

   c. Zurück zur Administratorberechtigungsebene:

```
cluster::*> set -privilege admin
cluster::>
```

4. führen Sie node4 in Quorum durch, indem Sie die folgenden Schritte durchführen:
   a. Boot node4. Siehe "installieren und booten sie node4" Um den Node zu booten, wenn Sie dies noch nicht getan haben.
   b. Vergewissern Sie sich, dass sich die neuen Cluster-Ports in der Cluster Broadcast-Domäne befinden:

   `network port show -node *node* -port *port* -fields broadcast-domain`Das folgende Beispiel zeigt, dass Port „e0a“ in der Cluster-Domäne auf node4 ist:

```
cluster::> network port show -node node4 -port e0a -fields broadcast-
domain

node       port broadcast-domain
---------- ---- ----------------
node4      e1a  Cluster
```

   c. Wenn sich die Cluster-Ports nicht in der Cluster Broadcast-Domäne befinden, fügen Sie sie mit dem folgenden Befehl hinzu:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports *node:port*`

   d. Fügen Sie die korrekten Ports zur Cluster Broadcast-Domäne hinzu:

   `network port modify -node -port -ipspace Cluster -mtu 9000`

   Dieses Beispiel fügt Cluster-Port „e1b“ auf node4 hinzu:

   `network port modify -node node4 -port e1b -ipspace Cluster -mtu 9000`

Bei einer MetroCluster-Konfiguration können Sie die Broadcast-Domäne unter einem Port möglicherweise nicht ändern, da dieser mit einem Port verknüpft ist, der die LIF einer synchronen-Ziel-SVM hostet. Außerdem werden Fehler wie die folgenden angezeigt:

```
command failed: This operation is not permitted on a Vserver that is
configured as the destination of a MetroCluster Vserver relationship.
```

Geben Sie den folgenden Befehl von der entsprechenden Quell-SVM auf dem Remote-Standort ein, um die synchrone Ziel-LIF einem entsprechenden Port zuzuweisen:

```
metrocluster vserver resync -vserver vserver_name
```

e. Migrieren Sie die Cluster-LIFs zu den neuen Ports, einmal für jede LIF:

```
network interface migrate -vserver Cluster -lif lif_name -source-node node4
- destination-node node4 -destination-port port_name
```

f. Ändern Sie den Startport der Cluster-LIFs:

```
network interface modify -vserver Cluster -lif lif_name –home-port port_name
```

g. Entfernen Sie die alten Ports aus der Cluster Broadcast-Domäne:

```
network port broadcast-domain remove-ports
```

Dieser Befehl entfernt Port „e0d“ auf node4:
`network port broadcast-domain remove-ports -ipspace Cluster -broadcast-domain Cluster -ports node4:e0d`

a. Vergewissern Sie sich, dass node4 Quorum erneut verbunden hat:

```
cluster show -node node4 -fields health
```

5. passen Sie die Broadcast-Domänen an, die Ihre Cluster-LIFs hosten, und LIFs für Node-Management/Cluster-Management. Vergewissern Sie sich, dass jede Broadcast-Domäne die richtigen Ports enthält. Ein Port kann nicht zwischen Broadcast-Domänen verschoben werden, wenn er als Host oder Home für eine LIF ist, sodass Sie möglicherweise die LIFs migrieren und ändern müssen, wie in den folgenden Schritten dargestellt:

a. Zeigen Sie den Startport einer logischen Schnittstelle an:

```
network interface show -fields home-node,home-port
```

b. Zeigen Sie die Broadcast-Domäne an, die diesen Port enthält:

```
network port broadcast-domain show -ports node_name:port_name
```

c. Ports aus Broadcast-Domänen hinzufügen oder entfernen:

```
network port broadcast-domain add-ports
```

```
network port broadcast-domain remove-ports
```

a. Ändern Sie den Home-Port eines LIF:

```
network interface modify -vserver vserver_name -lif lif_name –home-port
port_name
```

6. Passen Sie die Intercluster-Broadcast-Domänen an und migrieren Sie gegebenenfalls die Intercluster LIFs mithilfe derselben Befehle, die in dargestellt sind Schritt 5.
7. Passen Sie alle anderen Broadcast-Domänen an und migrieren Sie die Daten-LIFs, falls erforderlich, mit denselben Befehlen in Schritt 5.
8. Wenn in node4 keine Ports mehr vorhanden sind, löschen Sie diese wie folgt:

a. Zugriff auf die erweiterte Berechtigungsebene auf beiden Nodes:

```
set -privilege advanced
```

b. So löschen Sie die Ports:

```
network port delete -node node_name -port port_name
```

c. Zurück zur Administratorebene:

```
set -privilege admin
```

9. Passen Sie alle LIF Failover-Gruppen an:
`network interface modify -failover-group failover_group -failover-policy failover_policy`

Mit dem folgenden Befehl wird die Failover-Richtlinie auf festgelegt `broadcast-domain-wide` Und verwendet die Ports in Failover-Gruppe `fg1` Als Failover-Ziele für LIF `data1` Ein `node4`:

```
network interface modify -vserver node4 -lif data1 failover-policy broadcast-
domain-wide -failover-group fg1
```

Weitere Informationen finden Sie unter "Quellen" Um zu *Netzwerkverwaltung* oder den Befehlen *ONTAP 9 zu verlinken: Manual Page Reference*, und gehen Sie zu *Failover-Einstellungen auf einem LIF* konfigurieren.

10. Überprüfen Sie die Änderungen auf node4:

```
network port show -node node4
```

11. Jedes Cluster-LIF muss an Port 7700 zuhören. Vergewissern Sie sich, dass die Cluster-LIFs an Port 7700 zuhören:

```
::> network connections listening show -vserver Cluster
```

Port 7700, der auf Cluster-Ports hört, ist das erwartete Ergebnis, wie im folgenden Beispiel für ein Cluster mit zwei Nodes dargestellt:

```
Cluster::> network connections listening show -vserver Cluster
Vserver Name     Interface Name:Local Port     Protocol/Service
---------------- ----------------------------  -------------------
Node: NodeA
Cluster          NodeA_clus1:7700               TCP/ctlopcp
Cluster          NodeA_clus2:7700               TCP/ctlopcp
Node: NodeB
Cluster          NodeB_clus1:7700               TCP/ctlopcp
Cluster          NodeB_clus2:7700               TCP/ctlopcp
4 entries were displayed.
```

12. Legen Sie für jede Cluster-LIF, die nicht an Port 7700 angehört, den Administrationsstatus der LIF auf fest `down` Und dann `up`:

    ```
    ::> net int modify -vserver Cluster -lif cluster-lif -status-admin down; net
    int modify -vserver Cluster -lif cluster-lif -status-admin up
    ```

    Wiederholen Sie Schritt 11, um zu überprüfen, ob die Cluster-LIF jetzt auf Port 7700 angehört.

