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

Upgrade controllers

NetApp
February 22, 2024

Inhalt

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

Überblick

Dieses Verfahren beschreibt das unterbrechungsfreie Upgrade der Controller-Hardware auf einem HA-Paar mit Aggregatverschiebung (Aggregate Relocation, ARL) für die folgenden Systemkonfigurationen. Dabei wird das alte System in das Ersatzsystem konvertiert, wobei das alte Systemgehäuse und die alten Festplatten erhalten bleiben.

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

Altes System	Austauschsystem	Unterstützte ONTAP-Versionen
AFF A220 als All-SAN-Array (ASA) konfiguriert	ASA A150	9.13.1P1 und höher
AFF A220	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 und höher
AFF A200	AFF A150	9.10.1P15, 9.11.1P11 und höher AFF A200 unterstützt ONTAP Versionen ab 9.11.1 nicht.
AFF C 190	AFF A150	9.10.1P15, 9.11.1P11, 9.12.1P5 und höher
FAS2620	FAS2820	9.11,1 P7 (FAS2620) Die FAS2620 unterstützt ONTAP Versionen ab 9.11.1 nicht. 9.13.1 und höher (FAS2820)
FAS2720	FAS2820	9.13.1 und höher
AFF A700 – als ASA konfiguriert	ASA A900	9.13.1P1 und höher
AFF A700	AFF A900	9.10.1P10, 9.11.1P6 und höher
FAS9000	FAS9500	9.10.1P10, 9.11.1P6 und höher

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

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

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

Über diese Aufgabe

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

- Tauschen Sie das Controller-Modul an jedem Knoten des alten Controllers gegen das neue Modul aus. Dies gilt für ein System-Upgrade auf AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720.
- Tauschen Sie den Controller und die NVRAM-Module auf jedem Node des alten Controllers gegen die neuen Module aus. Dies gilt für ein Upgrade des AFF A700 oder FAS9000 Systems.

Sie müssen die I/O-Karten, Datenkabel, Platten-Shelfs und Festplatten nicht verschieben, trennen oder erneut anschließen.

Bei diesem Verfahren wird eine Methode namens Aggregate Relocation (ARL) verwendet. Diese Methode nutzt die HA-Konfiguration. So können Sie die Eigentümerschaft von nicht-Root-Aggregaten von einem Node auf einen anderen verschieben, wenn sie Storage innerhalb desselben Clusters gemeinsam nutzen.

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

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

Wichtige Informationen

- Diese Vorgehensweise ist komplex und setzt voraus, dass Sie über erweiterte ONTAP-Administrationsfähigkeiten verfügen. Sie sollten auch lesen und verstehen, die "Richtlinien für Controller Upgrades" Und das "Überblick über das ARL Upgrade" Abschnitte vor Beginn der Aktualisierung.
- Bei diesem Verfahren wird vorausgesetzt, dass die Ersatz-Controller-Hardware neu ist und nicht in einem anderen System verwendet wurde. Die erforderlichen Schritte zur Vorbereitung gebrauter Controller mit dem `wipeconfig` Befehl ist in dieser Prozedur nicht enthalten. Sie müssen sich an den technischen Support wenden, wenn die Ersatz-Controller-Hardware zuvor als Teil eines anderen ONTAP Clusters oder als Standalone-System mit einem einzelnen Node verwendet wurde.
- Sie können dieses Verfahren zum Upgrade der Controller Hardware in Clustern mit mehr als zwei Nodes verwenden. Sie müssen jedoch die Verfahren für jedes HA-Paar im Cluster separat durchführen.
- Wenn Sie über einen Switch verfügen, der von der ONTAP-Version und dem Ersatzsystem, auf das Sie aktualisieren, nicht unterstützt wird, finden Sie weitere Informationen unter "Quellen" Zum Verknüpfen mit

der *Hardware Universe*.

- Dieses Verfahren gilt nur für AFF A200, AFF A220, AFF C190, FAS2720, FAS2720, AFF A700 und FAS9000 Systeme. Informationen zu allen anderen Controller-Modellen, die ein Upgrade auf ein AFF A150-, FAS2820-, AFF A900- oder FAS9500-System erfordern, finden Sie unter "Quellen" Verwenden Sie zum Verlinken die Befehle „System Controller Replace“, um die Controller-Hardware mit ONTAP 9.8 oder höher und die Aggregatverschiebung _verwenden, um die Controller-Hardware mit ONTAP 9.8 oder neuer manuell zu aktualisieren.
- Die ASA Systeme A900, AFF A900 und FAS9500 unterstützen nur eine hohe Netzspannung (200 V bis 240 V). Wenn Ihr AFF A700 oder FAS9000 System mit niedriger Netzspannung (100 V bis 120 V) ausgeführt wird, müssen Sie vor diesem Verfahren die Eingangsspannung der AFF A700 oder FAS9000 konvertieren.
- Wenn Sie ein Upgrade von einer AFF A200, AFF A220, AFF C190, FAS2720, FAS2720, AFF A700 oder FAS9000 System mit Ausfallzeiten können Sie die Controller-Hardware durch Verschieben von Storage aufrüsten oder sich an den technischen Support wenden. Siehe "Quellen" Link zu *Upgrade durch Verschieben von Volumes oder Storage*.

Automatisierung des Controller-Upgrades

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

Entscheiden Sie, ob Sie das Verfahren zur Aggregatverschiebung verwenden

Dieser Inhalt beschreibt, wie Sie ein Upgrade von Storage Controllern in einem HA-Paar durchführen, ohne dabei alle vorhandenen Daten und Festplatten zu beeinträchtigen. Dies ist ein komplexes Verfahren, das nur von erfahrenen Administratoren verwendet werden sollte.

