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

Upgrade controllers

NetApp
July 05, 2024

Inhalt

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
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.