Überprüfen Sie die installation von node4

Nach der Installation und dem Booten von node4 müssen Sie überprüfen, ob node4 korrekt installiert ist, dass er Teil des Clusters ist und mit node3 kommunizieren kann.

Schritte

1. Melden Sie sich an der Eingabeaufforderung des Systems bei node4 an.
2. Vergewissern Sie sich, dass node4 beide Teil desselben Clusters wie node3 und ordnungsgemäß ist:

   ```
   cluster show
   ```

3. Vergewissern Sie sich, dass node4 mit node3 kommunizieren kann und dass alle LIFs aktiv sind:

   ```
   network interface show -curr-node node4
   ```

4. Führen Sie eine der folgenden Aktionen durch:

Wenn node4…	Dann…
In einem Gehäuse getrennt von node3	Verbinden Sie den HA Interconnect zwischen den Nodes, indem Sie die folgenden Schritte ausführen: a. Schließen Sie den oberen Interconnect-Port von node3 an den oberen Interconnect-Port von node4 an. b. Schließen Sie den unteren Interconnect-Port von node3 an den unteren Interconnect-Port von node4 an. c. Gehen Sie zu Schritt 5.

Wenn node4…	Dann…
Im selben Chassis wie Node3	Gehen Sie zu Schritt 5. Sie müssen den HA Interconnect nicht manuell zwischen den Nodes verbinden. In derselben Chassis-Konfiguration wird der HA Interconnect automatisch über die Backplane verbunden.

5. Nehmen Sie eine der folgenden Aktionen:

Falls das Cluster…	Dann…
In einer SAN-Umgebung erfolgreich positionieren	Vollständig Schritt 6 Und gehen Sie zum Abschnitt "Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4".
Nicht in einer SAN-Umgebung	Überspringen Sie Schritt 6, gehen Sie zum Abschnitt "Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4".

6. Überprüfen Sie, ob node3 und node4 in Quorum sind, indem Sie auf einem der Knoten den folgenden Befehl eingeben:

```
event log show -messagename scsiblade.*
```

Das folgende Beispiel zeigt die Ausgabe, wenn sich die Nodes im Cluster im Quorum befinden:

```
cluster::> event log show -messagename scsiblade.*
Time                Node   Severity      Event
------------------- ------ ------------- --------------------------
8/13/2012 14:03:51  node1  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:51  node2  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:48  node3  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
8/13/2012 14:03:43  node4  INFORMATIONAL scsiblade.in.quorum: The scsi-
blade ...
```

Verschieben Sie die NAS-Daten-LIFs von node2 von node3 auf node4 und überprüfen Sie SAN LIFs auf node4

Nachdem Sie die node4-Installation überprüft haben und bevor Sie node2-Aggregate von node3 auf node4 verschieben, müssen Sie die NAS-Daten-LIFs, die sich im Besitz von node2 befinden, in node3 von node3 auf node4 verschieben. Sie müssen auch die SAN LIFs auf node4 überprüfen.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die

LIFs ordnungsgemäß sind und sich in den entsprechenden Ports befinden, nachdem Sie node4 in den Online-Modus versetzt haben.

Schritte

1. Führen Sie alle NAS-Daten-LIFs auf, die nicht im Besitz von node3 sind, durch Eingabe des folgenden Befehls auf einem der Nodes und Erfassung der Ausgabe auf:

   ```
   network interface show -role data -curr-node node3 -is-home false
   ```

2. Wenn das Cluster für SAN LIFs konfiguriert ist, notieren Sie in diesem Fall die SAN LIFs und vorhandene Konfigurationsinformationen "Arbeitsblatt" Zur späteren Verwendung im Verfahren.

   a. Führen Sie die SAN-LIFs auf Knoten3 auf und untersuchen Sie die Ausgabe:

      ```
      network interface show -data-protocol fc*
      ```

      Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

      ```
      cluster1::> net int show -data-protocol fc*
        (network interface show)
                  Logical     Status     Network            Current
      Current Is
      Vserver     Interface   Admin/Oper Address/Mask       Node
      Port    Home
      ----------  ----------  ---------- ------------------ -------------
      ------- ----
      svm2_cluster1
                  lif_svm2_cluster1_340
                              up/up      20:02:00:50:56:b0:39:99
                                                            cluster1-01
      1b      true
                  lif_svm2_cluster1_398
                              up/up      20:03:00:50:56:b0:39:99
                                                            cluster1-02
      1a      true
                  lif_svm2_cluster1_691
                              up/up      20:01:00:50:56:b0:39:99
                                                            cluster1-01
      1a      true
                  lif_svm2_cluster1_925
                              up/up      20:04:00:50:56:b0:39:99
                                                            cluster1-02
      1b      true
      4 entries were displayed.
      ```

   b. Führen Sie die vorhandenen Konfigurationen auf und untersuchen Sie die Ausgabe:

      ```
      fcp adapter show -fields switch-port,fc-wwpn
      ```

Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  ----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

3. Führen Sie eine der folgenden Aktionen durch:

Falls Knoten 2…	Beschreibung
Schnittstellengruppen oder VLANs wurden konfiguriert	Gehen Sie zu Schritt 4.
Schnittstellengruppen oder VLANs waren nicht konfiguriert	Überspringen Sie Schritt 4, und fahren Sie mit fort Schritt 5.

4. Nehmen Sie die folgenden Schritte durch, um alle NAS-Daten-LIFs zu migrieren, die auf Schnittstellengruppen und VLANs gehostet wurden, die sich ursprünglich auf node2 von node3 auf node4 befanden.

   a. Migrieren Sie alle auf node3 gehosteten LIFs, die zuvor node2 auf einer Schnittstellengruppe zu einem Port auf node4 gehören, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

   ```
   network interface migrate -vserver vserver_name -lif lif_name -destination
   -node node4 -destination-port netport|ifgrp
   ```

   b. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt A Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

   ```
   network interface modify -vserver vserver_name -lif datalif_name -home-node
   node4 home-port netport|ifgrp
   ```

c. [[man_lif_verify_4_subsepc] Migrieren Sie alle auf node3 gehosteten LIFs, die zuvor zu node2 auf einem VLAN-Port gehörten, zu einem Port auf node4, der in der Lage ist, LIFs auf demselben Netzwerk zu hosten, indem Sie den folgenden Befehl eingeben – einmal für jede LIF:

```
network interface migrate -vserver vserver_name -lif datalif_name
-destination-node node4 -destination-port netport|ifgrp
```

d. Ändern Sie den Home-Port und den Home-Node der LIFs in Unterschritt C Geben Sie zum Port und Node, der derzeit die LIFs hostet, den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif datalif_name -home-node
node4 home-port netport|ifgrp
```

5. Nehmen Sie eine der folgenden Aktionen:

Wenn das Cluster konfiguriert ist für…	Dann…
NAS	Vollständig Schritt 6 Bis Schritt 9, überspringen Sie Schritt 10, und abgeschlossen Schritt 11 Bis Schritt 14.
San	Überspringen Sie Schritt 6 bis Schritt 9, und schließen Sie sie ab Schritt 10 Bis Schritt 14.
Sowohl NAS als auch SAN	Vollständig Schritt 6 Bis Schritt 14.

6. Wenn auf Ihren Plattformen nicht dieselben Daten-Ports vorhanden sind, geben Sie den folgenden Befehl ein, um die Ports der Broadcast-Domäne hinzuzufügen:

```
network port broadcast-domain add-ports -ipspace IPspace_name -broadcast
-domain mgmt ports node:port
```

Das folgende Beispiel fügt Port „e0a“ auf den Knoten „6280-1“ und Port „e0i“ auf Knoten „8060-1“ zum Broadcast-Domain-Management im IPspace hinzu Standard:

```
cluster::> network port broadcast-domain add-ports -ipspace Default
-broadcast-domain mgmt -ports 6280-1:e0a, 8060-1:e0i
```

7. Migrieren Sie jede LIF mit NAS-Daten auf node4, indem Sie einmal für jede logische Schnittstelle den folgenden Befehl eingeben:

```
network interface migrate -vserver vserver-name -lif datalif-name -destination
-node node4 -destination-port netport|ifgrp -home-node node4
```

8. Sicherstellen, dass die Datenmigration persistent ist:

```
network interface modify -vserver vserver_name -lif datalif_name -home-port
netport|ifgrp
```

9. Überprüfen Sie den Status aller Links als `up` Mit dem folgenden Befehl werden alle Netzwerk-Ports aufgelistet und ihre Ausgabe untersucht:

```
network port show
```

Das folgende Beispiel zeigt die Ausgabe von `network port show` Befehl mit einigen LIFs oben und anderen unten:

```
cluster::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- ------- -----------
node3
       a0a       Default      -                up       1500  auto/1000
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0a-1     Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
node4
       e0M       Default      172.17.178.19/24 up       1500  auto/100
       e0a       Default      172.17.178.19/24 up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
12 entries were displayed.
```

10. Wenn die Ausgabe des `network port show` Befehl zeigt Netzwerkports an, die im neuen Node nicht verfügbar sind und in den alten Nodes vorhanden sind. Löschen Sie die alten Netzwerk-Ports, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie die erweiterte Berechtigungsebene ein, indem Sie den folgenden Befehl eingeben:

       `set -privilege advanced`

    b. Geben Sie für jeden alten Netzwerk-Port den folgenden Befehl ein:

       `network port delete -node` *`node_name`* `-port` *`port_name`*

    c. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:

       `set -privilege admin`

11. Bestätigen Sie, dass sich die SAN-LIFs auf den richtigen Ports an node4 befinden, indem Sie die folgenden Teilschritte ausführen:

    a. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

       `network interface show -data-protocol iscsi|fcp -home-node node4`

       Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster::> network interface show -data-protocol iscsi|fcp -home-node
node4
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            a0a          up/down  10.63.0.53/24      node4
a0a     true
            data1        up/up    10.63.0.50/18      node4
e0c     true
            rads1        up/up    10.63.0.51/18      node4
e1a     true
            rads2        up/down  10.63.0.52/24      node4
e1b     true
vs1
            lif1         up/up    172.17.176.120/24  node4
e0c     true
            lif2         up/up    172.17.176.121/24  node4
```

b. Überprüfen Sie, ob die neue `adapter` Und `switch-port` Die Konfigurationen sind korrekt, indem die Ausgabe von dem verglichen wird `fcp adapter show` Befehl mit den neuen Konfigurationsinformationen, die Sie im Arbeitsblatt in aufgezeichnet haben Schritt 2.

   Liste der neuen SAN LIF-Konfigurationen auf node4:

   `fcp adapter show -fields switch-port,fc-wwpn`

   Das System gibt die Ausgabe wie im folgenden Beispiel zurück:

```
cluster1::> fcp adapter show -fields switch-port,fc-wwpn
  (network fcp adapter show)
node         adapter  fc-wwpn                  switch-port
-----------  -------  -----------------------  -------------
cluster1-01  0a       50:0a:09:82:9c:13:38:00  ACME Switch:0
cluster1-01  0b       50:0a:09:82:9c:13:38:01  ACME Switch:1
cluster1-01  0c       50:0a:09:82:9c:13:38:02  ACME Switch:2
cluster1-01  0d       50:0a:09:82:9c:13:38:03  ACME Switch:3
cluster1-01  0e       50:0a:09:82:9c:13:38:04  ACME Switch:4
cluster1-01  0f       50:0a:09:82:9c:13:38:05  ACME Switch:5
cluster1-01  1a       50:0a:09:82:9c:13:38:06  ACME Switch:6
cluster1-01  1b       50:0a:09:82:9c:13:38:07  ACME Switch:7
cluster1-02  0a       50:0a:09:82:9c:6c:36:00  ACME Switch:0
cluster1-02  0b       50:0a:09:82:9c:6c:36:01  ACME Switch:1
cluster1-02  0c       50:0a:09:82:9c:6c:36:02  ACME Switch:2
cluster1-02  0d       50:0a:09:82:9c:6c:36:03  ACME Switch:3
cluster1-02  0e       50:0a:09:82:9c:6c:36:04  ACME Switch:4
cluster1-02  0f       50:0a:09:82:9c:6c:36:05  ACME Switch:5
cluster1-02  1a       50:0a:09:82:9c:6c:36:06  ACME Switch:6
cluster1-02  1b       50:0a:09:82:9c:6c:36:07  ACME Switch:7
16 entries were displayed
```

Wenn sich ein SAN LIF in der neuen Konfiguration nicht auf einem Adapter befindet, der noch an denselben angeschlossen ist `switch-port`, Es kann zu einem Systemausfall führen, wenn Sie den Node neu booten.

c. Wenn node4 eine SAN-LIFs oder Gruppen von SAN-LIFs hat, die sich auf einem Port befinden, der in node2 nicht vorhanden war, verschieben Sie sie in einen entsprechenden Port an node4, indem Sie einen der folgenden Befehle eingeben:

   i. Setzen Sie den LIF-Status auf „down“:

      `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-status -admin down`

   ii. Entfernen Sie das LIF aus dem Portsatz:

      `portset remove -vserver` *`vserver_name`* `-portset` *`portset_name`* `-port-name` *`port_name`*

   iii. Geben Sie einen der folgenden Befehle ein:

      - Verschieben eines einzelnen LIF:

        `network interface modify -lif` *`lif_name`* `-home-port` *`new_home_port`*

      - Verschieben Sie alle LIFs auf einem einzelnen nicht vorhandenen oder falschen Port in einen neuen Port:

```
network interface modify {-home-port port_on_node2 -home-node node2
-role data} -home-port new_home_port_on_node4
```

- Fügen Sie die LIFs wieder dem Portsatz hinzu:

```
portset add -vserver vserver_name -portset portset_name -port-name
port_name
```

Sie müssen SAN-LIFs zu einem Port verschieben, der die gleiche Verbindungsgeschwindigkeit wie der ursprüngliche Port hat.