Sie können dieses Verfahren unter folgenden Umständen verwenden:

- Sie führen eines der folgenden Controller-Upgrades aus:

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

- Sie haben mit Ihrem NetApp Vertriebsmitarbeiter verifiziert, dass Sie die Hardware für das Controller-Upgrade erhalten haben:
  - ASA Controller A150, AFF A150 oder FAS2820
  - ASA Controller- und NVRAM-Module A900, AFF A900 oder FAS9500 sowie die für das Upgrade

erforderlichen Teile

- Sie verwenden die minimale ONTAP-Version für Ihr Upgrade. Weitere Informationen finden Sie unter "Überblick".
- Sie möchten die neuen Controller nicht als neues HA-Paar zum Cluster hinzufügen und die Daten mithilfe von Volume-Verschiebungen migrieren.
- Sie sind erfahren in der Verwaltung von ONTAP und sind mit den Risiken der Arbeit im Diagnose-Privilege-Modus vertraut.

Sie können dieses Verfahren unter folgenden Umständen nicht verwenden:

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

Informationen zum Upgrade von Fabric MetroCluster- oder MetroCluster IP-Konfigurationen auf AFF A700 oder FAS9000 Systemen finden Sie unter "Quellen" Zum Verlinken auf den Inhalt *MetroCluster Upgrade und Expansion*.

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

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

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

Die erforderlichen Tools und Dokumentationen

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

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

Richtlinien für Controller Upgrades

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

Unterstützte Upgrades für ARL

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

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

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

2-Node-Cluster ohne Switches

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

Switch Attached-Cluster

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

Fehlerbehebung

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

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

Überblick über das ARL Upgrade

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

Aktualisieren Sie das Node-Paar

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

Übersicht über die ARL-Upgrade-Sequenz

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

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

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

Stufe	Schritte
"Phase 1: Upgrade vorbereiten"	In Phase 1 überprüfen Sie, ob Sie über die richtige Hardware für Ihr Upgrade verfügen, führen Vorabprüfungen durch und korrigieren bei Bedarf die Eigentümerschaft für Aggregate. Sie müssen bestimmte Informationen aufzeichnen, wenn Sie Storage Encryption mit dem Onboard Key Manager managen und die SnapMirror Beziehungen stilllegen möchten. Gesamteigentum am Ende von Phase 1: • Node1 ist der Hausbesitzer und der aktuelle Besitzer der node1 Aggregate • Node2 ist der Hausbesitzer und der aktuelle Besitzer der node2 Aggregate
"Phase 2: Ressourcen verlagern und Knoten in den Ruhestand zurücknehmen 1"	In Phase 2 verschieben Sie Node1-nicht-Root-Aggregate und NAS-Daten-LIFs von Node1 zu Node2. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie erfassen Node1-Informationen für die spätere Verwendung im Verfahren vor dem Ausscheiden von node1. Sie können sich auch später beim Verfahren auf den Netzboot node1 vorbereiten. Gesamteigentum am Ende von Phase 2: • Node2 ist der aktuelle Besitzer von node1 Aggregaten • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten
"Stufe 3: Starten Sie Node1 mit den Ersatz-Systemmodulen"	In Phase 3 starten Sie node1 mit aktualisierten Systemmodulen und überprüfen die aktualisierte node1-Installation. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1 Aggregate und NAS-Daten-LIFs von node2 auf die aktualisierte Node1 verschoben und Sie überprüfen, ob die SAN-LIFs auf node1 vorhanden sind. Gesamteigentum am Ende von Stufe 3: • Aktualisierter node1 ist der Haupteigentümer und aktueller Besitzer von node1-Aggregaten • Node2 ist der Hausbesitzer und der aktuelle Besitzer von node2 Aggregaten

Stufe	Schritte
"Phase 4: Ressourcen verlagern und Knoten zurücknehmen 2"	Während Phase 4 verschieben Sie Aggregate und NAS-Daten-LIFs von Knoten 2 auf die aktualisierte Knoten 1 und Mustern Knoten 2 aus. Gesamteigentum am Ende von Stufe 4: • Der aktualisierte Knoten 1 ist der Hausbesitzer und der aktuelle Besitzer von Aggregaten, die ursprünglich zu node1 gehörten • Der aktualisierte Knoten 1 ist der aktuelle Besitzer von node2 Aggregaten
"Stufe 5: Installieren Sie die Ersatz-Systemmodule auf Knoten 2"	In Phase 5 installieren Sie die neuen Systemmodule, die Sie für den aktualisierten Knoten 2 erhalten haben, und dann Netboot Knoten 2. Gesamteigentum am Ende von Stufe 5: • Der aktualisierte Node1 ist der Hausbesitzer und der aktuelle Besitzer der Aggregate, die ursprünglich zu node1 gehörten. • Upgrade node2 ist der Hausbesitzer und der aktuelle Besitzer von Aggregaten, die ursprünglich zu node2 gehörten.
"Stufe 6: Starten Sie Node2 mit den Ersatz-Systemmodulen"	In Phase 6 starten Sie Knoten 2 mit aktualisierten Systemmodulen und überprüfen die aktualisierte Installation von Knoten 2. Wenn Sie NVE verwenden, stellen Sie die Konfiguration für Schlüsselmanager wieder her. Außerdem werden node1-Aggregate und NAS-Daten-LIFs von node1 auf die aktualisierte Node2 verschoben und Sie überprüfen, ob die SAN-LIFs auf node2 vorhanden sind.
"Phase 7: Das Upgrade abschließen"	In Phase 7 bestätigen Sie, dass die neuen Nodes korrekt eingerichtet wurden. Und wenn die neuen Nodes verschlüsselt sind, konfigurieren und einrichten Sie Storage Encryption oder NVE. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Stufe 1: Upgrade vorbereiten

Überblick

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

Schritte

1. "Überprüfen Sie die Upgrade-Hardware"
2. "Bereiten Sie die Knoten für ein Upgrade vor"

3. "Managen Sie die Storage-Verschlüsselung mit dem Onboard Key Manager"

Überprüfen Sie die Upgrade-Hardware

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

Wenn Sie ein Upgrade …	Sie müssen haben …
AFF A220 als ASA auf ASA A150 konfiguriert	Zwei Controller-Module
AFF A220, AFF A200 oder AFF C190 auf AFF A150	Zwei Controller-Module
FAS2720 oder FAS2720 zu FAS2720	Zwei Controller-Module
AFF A700 als ASA zu ASA A900 konfiguriert	Zwei Controller und zwei NVRAM-Module
AFF A700 AUF AFF A900	Zwei Controller und zwei NVRAM-Module
FAS9000 auf FAS9500 Systeme	Zwei Controller und zwei NVRAM-Module

Bereiten Sie die Knoten für ein Upgrade vor

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

Schritte

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

   ```
   service-processor show
   ```

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

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

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

   ```
   set -privilege advanced
   ```

`system controller replace start -nodes node_names`

Sie werden eine Ausgabe wie die folgende sehen:

```
Warning:
1. Current ONTAP version is 9.x

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   > FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
   >
   > SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

   "Weitere Informationen zu unterstützten Self-Encrypting Drives".

Korrigieren Sie die Aggregateigentümer bei Ausfall einer ARL-Vorabprüfung

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

Schritte

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

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

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

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

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

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

4 entries were displayed.
```

Nachdem Sie fertig sind

Sie müssen den Controller-Ersatzprozess neu starten:

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

Lizenz

Jeder Knoten im Cluster muss über eine eigene NetApp-Lizenzdatei (NLF) verfügen.

Wenn Sie nicht über eine Lizenzdatei verfügen, stehen dem neuen Controller derzeit lizenzierte Funktionen im Cluster zur Verfügung. Wenn Sie jedoch nicht lizenzierte Funktionen auf dem Controller verwenden, unterläuft dies möglicherweise die Einhaltung Ihrer Lizenzvereinbarung. Daher sollten Sie nach Abschluss des Upgrades die Lizenzdatei für den neuen Controller installieren.

Siehe "Quellen" Um eine Verknüpfung zur *NetApp Support-Website* zu erstellen, auf der Sie Ihre Lizenzdatei erhalten können. Die NLFs sind im Abschnitt *My Support* unter *Softwarelizenzen* verfügbar. Wenn der Standort nicht über die benötigten NLFs verfügt, wenden Sie sich an Ihren NetApp Ansprechpartner.

Ausführliche Informationen zur Lizenzierung finden Sie unter "Quellen" Verknüpfen mit der Referenz *Systemadministration*.

Management der Storage-Verschlüsselung mit dem Onboard Key Manager

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

Schritte

1. Notieren Sie die Cluster-weite Passphrase.

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

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

Stilllegen der SnapMirror Beziehungen (optional)

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

Schritte

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

   ```
   snapmirror show
   ```

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

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

2. Alle Beziehungen zwischen dem Cluster stilllegen:

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

Phase 2. Verschieben von Ressourcen und Ausmustern von Knoten1

Überblick

Während Phase 2 werden node1-Aggregate und NAS-Daten-LIFs in Knoten 2 verschoben. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Bei Bedarf verschieben Sie fehlerhafte oder Vetos Aggregate. Sie zeichnen auch node1-Informationen für die spätere Verwendung im Verfahren auf und tauschen dann die entsprechenden node1-Systemmodule aus, entfernen node1 und starten den aktualisierten node1.

Schritte

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

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

Bevor Sie Node1 durch die Ersatzmodule für Ihr System-Upgrade ersetzen können, müssen Sie die nicht-Root-Aggregate und NAS-Daten-LIFs von Node1 zu Node2 verschieben, bevor Sie die node1-Ressourcen auf Node1, der auf dem Ersatzsystem ausgeführt wird, wieder wiederherstellen können. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können.

Bevor Sie beginnen

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

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Sie müssen während des Upgrades keine SAN-LIFs für den Cluster- oder Systemzustand verschieben. Sie müssen überprüfen, ob die LIFs in gutem Zustand und an den entsprechenden Ports angeschlossen sind, nachdem Sie node1 als Ersatzsystem online geschaltet haben.

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

Schritte

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

   ```
   system controller replace resume
   ```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Verschiebung ausgefallener oder Vetos von Aggregaten

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

Über diese Aufgabe

Der Umzugsvorgang wird aufgrund des Fehlers angehalten.