12. Ändern Sie den Status aller LIFs in `up` Damit die LIFs Datenverkehr auf dem Node akzeptieren und senden können, indem Sie den folgenden Befehl eingeben:

```
network interface modify -vserver vserver_name -home-port port_name -home-node
node4 lif lif_name -status-admin up
```

13. Überprüfen Sie, ob alle SAN-LIFs zu den richtigen Ports verschoben wurden und ob die LIFs den Status von aufweisen `up` Wenn Sie auf einem der beiden Nodes den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
network interface show -home-node node4 -role data
```

14. Wenn LIFs ausgefallen sind, setzen Sie den Administrationsstatus der LIFs auf `up` Geben Sie den folgenden Befehl ein, einmal für jede LIF:

```
network interface modify -vserver vserver_name -lif lif_name -status-admin up
```

Arbeitsblatt: Informationen, die aufgezeichnet werden sollen, bevor NAS-Daten-LIFs in node4 verschoben werden

Um zu überprüfen, ob Sie die richtige Konfiguration haben, nachdem Sie SAN LIFs von node3 nach node4 verschoben haben, können Sie das folgende Arbeitsblatt verwenden, um die aufzuzeichnen `adapter` Und `switch-port` Informationen für jedes LIF.

Notieren Sie das LIF `adapter` Informationen aus dem `network interface show -data-protocol fc*` Befehlsausgabe und das `switch-port` Informationen aus dem `fcp adapter show -fields switch-port,fc-wwpn` Befehlsausgabe für node3.

Notieren Sie nach Abschluss der Migration zu node4 die LIF `adapter` Und `switch-port` Informationen für die LIFs auf node4 und vergewissern Sie sich, dass jede LIF noch immer mit derselben verbunden ist `switch-port`.

Node3			**Node4**		
LIF	`adapter`	`switch-port`	LIF	`adapter`	`switch-port`

Node3			Node4		

Verschiebung von nicht-Root-Aggregaten node2 von Node3 in node4

Nachdem node2's nicht-Root-Aggregate in node3 verschoben wurden, müssen Sie sie nun von node3 auf node4 verschieben.

Schritte

1. Geben Sie den folgenden Befehl auf beiden Controllern ein, und überprüfen Sie die Ausgabe, um zu ermitteln, welche nicht-Root-Aggregate verschoben werden sollen:

   `storage aggregate show -owner-name node3 -home-id node2_system_id`

2. Verschieben Sie die Aggregate, indem Sie die folgenden Teilschritte ausführen:

   a. Greifen Sie auf die erweiterte Berechtigungsebene zu, indem Sie den folgenden Befehl auf einem der Nodes eingeben:

      `set -privilege advanced`

   b. Geben Sie den folgenden Befehl ein:

      `storage aggregate relocation start -node node3 -destination node4 -aggregate -list aggr_name1, aggr_name2… -ndo-controller-upgrade true`

   Die Aggregatliste ist die Liste der Aggregate, deren Eigentümer node4 sind, die Sie in erhalten haben Schritt 1.

   a. Geben Sie bei der entsprechenden Aufforderung ein `y`.

      Umzüge finden im Hintergrund statt. Um ein Aggregat verschieben zu können, dauerte der Vorgang einige Sekunden oder Minuten. Die Zeit umfasst sowohl einen Client-Ausfall als auch Teile ohne Ausfälle. Mit dem Befehl werden keine Offline- oder eingeschränkten Aggregate verschoben.

   b. Zurück zur Administratorebene:

      `set -privilege admin`

3. Standortstatus prüfen:

   `storage aggregate relocation show -node node3`

   Die Ausgabe wird angezeigt `Done` Für ein Aggregat, nachdem es verlegt wurde.

   Warten Sie, bis alle node2-Aggregate in node4 verschoben wurden, bevor Sie mit dem nächsten Schritt fortfahren.

4. Führen Sie eine der folgenden Aktionen durch:

Bei Umzug von…	Dann…
Alle Aggregate waren erfolgreich	Gehen Sie zu Schritt 5.

Aggregate sind ausgefallen oder sie wurden Vetos gemacht	a. Überprüfen Sie die EMS-Protokolle auf Korrekturmaßnahmen.
	b. Führen Sie die Korrekturmaßnahme durch.
	c. Greifen Sie auf die erweiterte Berechtigungsebene zu, indem Sie den folgenden Befehl auf einem der Nodes eingeben:
	`set -privilege advanced`
	d. Verschiebung ausgefallener oder Vetos von Aggregaten:
	`storage aggregate relocation start -node node3 destination node4 -aggregate-list aggr_name1, aggr_name2… ndo-controller-upgrade true`
	Die aggregierte Liste enthält fehlerhafte oder Vetos zusammengesetzte Aggregate.
	e. Geben Sie bei der entsprechenden Aufforderung ein `y`.
	f. Kehren Sie zur Administratorebene zurück, indem Sie den folgenden Befehl eingeben:
	`set -privilege admin`
	Bei Bedarf können Sie die Verschiebung mit einer der folgenden Methoden erzwingen:
	• Veto-Prüfungen überschreiben:
	`storage aggregate relocation start -override -vetoes -ndo-controller-upgrade`
	• Zielprüfungen überschreiben:
	`storage aggregate relocation start -override -destination-checks -ndocontroller-upgrade`
	Weitere Informationen zu den Befehlen zum Verlegen von Storage-Aggregaten finden Sie unter "Quellen" Verbinden mit *Disk und Aggregat-Management mit den Befehlen CLI* und *ONTAP 9: Manual Page Reference*.

5. Überprüfen Sie, ob alle node2 nicht-Root-Aggregate online sind und ihren Status auf node4 haben:

   `storage aggregate show -node node4 -state offline -root false`

   Die node2 Aggregate wurden in der Ausgabe des Befehls in aufgeführt Schritt 1.

6. Wenn ein Aggregat offline gegangen ist oder fremd geworden ist, bringen Sie es mit dem folgenden Befehl

für jedes Aggregat online:

```
storage aggregate online -aggregate aggr_name
```

7. Überprüfen Sie, ob alle Volumes in node2 Aggregaten auf node4 online sind:

```
volume show -node node4 -state offline
```

8. Wenn Volumes auf node4 offline sind, bringen Sie sie online:

```
volume online -vserver vserver-name -volume volume_name
```

9. Senden Sie eine AutoSupport Nachricht nach dem Upgrade an NetApp für node4:

```
system node autosupport invoke -node node4 -type all -message "node2
successfully upgraded from platform_old to platform_new"
```

Phase 6: Schließen Sie das Upgrade ab

Phase-6-Übersicht

In Phase 6 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

1. "Authentifizierungsmanagement mit KMIP-Servern"
2. "Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind"
3. "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein"
4. "Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul"
5. "Ausmustern des alten Systems"
6. "Setzen Sie den SnapMirror Betrieb fort"

Authentifizierungsmanagement mit KMIP-Servern

Mit ONTAP 9.5 und höher können KMIP-Server (Key Management Interoperability Protocol) Authentifizierungsschlüssel managen.

Schritte

1. Hinzufügen eines neuen Controllers:

```
security key-manager setup -node new_controller_name
```

2. Fügen Sie den Schlüsselmanager hinzu:

```
security key-manager -add key_management_server_ip_address
```

3. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server konfiguriert und für alle Nodes im Cluster verfügbar sind:

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

4. Stellen Sie die Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern auf den neuen Knoten wieder her:

```
security key-manager restore -node new_controller_name
```

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um die korrekte Einrichtung zu bestätigen, aktivieren Sie das HA-Paar. Außerdem überprüfen Sie, ob Node 3 und node 4 auf den Storage zugreifen können und ob keine der Daten-LIFs gehören, die zu anderen Nodes im Cluster gehören. Außerdem bestätigen Sie, dass Node 3 Eigentümer der Aggregate von Node 1 ist und node4 Eigentümer der Aggregate von Node 2 ist und die Volumes für beide Nodes online sind.

Schritte

1. Aktivieren Sie Storage Failover, indem Sie auf einem der Nodes den folgenden Befehl eingeben:

```
storage failover modify -enabled true -node node3
```

2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

```
storage failover show
```

Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt, wenn ein Storage Failover aktiviert ist:

```
cluster::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ------------------
node3          node4          true     Connected to node4
node4          node3          true     Connected to node3
```

3. Führen Sie eine der folgenden Aktionen durch:

Wenn der Cluster ein…	Beschreibung
Cluster mit zwei Nodes	Aktivieren Sie die Hochverfügbarkeit im Cluster, indem Sie auf einem der Nodes den folgenden Befehl eingeben: `cluster ha modify -configured true`
Cluster mit mehr als zwei Nodes	Gehen Sie zu Schritt 4.

4. Überprüfen Sie, ob node3 und node4 zum selben Cluster gehören, indem Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
cluster show
```

5. Stellen Sie sicher, dass node3 und node4 auf den Storage der jeweils anderen zugreifen können, indem

Sie den folgenden Befehl eingeben und die Ausgabe überprüfen:

```
storage failover show -fields local-missing-disks,partner-missing-disks
```

6. Vergewissern Sie sich, dass weder node3 noch node4 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Geben Sie dazu den folgenden Befehl ein und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn Node3 oder node4 im Besitz von Daten-LIFs sind, die sich im Besitz anderer Nodes im Cluster befinden, verwenden Sie die `network interface revert` Befehl zum Zurücksetzen der Daten-LIFs auf den Home-Eigentümer.

7. Überprüfen Sie, ob node3 die Aggregate von node1 besitzt und dass node4 die Aggregate von node2 besitzt:

   ```
   storage aggregate show -owner-name node3
   storage aggregate show -owner-name node4
   ```

8. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node node3 -state offline
   volume show -node node4 -state offline
   ```

9. Wenn Volumes offline sind, vergleichen Sie sie mit der Liste der Offline-Volumes, die Sie in erfasst haben "Schritt 19 (d)" In *die Nodes für Upgrade* vorbereiten und jedes der Offline-Volumes nach Bedarf durch Eingabe des folgenden Befehls ein Mal für jedes Volume den Online-Modus versetzen:

   ```
   volume online -vserver vserver_name -volume volume_name
   ```

10. Installieren Sie neue Lizenzen für die neuen Nodes, indem Sie den folgenden Befehl für jeden Node eingeben:

    ```
    system license add -license-code license_code,license_code,license_code…
    ```

    Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, jeden Lizenzschlüssel durch ein Komma getrennt.

11. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie den eingestellt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel in "Schritt 16" Von *Install and Boot node3*) müssen Sie die Variable aufheben:

    ```
    set diag; systemshell -node node_name -command sudo kenv -u -p
    kmip.init.maxwait
    ```

12. Geben Sie einen der folgenden Befehle ein, um alle alten Lizenzen von den ursprünglichen Nodes zu entfernen:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number node_serial_number -package
    licensable_package
    ```

    - Um alle abgelaufenen Lizenzen zu löschen, geben Sie Folgendes ein:

```
system license clean-up -expired
```

- Um alle nicht verwendeten Lizenzen zu löschen, geben Sie Folgendes ein:

```
system license clean-up -unused
```

- Geben Sie zum Löschen einer bestimmten Lizenz von einem Cluster die folgenden Befehle auf den Nodes ein:

```
system license delete -serial-number node1_serial_number -package *
system license delete -serial-number node2_serial_number -package *
```

Die folgende Ausgabe wird angezeigt:

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

+
Eingabe `y` Um alle Pakete zu entfernen.

13. Überprüfen Sie die ordnungsgemäße Installation der Lizenzen, indem Sie den folgenden Befehl eingeben und seine Ausgabe überprüfen:

```
system license show
```

Sie können die Ausgabe mit der Ausgabe vergleichen, die Sie in erfasst haben "Schritt 30" Von *die Nodes für Upgrade vorbereiten*.

14. Konfigurieren Sie die SPs, indem Sie auf beiden Knoten den folgenden Befehl ausführen:

```
system service-processor network modify -node node_name
```

Gehen Sie zu "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen über die SPs und die Befehle *ONTAP 9: Manual Page Reference* für detaillierte Informationen zum `system service-processor network modify` Befehl.

15. Wenn Sie ein Cluster ohne Switches auf den neuen Nodes einrichten möchten, fahren Sie mit fort "Quellen" Um eine Verbindung zur *Network Support Site* herzustellen, befolgen Sie die Anweisungen unter „ Wechsel zu einem 2-Node-Cluster ohne Switch_“.

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf Node3 und node4 aktiviert ist, führen Sie die Schritte in aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Führen Sie andernfalls die Schritte unter aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

Wenn der ersetzte Controller oder der HA-Partner des neuen Controllers Storage Encryption verwendet, müssen Sie das neue Controller-Modul für Storage Encryption konfigurieren, einschließlich der Installation von SSL-Zertifikaten und der Einrichtung von

Key Management-Servern.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

   ```
   security key-manager show -status

   security key-manager query
   ```

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers im neuen Controller hinzu.
   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

      ```
      security key-manager -add key_management_server_ip_address
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server.

      Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.

   c. Überprüfen Sie, ob die Verschlüsselungsmanagementserver erfolgreich hinzugefügt wurden:

      ```
      security key-manager show
      ```

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Schlüsselmanagementserver auf dem neuen Knoten:

      ```
      security key-manager setup -node new_controller_name
      ```

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.
4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her:

   ```
   security key-manager restore -node new_controller_name
   ```

Einrichtung von NetApp Volume oder Aggregate Encryption auf dem neuen Controller-Modul

Wenn der ersetzte Controller oder der HA-Partner (High Availability, Hochverfügbarkeit) des neuen Controllers NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) verwendet, muss das neue Controller-Modul für NVE oder NAE konfiguriert werden.

Über diese Aufgabe

Dieses Verfahren umfasst Schritte, die auf dem neuen Controller-Modul ausgeführt werden. Sie müssen den Befehl auf dem richtigen Node eingeben.

Schritte

1. Vergewissern Sie sich, dass die Verschlüsselungsmanagement-Server weiterhin verfügbar sind, deren Status und ihre Authentifizierungsdaten folgendermaßen sind:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 oder 9.7	`security key-manager key query -node node`
ONTAP 9.5 oder früher	`security key-manager key show`

2. Fügen Sie die im vorherigen Schritt aufgeführten Verschlüsselungsmanagement-Server der Liste des zentralen Management-Servers des neuen Controllers hinzu:
   a. Fügen Sie den Verschlüsselungsmanagementserver mit dem folgenden Befehl hinzu:

      `security key-manager -add key_management_server_ip_address`

   b. Wiederholen Sie den vorherigen Schritt für jeden aufgeführten Key Management Server. Sie können bis zu vier Verschlüsselungsmanagement-Server verknüpfen.
   c. Überprüfen Sie, ob die Verschlüsselungsmanagement-Server erfolgreich hinzugefügt wurden. Verwenden Sie dazu den folgenden Befehl:

      `security key-manager show`

3. Führen Sie auf dem neuen Controller-Modul den Setup-Assistenten für das Verschlüsselungsmanagement aus, um die wichtigsten Management-Server einzurichten und zu installieren.

   Sie müssen dieselben Key Management-Server installieren, die auf dem vorhandenen Controller-Modul installiert sind.

   a. Starten Sie den Setup-Assistenten für den Verschlüsselungsmanagement-Server auf dem neuen Knoten, indem Sie den folgenden Befehl verwenden:

      `security key-manager setup -node new_controller_name`

   b. Führen Sie die Schritte im Assistenten zum Konfigurieren von Verschlüsselungsmanagementservern durch.
4. Stellen Sie Authentifizierungsschlüssel von allen verknüpften Verschlüsselungsmanagementservern mit dem neuen Knoten wieder her.

   - Authentifizierung für externen Schlüsselmanager wiederherstellen:

     `security key-manager external restore`

     Für diesen Befehl ist die OKM-Passphrase (Onboard Key Manager) erforderlich

   Weitere Informationen finden Sie im Knowledge Base-Artikel "So stellen Sie die Konfiguration des externen Schlüsselmanager-Servers aus dem ONTAP-Startmenü wieder her".

   - Authentifizierung für den OKM wiederherstellen:

Für diese ONTAP-Version…	Befehl
Alle anderen ONTAP-Versionen	`security key-manager onboard sync`
ONTAP 9.5	`security key-manager setup -node node_name`

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder externe Verschlüsselungsmanagementserver nicht erreicht werden konnten. Stellen Sie diese Volumes mithilfe der wieder online `volume online` Befehl.

Ausmustern des alten Systems

Nach dem Upgrade kann das alte System über die NetApp Support Site außer Betrieb gesetzt werden. Die Deaktivierung des Systems sagt NetApp, dass das System nicht mehr in Betrieb ist und dass es aus Support-Datenbanken entfernt wird.

Schritte

1. Siehe "Quellen" Um auf die *NetApp Support Site* zu verlinken und sich anzumelden.
2. Wählen Sie im Menü die Option **Produkte > Meine Produkte**.
3. Wählen Sie auf der Seite **installierte Systeme anzeigen** die **Auswahlkriterien** aus, mit denen Sie Informationen über Ihr System anzeigen möchten.

   Sie können eine der folgenden Optionen wählen, um Ihr System zu finden:

   - Seriennummer (auf der Rückseite des Geräts)
   - Seriennummern für „My Location“
4. Wählen Sie **Los!**

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.
5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

Sie können SnapMirror Transfers, die vor dem Upgrade stillgelegt wurden, fortsetzen und die SnapMirror Beziehungen fortsetzen. Die Updates sind nach Abschluss des Upgrades im Zeitplan.

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```
2. Wiederaufnahme der SnapMirror Beziehung:

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Fehlerbehebung

Fehlerbehebung

Möglicherweise ist beim Upgrade des Node-Paars ein Fehler auftritt. Der Node kann abstürzen, Aggregate werden möglicherweise nicht verschoben oder LIFs werden nicht migriert. Die Ursache des Fehlers und seiner Lösung hängt davon ab, wann der Fehler während des Aktualisierungsvorgangs aufgetreten ist.

Siehe Tabelle, in der die verschiedenen Phasen des Verfahrens im Abschnitt beschrieben werden "ARL Upgrade-Workflow". Die Informationen über mögliche Fehler werden in der Phase des Verfahrens aufgelistet.

- "Fehler bei der Aggregatverschiebung"
- "Neustarts, Panikspiele oder Energiezyklen"
- "Probleme, die in mehreren Phasen des Verfahrens auftreten können"
- "Fehler bei der LIF-Migration"
- "LIFs befinden sich bei ungültigen Ports nach dem Upgrade"

Fehler bei der Aggregatverschiebung

Bei der Aggregatverschiebung (ARL, Aggregate Relocation) fallen während des Upgrades möglicherweise an verschiedenen Punkten aus.

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

Während des Verfahrens kann ARL in Phase 2, Phase 3 oder Phase 5 fehlschlagen.

Schritte

1. Geben Sie den folgenden Befehl ein und überprüfen Sie die Ausgabe:

   ```
   storage aggregate relocation show
   ```

   Der `storage aggregate relocation show` Der Befehl zeigt Ihnen, welche Aggregate erfolgreich umgezogen wurden und welche nicht, zusammen mit den Ursachen des Ausfalls.

2. Überprüfen Sie die Konsole auf EMS-Nachrichten.
3. Führen Sie eine der folgenden Aktionen durch:

   - Führen Sie die entsprechenden Korrekturmaßnahmen durch, je nach der Ausgabe des `storage aggregate relocation show` Befehl und Ausgabe der EMS-Nachricht.
   - Erzwingen Sie das verlagern des Aggregats oder der Aggregate mit dem `override-vetoes` Oder die Option `override-destination-checks` Option des `storage aggregate relocation start` Befehl.

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 waren, gehören node4 nach Abschluss des Upgrades

Beim Abschluss des Upgrade-Verfahrens muss die Knoten3 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node die Knoten1 hatten. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Unter den folgenden Umständen kann es nicht gelingen, Aggregate ordnungsgemäß zu verschieben und Node 1 als Home Node anstelle von Knoten3 zu verwenden:

- In Phase 3, wenn Aggregate von node2 auf node3 verschoben werden. Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann wird das Aggregat auf node2 zurückgelassen.
- Nach Stufe 4, wenn node2 durch node4 ersetzt wird. Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node4 als Home-Node statt node3 online.

Sie können das falsche Eigentümerproblem nach Phase 6 beheben, wenn ein Storage-Failover aktiviert wurde, indem Sie die folgenden Schritte durchführen:

Schritte

1. Geben Sie den folgenden Befehl ein, um eine Liste der Aggregate zu erhalten:

   `storage aggregate show -nodes` *`node4`* `-is-home true`

   Informationen zur Identifizierung von Aggregaten, die nicht korrekt verschoben wurden, finden Sie in der Liste der Aggregate mit dem Home-Inhaber von node1, die Sie im Abschnitt erhalten haben "Bereiten Sie die Knoten für ein Upgrade vor" Und vergleichen Sie ihn mit der Ausgabe des obigen Befehls.

2. Vergleichen Sie die Ausgabe von Schritt 1 Mit der Ausgabe, die Sie für node1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links auf node4:

   `storage aggregate relocation start -node` *`node4`* `-aggr` *`aggr_node_1`* `-destination` *`node3`*

   Verwenden Sie das nicht `-ndo-controller-upgrade` Parameter während dieser Verschiebung.

4. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob node3 jetzt der Haupteigentümer der Aggregate ist:

   `storage aggregate show -aggregate` *`aggr1,aggr2,aggr3…`* `-fields home-name`

   `aggr1,aggr2,aggr3…` Ist die Liste der Aggregate, die node1 als ursprünglichen Besitzer hatten.

   Aggregate, die nicht über Node3 als Hausbesitzer verfügen, können mit dem gleichen Relocation-Befehl in auf node3 verschoben werden Schritt 3.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, in Panik geraten oder aus- und wieder eingeschaltet werden. Die Lösung dieser

Probleme hängt davon ab, wann sie auftreten.

Neustarts, Panikspiele oder Energiezyklen in Phase 2

Abstürze können vor, während oder unmittelbar nach Phase 2 auftreten, während der Sie Aggregate von node1 auf node2 verschieben, Daten-LIFs und SAN-LIFs im Besitz von node1 auf node2 verschieben, node1-Informationen aufzeichnen und Knoten1 ausmustern.

Node1 oder node2 stürzt vor Phase 2 ab, und HA ist noch aktiviert

Wenn node1 oder node2 vor Phase 2 abstürzt, wurden noch keine Aggregate verschoben und die HA-Konfiguration ist noch aktiviert.

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

1. Überprüfen Sie die Konsole auf EMS-Meldungen, die das System möglicherweise ausgegeben hat, und ergreifen Sie die empfohlenen Korrekturmaßnahmen.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt während oder direkt nach Phase 2 ab, und HA ist noch aktiviert

Einige oder alle Aggregate wurden von node1 in node2 verschoben und die HA ist noch aktiviert. Node2 wird das Root-Volume von node1 und alle nicht-Root-Aggregate übernehmen, die nicht verschoben wurden.

Über diese Aufgabe

Das Eigentum an verlagerten Aggregaten sieht mit dem Eigentum nicht-Root-Aggregaten identisch aus, die übernommen wurden, da sich der Home-Eigentümer nicht geändert hat. Wenn node1 in den eintritt `waiting for giveback state`, Node2 wird alle node1 nicht-Root-Aggregate zurückgeben.

Schritte

1. Vollständig "Schritt 1" Im Abschnitt *Non-Root-Aggregate wieder von node1 nach node2* verschieben.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node1 stürzt nach Phase 2 ab, während HA deaktiviert ist

Node2 wird nicht übernehmen, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 1 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

   Möglicherweise sehen Sie einige Änderungen in der Ausgabe von `storage failover show` Befehl, aber das ist typisch und hat keine Auswirkung auf das Verfahren. Siehe Abschnitt Fehlerbehebung "Unerwarteter Storage-Failover zeigt die Befehlsausgabe an".

Node2 fällt während oder nach Phase 2 aus, bei aktiviertem HA

Node1 hat einige oder alle seine Aggregate in node2 verschoben. HA ist aktiviert.

Über diese Aufgabe

Node1 wird alle Aggregate node2 sowie alle eigenen Aggregate übernehmen, die es auf node2 verlagert hatte. Wenn node2 in den eintritt `Waiting for Giveback` Zustand: Node1 gibt alle Aggregate node2 zurück.

Schritte

1. Vollständig "Schritt 1" Im Abschnitt *Non-Root-Aggregate wieder von node1 nach node2* verschieben.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt nach Phase 2 ab und nach HA ist deaktiviert

Node1 wird nicht übernehmen.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall wird für alle Aggregate auftreten, während node2 gestartet wird.

2. Fahren Sie mit dem verbleibenden Upgrade des Node-Paars fort.

Neustarts, Panikspiele oder Energiezyklen in Phase 3

Ausfälle können während oder unmittelbar nach Phase 3 auftreten. In dieser Phase installieren und booten Sie Node3, weisen Ports von node1 zu node3 zu, verschieben Daten-LIFs und SAN-LIFs, die zu node1 und node2 zu node3 gehören, und verschieben alle Aggregate von node2 auf node3.

Knoten 2 Absturz in Phase 3 mit deaktiviertem HA und vor dem Verschieben von Aggregaten

Node3 wird nach einem Absturz nach einem node2 nicht mehr übernehmen, da HA bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

   Ein Client-Ausfall wird für alle Aggregate auftreten, während node2 gestartet wird.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node2 stürzt während Phase 3 ab, nachdem einige oder alle Aggregate verschoben wurden

Node2 hat einige oder alle seine Aggregate in Node3 verschoben, die Daten von Aggregaten bereitstellen, die umgezogen wurden. HA ist deaktiviert.

Über diese Aufgabe

Es wird ein Client-Ausfall für Aggregate geben, die nicht verlagert wurden.

Schritte

1. Knoten 2 aufbring.
2. Verschieben Sie die verbleibenden Aggregate durch Abschluss "Schritt 1" Bis "Schritt 3" Im Abschnitt *Non-Root-Aggregate von node2 auf node3* verschieben.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während Phase 3 und vor node2 hat alle Aggregate verschoben

Node2 übernimmt nicht, aber es stellt immer noch Daten aus allen nicht-Root-Aggregaten bereit.

Schritte

1. Knoten 3 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt während der Phase 3 während der Aggregatverschiebung ab

Falls node3 abstürzt, während node2 Aggregate zu node3 verschoben wird, wird node2 die Verschiebung aller verbleibenden Aggregate abbrechen.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, doch Aggregate, die bereits in Knoten 3 verlagert wurden, begegnen ein Client-Ausfall, während node3 gebootet wird.

Schritte

1. Knoten 3 aufbring.
2. Vollständig "Schritt 3" Wieder im Abschnitt *Verschiebung von nicht-Root-Aggregaten von node2 zu node3*.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 startet nach einem Absturz in Phase 3 nicht

Aufgrund eines katastrophalen Ausfalls kann nach einem Absturz in Phase 3 nicht node3 gestartet werden.

Schritt

1. Wenden Sie sich an den technischen Support.

Node2 stürzt nach Phase 3 aber vor Phase 5 ab

Node3 stellt weiterhin Daten für alle Aggregate bereit. Das HA-Paar ist deaktiviert.

Schritte

1. Knoten 2 aufbring.
2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node3 stürzt nach Phase 3, aber vor Phase 5 ab

Node3 stürzt nach Phase 3, aber vor Phase 5 ab. Das HA-Paar ist deaktiviert.

Schritte

1. Knoten 3 aufbring.

   Es gibt einen Client-Ausfall für alle Aggregate.

2. Fahren Sie mit dem Upgrade des Node-Paars fort.

Neustarts, Panikspiele oder Energiezyklen in Phase 5

Es können zu Abstürzen kommen, während Phase 5, in der Sie node4 installieren und booten, Ports von node2 nach node4 abbilden, Daten-LIFs und SAN-LIFs, die zu node2 von node3 nach node4 gehören, und alle Aggregate von node2 in node4 verschieben.

Node3 stürzt in Phase 5 ab

Node3 hat einige oder alle node2 Aggregate in node4 verschoben. Node4 übernimmt nicht, dient aber weiterhin nicht-Root-Aggregate, die node3 bereits verschoben hat. Das HA-Paar ist deaktiviert.

Über diese Aufgabe

Es gibt einen Ausfall für den Rest der Aggregate, bis node3 wieder hochfährt.

Schritte

1. Knoten 3 aufbring.
2. Verschiebung der verbleibenden Aggregate, die zu Knoten 2 gehörten, durch Wiederholung "Schritt 1" Bis "Schritt 3" Im Abschnitt *Verschiebung der nicht-Root-Aggregate von node2 nach node3*.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Node4 stürzt in Phase 5 ab

Node3 hat einige oder alle node2 Aggregate in node4 verschoben. Node3 übernimmt nicht die Übernahme, dient aber weiterhin nicht-Root-Aggregate, die Node3 besitzt, sowie solche, die nicht verlagert wurden. HA ist deaktiviert.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits verschoben wurden, bis node4 wieder hochfährt.

Schritte

1. bringen sie node4 auf.
2. Verschiebung der verbleibenden Aggregate, die zu node2 gehörten, durch erneute Fertigstellung "Schritt 1" Bis "Schritt 3" In *Verschiebung der nicht-Root-Aggregate von node2 nach node4*.
3. Fahren Sie mit dem Upgrade des Node-Paars fort.

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

Wenn während der Prozedur der Node, der alle Daten hostet, „Panik und“ oder versehentlich neu gebootet wird, wird möglicherweise die unerwartete Ausgabe für den angezeigt `storage failover show` Befehl vor und nach dem Neubooten, Panic oder aus- und Wiedereinschalten.

Über diese Aufgabe

Möglicherweise wird eine unerwartete Ausgabe von der angezeigt `storage failover show` Befehl in Phase 2, Stufe 3, Stufe 4 oder Stufe 5.

Das folgende Beispiel zeigt die erwartete Ausgabe von `storage failover show` Befehl, wenn auf dem Node, der alle Datenaggregate hostet, kein Neubooten oder „Panic“ erfolgt:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------  --------- -----------------
node1    node2     false     Unknown
node2    node1     false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

Das folgende Beispiel zeigt die Ausgabe von `storage failover show` Befehl nach einem Neubooten oder Panic:

```
cluster::> storage failover show

                    Takeover
Node     Partner    Possible  State Description
-------  --------  --------- -----------------
node1    node2     -         Unknown
node2    node1    false      Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

Obwohl die Ausgabe sagt, dass sich ein Node im teilweise Giveback befindet und der Storage-Failover deaktiviert ist, können Sie diese Meldung ignorieren.

Schritte

Es ist keine Aktion erforderlich. Fahren Sie mit dem Upgrade des Node-Paars fort.

Fehler bei der LIF-Migration

Nach der Migration der LIFs sind diese nach der Migration in Phase 2, Phase 3 oder Phase 5 möglicherweise nicht online.

Schritte

1. Vergewissern Sie sich, dass die MTU-Port-Größe mit der Größe des Quell-Nodes identisch ist.

   Wenn beispielsweise die MTU-Größe des Cluster-Ports am Quell-Node 9000 ist, sollte sie auf dem Ziel-Node 9000 sein.

2. Überprüfen Sie die physische Konnektivität des Netzwerkkabels, wenn der physische Status des Ports „ausgefallen“ ist.

LIFs befinden sich bei ungültigen Ports nach dem Upgrade

Nach Abschluss des Upgrades befinden sich die logischen FC-Schnittstellen (LIFs) bei einer MetroCluster-Konfiguration möglicherweise auf falschen Ports. Sie können einen Neusynchronisierung durchführen, um die LIFs den richtigen Ports zuzuweisen.

Schritt

1. Geben Sie das ein `metrocluster vserver resync` Befehl zum Neuzuweisen der LIFs zu den richtigen Ports.

   `metrocluster vserver resync -vserver` *`vserver_name`* `fcp-mc.headupgrade.test.vs`

Quellen

Wenn Sie die Verfahren in diesem Inhalt ausführen, müssen Sie möglicherweise Referenzinhalt konsultieren oder zu Referenzwebsites gehen.

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

Die für dieses Upgrade spezifischen Inhalte sind in der folgenden Tabelle aufgeführt.

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.

Inhalt	Beschreibung
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.

Inhalt	Beschreibung
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

Der "NetApp Support Website" Enthält auch Dokumentation zu Netzwerkschnittstellenkarten (NICs) und anderer Hardware, die Sie mit Ihrem System verwenden könnten. Es enthält auch die "Hardware Universe", Die Informationen über die Hardware liefert, die das neue System unterstützt.

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.