Schritte

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

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr_name -ndo-controller-upgrade true
```

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

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

Node1 ausmustern

Um node1 auszumustern, setzen Sie den automatisierten Vorgang fort, um das HA-Paar mit node2 zu deaktivieren und node1 ordnungsgemäß herunterzufahren.

Schritte

1. Vorgang fortsetzen:

   ```
   system controller replace resume
   ```

2. Vergewissern Sie sich, dass node1 angehalten wurde:

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

   Nachdem node1 vollständig angehalten wurde, sollte node1 an DER LOADER>-Eingabeaufforderung sein. Um die LOADER>-Eingabeaufforderung anzuzeigen, stellen Sie eine Verbindung mit der seriellen Konsole von node1 her.

Ersetzen Sie die node1-Systemmodule

Ersetzen Sie die node1-Systemmodule für Ihre Upgrade-Konfiguration:

- Austausch des Controller-Moduls AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720

  Mit diesem Verfahren können Sie auch einen AFF A220 ersetzen, der als ASA konfiguriert ist.

- Ersetzen Sie den AFF A700- oder FAS9000-Controller und die NVRAM-Module

  Mit diesem Verfahren können Sie auch eine als ASA konfigurierte AFF A700 ersetzen.

Austausch des Controller-Moduls AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720

An dieser Stelle ist node1 ausgefallen und alle Daten werden von node2 bereitgestellt. Da sich Node1 und Node2 im gleichen Chassis befinden und durch denselben Satz an Netzteilen mit Strom versorgt werden, schalten Sie das Chassis NICHT aus. Sie müssen darauf achten, nur das Knoten 1-Controller-Modul zu entfernen. Normalerweise ist node1 Controller A, der sich auf der linken Seite des Chassis befindet, wenn man sich die Controller von der Rückseite des Systems ansieht. Das Controller-Etikett befindet sich direkt über dem Controller-Modul auf dem Chassis.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Entfernen Sie das Controller-Modul AFF A220, AFF A200, AFF C190, FAS2720 oder FAS2720

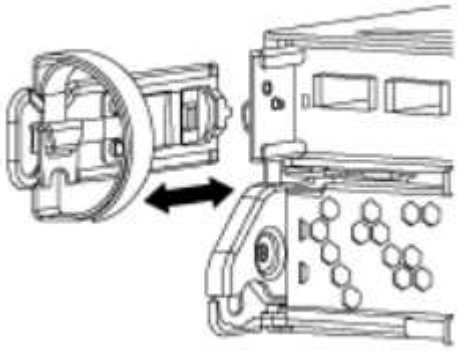
Um auf Komponenten innerhalb des Controllers zuzugreifen, müssen Sie zuerst das Controller-Modul aus dem System entfernen und dann die Abdeckung am Controller-Modul entfernen.

Schritte

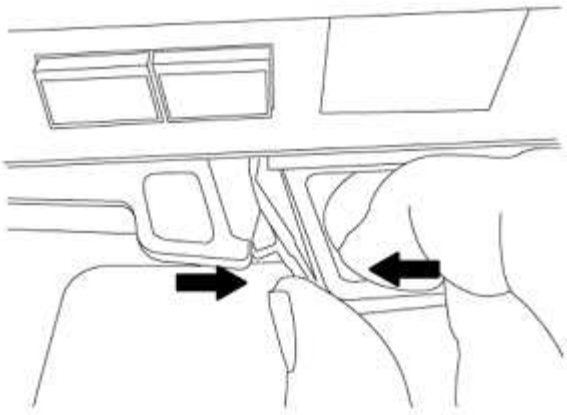
1. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel am Kabelführungsgerät befestigt sind, und ziehen Sie dann die Systemkabel und SFPs (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.

   Lassen Sie die Kabel im Kabelverwaltungs-Gerät so, dass bei der Neuinstallation des Kabelverwaltungsgeräts die Kabel organisiert sind.

2. Entfernen Sie die Kabelführungsgeräte von der linken und rechten Seite des Controller-Moduls und stellen Sie sie zur Seite.



3. Drücken Sie die Verriegelung am Nockengriff, bis sie loslässt, öffnen Sie den Nockengriff vollständig, um das Controller-Modul aus der Mittelplatine zu lösen, und ziehen Sie das Controller-Modul anschließend mit zwei Händen aus dem Gehäuse heraus.



4. Drehen Sie das Controller-Modul um und legen Sie es auf eine flache, stabile Oberfläche.

Installieren Sie das Controller-Modul ASA A150, AFF A150 oder FAS2820

Gehen Sie wie folgt vor, um das Controller-Modul ASA A150, AFF A150 oder FAS2820 in Knoten1 zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   > Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

   > Da das Gehäuse bereits eingeschaltet ist, startet node1 die BIOS-Initialisierung und dann Autoboot, sobald es vollständig eingesetzt ist. Um den node1-Boot zu unterbrechen, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird, wird empfohlen, die serielle Konsole und die Verwaltungskabel mit dem node1-Controller-Modul zu verbinden.

3. Schieben Sie das Steuermodul bei geöffnetem Nockengriff fest hinein, bis es auf die Mittelplatine trifft und vollständig eingesetzt ist. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Schließen Sie den Nockengriff in die verriegelte Position.

   > Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DIE AUTOBOOT-Funktion unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten. Wenn Sie DAS AUTOBOOT nicht rechtzeitig unterbrechen und node1 startet, warten Sie auf die Eingabeaufforderung und drücken Sie **Strg-C**, um in das Boot-Menü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, können Sie den Node mit Option 8 neu booten und DEN AUTOBOOT während des Neubootens unterbrechen.
6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

```
set-defaults
```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

```
saveenv
```

Ersetzen Sie den AFF A700- oder FAS9000-Controller und die NVRAM-Module

An dieser Stelle ist node1 ausgefallen und alle Daten werden von node2 bereitgestellt. Da sich Node1 und Node2 im gleichen Chassis befinden und durch denselben Satz an Netzteilen mit Strom versorgt werden, schalten Sie das Chassis NICHT aus. Achten Sie darauf, nur das Node1-Controller-Modul und das node1-NVRAM-Modul zu entfernen. Normalerweise ist node1 Controller A, der sich auf der linken Seite des Chassis befindet, wenn man sich die Controller von der Rückseite des Systems ansieht. Das Controller-Etikett befindet sich direkt über dem Controller-Modul auf dem Chassis.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

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

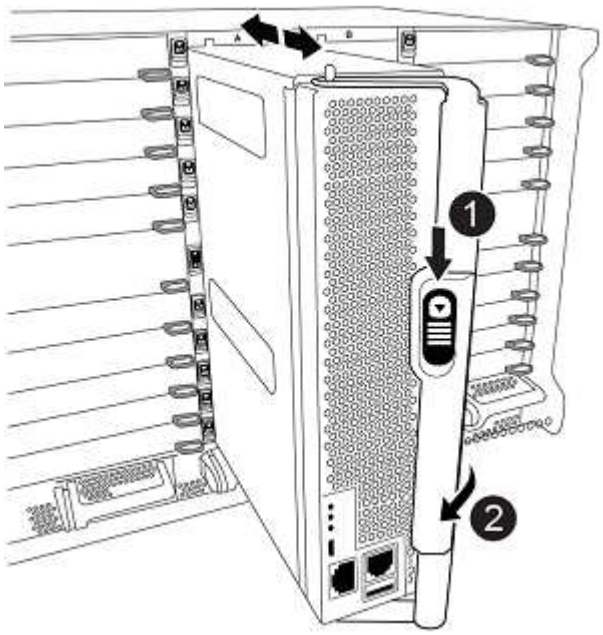
Schritte

1. Trennen Sie ggf. das Konsolenkabel und das Managementkabel aus dem node1-Controller-Modul, bevor Sie das Controller-Modul aus node1 entfernen.

> Wenn Sie an node1 arbeiten, entfernen Sie nur die Konsole und E0M-Kabel von node1. Sie dürfen während dieses Vorgangs keine anderen Kabel oder Anschlüsse an node1 oder node2 entfernen oder austauschen.

2. Entriegeln und entfernen Sie das Controller-Modul A aus dem Gehäuse.

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



❶	Freigabetaste für den CAM-Griff
❷	CAM-Griff

a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse.

   Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder FAS9000 NVRAM-Modul

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

> Das AFF A700 oder FAS9000 NVRAM-Modul befindet sich in Steckplatz 6 und hat die doppelte Höhe der anderen Module im System.

Schritte

1. Entriegeln und entfernen Sie das NVRAM-Modul aus Steckplatz 6 der Node1.

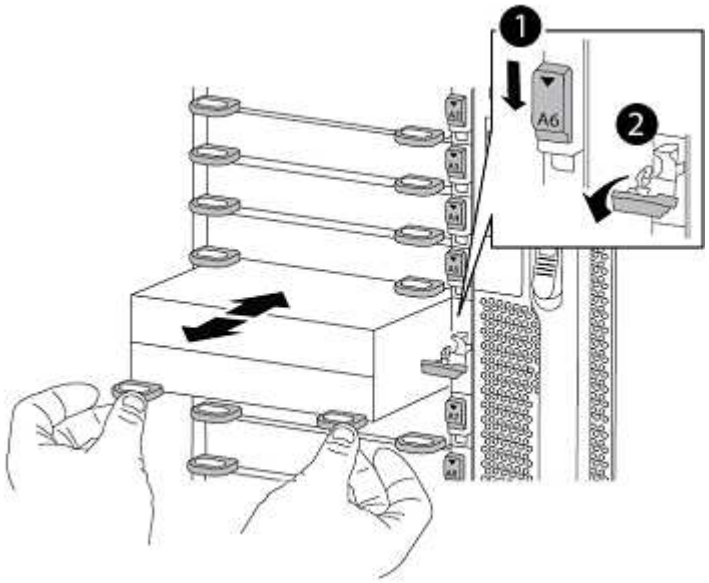
   a. Drücken Sie die Taste mit der Nummerierung und dem Buchstaben.

      Die Nockentaste bewegt sich vom Gehäuse weg.

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

      Das NVRAM-Modul geht aus dem Chassis aus und verschiebt ein paar Zentimeter.

   c. Entfernen Sie das NVRAM-Modul aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



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

Installieren Sie die NVRAM- und Controller-Module ASA A900, AFF A900 oder FAS9500

Installieren Sie die ASA A900, AFF A900 oder FAS9500 NVRAM- und Controller-Module, die Sie für das Upgrade auf Knoten1 erhalten haben.

Bei der Installation müssen Sie Folgendes beachten:

- Verschieben Sie alle Leereinfüllmodule in den Steckplätzen 6-1 und 6-2 vom alten NVRAM-Modul in das neue NVRAM-Modul.
- Verschieben Sie das coredump-Gerät NICHT aus dem AFF A700 NVRAM-Modul in das ASA A900- oder AFF A900 NVRAM-Modul.
- Verschieben Sie alle Flash Cache Module, die im FAS9000 NVRAM-Modul installiert sind, auf das FAS9500 NVRAM-Modul.

Bevor Sie beginnen

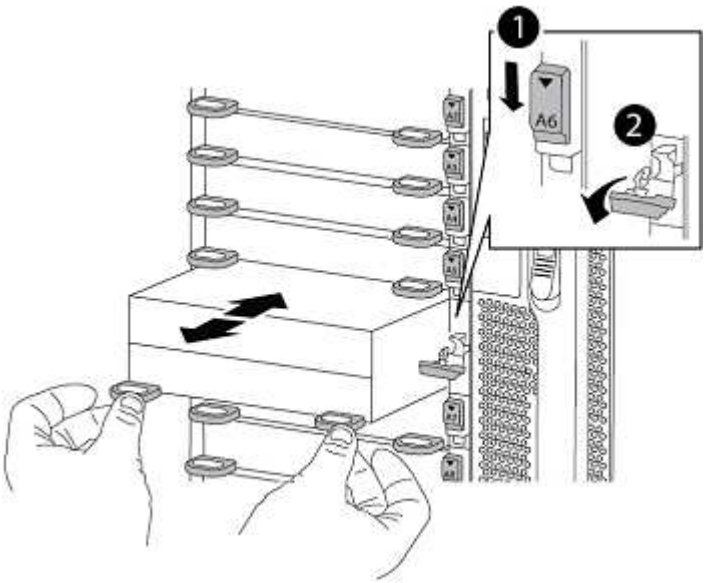
Wenn du nicht bereits geerdet bist, beground dich richtig.

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500

Gehen Sie wie folgt vor, um das NVRAM-Modul ASA A900, AFF A900 oder FAS9500 in Steckplatz 6 von Knoten1 zu installieren.

Schritte

1. Richten Sie das NVRAM-Modul an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie das NVRAM-Modul vorsichtig in den Steckplatz, bis der vorletzte und nummerierte E/A-Nockenriegel mit dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVRAM-Moduls.



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

Installieren Sie das Controller-Modul ASA A900, AFF A900 oder FAS9500 auf Knoten1.

Gehen Sie wie folgt vor, um das Controller-Modul ASA A900, AFA A900 oder FAS9500 in Knoten1 zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung A im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu aufgefordert werden.

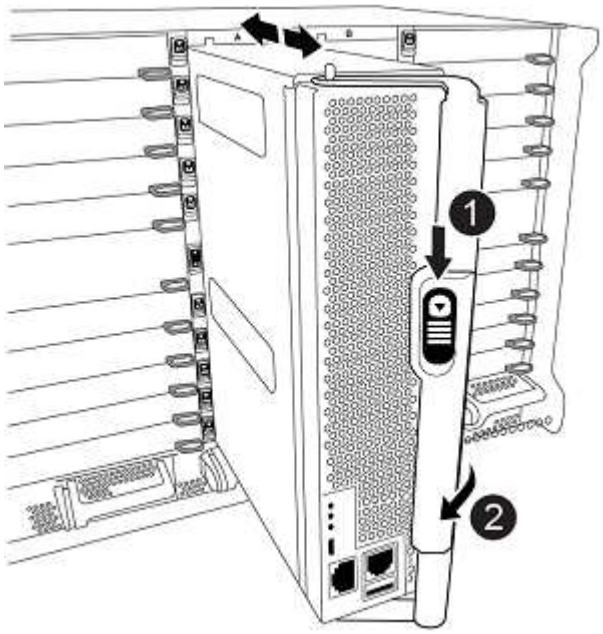
2. Verkabeln Sie die Management- und Konsolen-Ports mit dem Node1-Controller-Modul.

   Da das Gehäuse bereits eingeschaltet ist, startet node1 die BIOS-Initialisierung und dann Autoboot, sobald es vollständig eingesetzt ist. Um den node1-Boot zu unterbrechen, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird, wird empfohlen, die serielle Konsole und die Verwaltungskabel mit dem node1-Controller-Modul zu verbinden.

3. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt.

   Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.



❶	Verriegelungsverschluss am CAM-Griff
❷	Nockengriff in der nicht entriegeln Position

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DIE AUTOBOOT-Funktion unterbrochen haben, wird node1 an der LOADER-Eingabeaufforderung angehalten. Wenn SIE DIE AUTOBOOT-Zeit nicht unterbrechen und node1 den Startvorgang startet, warten Sie auf die Eingabeaufforderung und drücken Sie **Strg-C**, um in das Startmenü zu gelangen. Nachdem der Knoten im Startmenü angehalten wurde, verwenden Sie die Option `8` Um den Node neu zu booten und den AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung „LOADER> von node1“ die Standardvariablen für die Umgebung fest:

   ```
   set-defaults
   ```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

   ```
   saveenv
   ```

Netzboot Nr. 1

Nach dem Austausch der entsprechenden Ersatz-Systemmodule müssen Sie netboot node1. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf Netzboot fügen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver hinzu, auf den das System zugreifen kann.

Es ist nicht möglich, die auf dem Boot-Medium des Ersatz-Controller-Moduls installierte ONTAP-Version zu überprüfen, es sei denn, sie ist in einem Gehäuse installiert und eingeschaltet. Die ONTAP-Version auf dem Ersatz-System-Startmedium muss mit der ONTAP-Version auf dem alten System übereinstimmen, das Sie aktualisieren, und sowohl das primäre als auch das Backup-Startabbild müssen übereinstimmen. Informationen zur Überprüfung der unterstützten ONTAP-Mindestversion für Ihr Upgrade finden Sie unter "Überblick".

Sie können die Images konfigurieren, indem Sie einen Netzboot gefolgt vom ausführen `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

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

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Laden Sie die für Ihr System erforderlichen Systemdateien und die korrekte Version von ONTAP von *NetApp Support Site* herunter. Siehe "Quellen" Link zur NetApp Support Site_.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert ist. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Siehe "Quellen" Um eine Verknüpfung zur NetApp Support Site_ zu erhalten, um die Dateien zum Ausführen des Netzboots des Systems herunterzuladen.
2. Laden Sie die entsprechende ONTAP Software aus dem Bereich zum Software Download der *NetApp Support Site* herunter und speichern Sie die `<ontap_version>_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.
4. Ihre Verzeichnisliste sollte enthalten `<ontap_version>_image.tgz`.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie müssen den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

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

6. Ausführen des Netzboots auf Knoten 1:

```
netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel
```

> Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis node1 jetzt auf dem Controller-Modul ASA A900, AFF A900 oder FAS9500 ausgeführt wird, um die Boot-Menüoptionen wie unten gezeigt zu starten und anzuzeigen:

```
Please choose one of the following:

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

8. Wählen Sie im Startmenü Option `(7) Install new software first.`

   Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

   Ignorieren Sie die folgende Meldung:

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

   Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades.

   > Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

9. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:
   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:

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

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

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

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

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

11. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium:

a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`:

```
This will delete critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken
over.
Are you sure you want to continue?:
```

b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.

12. Wählen Sie die Option `5` Wechseln Sie vom Boot-Menü zum Wartungsmodus. Antwort `yes` Zu den Aufforderungen, bis der Node im Wartungsmodus und mit der Eingabeaufforderung angehalten wird `*>`.

13. Vergewissern Sie sich, dass Controller und Chassis als konfiguriert sind `ha`:

```
ha-config show
```

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

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

14. Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

```
ha-config modify controller ha

ha-config modify chassis ha
```

15. Überprüfen Sie die `ha-config` Einstellungen:

```
ha-config show
```

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

16. Stopp-Nr. 1:

    ```
    halt
    ```

    Node1 sollte an der LOADER-Eingabeaufforderung angehalten werden.

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

    ```
    date
    ```

18. Überprüfen Sie bei node1 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show date
    ```

19. Legen Sie bei Bedarf das Datum auf Knoten 1 fest:

    `set date mm/dd/yyyy`

    ⓘ Legen Sie das entsprechende UTC-Datum auf Knoten 1 fest.

20. Überprüfen Sie bei node1 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show time
    ```

21. Stellen Sie bei Bedarf die Zeit auf node1 ein:

    `set time hh:mm:ss`

    ⓘ Legen Sie die entsprechende UTC-Zeit auf node1 fest.

22. Legen Sie die Partner-System-ID auf node1 fest:

    `setenv partner-sysid node2_sysid`

    Für node1, die `partner-sysid` Muss der von node2 sein. Sie können die System-ID node2 vom beziehen `node show -node node2` Befehlsausgabe auf node2.

    a. Einstellungen speichern:

    ```
    saveenv
    ```

23. Überprüfen Sie bei node1 an der LOADER-Eingabeaufforderung den `partner-sysid` Für Knoten 1:

    ```
    printenv partner-sysid
    ```

Phase 3: Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Überblick

In Phase 3 starten Sie node1 mit aktualisierten Systemmodulen und überprüfen die aktualisierte node1-Installation. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1 Aggregate und NAS-Daten-LIFs von node2 auf die aktualisierte Node1 verschoben und Sie überprüfen, ob die SAN-LIFs auf node1 vorhanden sind.

Schritte

1. "Starten Sie Knoten 1 mit den Ersatz-Systemmodulen"
2. "Überprüfen Sie die Installation node1"
3. "Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her"
4. "Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1"

Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Node1 mit den Ersatzmodulen ist nun startbereit. In diesem Abschnitt werden die Schritte beschrieben, die zum Starten von Knoten 1 mit den Ersatzmodulen für die folgenden Upgrade-Konfigurationen erforderlich sind:

Alter Knoten 1-Controller	Ersatz-Knoten 1-Systemmodule
AFF A220 als ASA konfiguriert	AFF A150-Controller-Modul [1]
AFF A220 AFF A200 AFF C 190	AFF A150-Controller-Modul [1]
FAS2620 FAS2720	FAS2820 Controller-Modul [1]
AFF A700 – als ASA konfiguriert	ASA A900-Controller und NVRAM-Module [2]
AFF A700	AFF A900-Controller und NVRAM-Module [2]
FAS9000	FAS9500 Controller- und NVRAM-Module [2]

[1] beim Austausch von Controller-Modulen verschieben Sie alle Verbindungen vom alten zum Ersatz-Controller-Modul.
[2] beim Austauschen des Controllers und der NVRAM-Module verschieben Sie nur die Konsole und die Managementverbindungen.

Schritte

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

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

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

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

> FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

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

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

2. Starten Sie den Knoten im Startmenü:

```
boot_ontap menu
```

3. Weisen Sie die alten node1-Festplatten dem Ersatznode1 neu zu, indem Sie „22/7“ eingeben und die versteckte Option auswählen `boot_after_controller_replacement` Wenn der Node im Boot-Menü angehalten wird.

   Nach einer kurzen Verzögerung werden Sie aufgefordert, den Namen des Node einzugeben, der ersetzt wird. Wenn gemeinsam genutzte Festplatten vorhanden sind (auch Advanced Disk Partitioning (ADP) oder partitionierte Festplatten), werden Sie aufgefordert, den Node-Namen des HA-Partners einzugeben.

   Diese Eingabeaufforderungen sind möglicherweise in den Konsolenmeldungen verborgen. Wenn Sie keinen Node-Namen eingeben oder einen falschen Namen eingeben, werden Sie aufgefordert, den Namen erneut einzugeben.

Wenn `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` Und oder `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` Fehler auftreten, führen Sie die folgenden Schritte aus:

a. Halten Sie den Node an der LOADER-Eingabeaufforderung an.
b. Prüfen und setzen Sie die Storage Encryption Boot-Optionen zurück, die in erwähnt sind Schritt 1.
c. An der Loader-Eingabeaufforderung booten Sie:

```
boot_ontap
```

Das folgende Beispiel kann als Referenz verwendet werden:

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
.
<output truncated>
.
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

Please choose one of the following:

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

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

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

Die im vorhergehenden Beispiel gezeigten System-IDs sind Beispiel-IDs. Die tatsächlichen System-IDs der Nodes, die Sie aktualisieren, unterscheiden sich.

Zwischen der Eingabe von Node-Namen an der Eingabeaufforderung und der Eingabeaufforderung für die Anmeldung wird der Node mehrmals neu gebootet, um die Umgebungsvariablen wiederherzustellen, die Firmware auf den im System verwendeten Karten zu aktualisieren und für andere ONTAP Updates zu sorgen.

Überprüfen Sie die Installation node1

Sie müssen die Installation von node1 mit den Ersatz-Systemmodulen überprüfen. Da keine Änderung an physischen Ports vorgenommen wird, sind Sie nicht verpflichtet, die physischen Ports von der alten Knoten1 auf den Ersatz-Knoten1 zuzuordnen.

Über diese Aufgabe

Nachdem Sie node1 mit dem Ersatz-Controller-Modul gestartet haben, überprüfen Sie, ob es richtig installiert ist. Sie müssen warten, bis node1 dem Quorum beitreten und dann den Controller-Ersatzvorgang fortsetzen.

An diesem Punkt in der Prozedur sollte der Upgrade-Vorgang des Controllers angehalten sein, da node1 versucht hat, Quorum automatisch beizutreten.

Schritte

1. Vergewissern Sie sich, dass node1 dem Quorum beigetreten ist:

   ```
   cluster show -node node1 -fields health
   ```

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

2. Vergewissern Sie sich, dass node1 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Wechseln in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

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

   ```
   system controller replace show
   ```

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

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Controller-Ersatzvorgang hält für Eingriffe mit der folgenden Meldung an:

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

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


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

In diesem Verfahren wurde Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node1_ umbenannt.

7. Wenn sich der Controller-Austausch im Status „Pause“ befindet, fahren Sie mit fort Stellen Sie die Netzwerkkonfiguration auf node1 wieder her.

Stellen Sie die Netzwerkkonfiguration auf node1 wieder her

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

Über diese Aufgabe

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

Schritte

1. Listen Sie alle physischen Ports auf, die auf Upgrade-Knoten1 stehen:

```
network port show -node node1
```

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

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node1 auflisten:

```
network port reachability show -node node1
```

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ------------------------------------
---------------------
Node1
          a0a      Default:Default                      ok
          a0a-822  Default:822                          ok
          a0a-823  Default:823                          ok
          e0M      Default:Mgmt                         ok
          e11a     -                                    no-reachability
          e11b     -                                    no-reachability
          e11c     -                                    no-reachability
          e11d     -                                    no-reachability
          e3a      -                                    no-reachability
          e3b      -                                    no-reachability
          e4a      Cluster:Cluster                      ok
          e4e      Cluster:Cluster                      ok
          e5a      -                                    no-reachability
          e7a      -                                    no-reachability
          e9a      Default:Default                      ok
          e9a-822  Default:822                          ok
          e9a-823  Default:823                          ok
          e9b      Default:Default                      ok
          e9b-822  Default:822                          ok
          e9b-823  Default:823                          ok
          e9c      Default:Default                      ok
          e9d      Default:Default                      ok
22 entries were displayed.
```

Im vorherigen Beispiel wurde node1 nach dem Austausch des Controllers gebootet. Einige Ports verfügen nicht über Reachability, da es keine physische Verbindung gibt. Sie müssen alle Ports mit einem anderen Status als für die Erreichbarkeit reparieren `ok`.

> Während des Upgrades sollten sich die Netzwerkports und ihre Konnektivität nicht ändern. Alle Ports sollten sich in den richtigen Broadcast-Domänen befinden, und die Erreichbarkeit des Netzwerkports sollte sich nicht ändern. Bevor Sie jedoch LIFs von node2 zurück auf node1 verschieben, müssen Sie die Erreichbarkeit und den Integritätsstatus der Netzwerk-Ports überprüfen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node1 mit einem anderen Status als der Erreichbarkeit `ok` Mit dem folgenden Befehl in der folgenden Reihenfolge:

   `network port reachability repair -node` *`node_name`* `-port` *`port_name`*

a. Physische Ports
b. VLAN-Ports

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node1 -port e11b
```

```
Warning: Repairing port "node1:e11b" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Eine Warnmeldung, wie im vorhergehenden Beispiel dargestellt, wird für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Erreichbarkeit der Broadcast-Domäne unterscheiden können, in der sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

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

```
network port reachability show
```

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

5. Überprüfen der Port-Erreichbarkeit:

```
network port reachability show
```

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

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

```
network port show
```

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

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

8. Stellen Sie die LIF-Home-Ports wieder her und geben Sie ggf. den Vserver und die LIF-Home-Ports an, die Sie mit folgenden Schritten wiederherstellen müssen:
   a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

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

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

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

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

Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her

Wenn Sie NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) zur Verschlüsselung von Volumes auf dem System verwenden, das Sie aktualisieren, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht neu synchronisieren, wenn Sie die node1-Aggregate mithilfe von ARL von node2 zur aktualisierten node1 verschieben, können Ausfälle auftreten, da node1 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

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

Schritte

1. Führen Sie den folgenden Befehl aus node1:

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

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node1 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node1 -fields restored -key
-type SVM-KEK
```

Beispiel

```
::> security key-manager key query -node node1 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node1    svm1      ""           00000000000000000200000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1

Nachdem Sie die Netzwerkkonfiguration auf Knoten 1 überprüft und bevor Sie Aggregate von Knoten 2 zu Knoten 1 verschieben, überprüfen Sie, ob die NAS-Daten-LIFs, die zu Knoten 1 gehören, die sich derzeit auf Knoten 2 befinden, von Knoten 2 zu Knoten 1 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN LIFs auf Knoten1 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Nachdem Sie node1 in den Online-Modus versetzt haben, müssen Sie überprüfen, ob sich die LIFs in einem ordnungsgemäßen Zustand und auf den entsprechenden Ports befinden.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

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

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

2. Durchführen einer Prüfung der Netzwerkfähigkeit:

   ```
   network port reachability show -node node1
   ```

Vergewissern Sie sich, dass alle verbundenen Ports, einschließlich der Schnittstellengruppe und VLAN-Ports, ihren Status als anzeigen `OK`.

3. 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, in die neue Knoten1.

   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 node1 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. Verschieben von Ressourcen und Ausmustern von Knoten2

Überblick

Während Phase 4 verschieben Sie Aggregate und NAS-Daten-LIFs von Knoten 2 auf die aktualisierte Knoten 1 und Mustern Knoten 2 aus.

Schritte

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

Verschieben von Aggregaten ohne Root-Wurzeln und NAS-Daten-LIFs von Knoten 2 auf Knoten 1

Bevor Sie Knoten 2 durch das Ersatz-Systemmodul ersetzen können, müssen Sie zunächst die nicht-Root-Aggregate, die im Besitz von Knoten 2 sind, in Knoten 1 verschieben.

Bevor Sie beginnen

Nach den Nachprüfungen aus der vorherigen Phase wird automatisch die Ressourcenfreigabe für node2 gestartet. Die Aggregate außerhalb des Root-Bereichs und LIFs für nicht-SAN-Daten werden von node2 in die neue Knoten1 migriert.

Über diese Aufgabe

Nach der Migration der Aggregate und LIFs wird der Vorgang zu Verifizierungszwecken angehalten. An dieser Phase müssen Sie überprüfen, ob alle Aggregate ohne Root-Root-Daten und LIFs außerhalb des SAN in die neue Knoten1 migriert werden.

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

Schritte

1. Vergewissern Sie sich, dass alle nicht-Root-Aggregate online sind und ihren Status auf node1:

   ```
   storage aggregate show -node node1 -state online -root false
   ```

   Das folgende Beispiel zeigt, dass die nicht-Root-Aggregate auf node1 online sind:

```
cluster::> storage aggregate show -node node1 state online -root false

Aggregate     Size        Available   Used%   State   #Vols  Nodes
RAID     Status
----------    ---------   ---------   ------  -----   -----  ------
-------  ------
aggr_1        744.9GB     744.8GB     0%      online      5  node1
raid_dp  normal
aggr_2        825.0GB     825.0GB     0%      online      1  node1
raid_dp  normal
2 entries were displayed.
```

Wenn die Aggregate offline gegangen sind oder in node1 fremd geworden sind, stellen Sie sie mit dem folgenden Befehl auf der neuen node1, einmal für jedes Aggregat online:

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

2. Überprüfen Sie, ob alle Volumes auf node1 online sind, indem Sie den folgenden Befehl auf node1 verwenden und seine Ausgabe überprüfen:

   ```
   volume show -node node1 -state offline
   ```

   Wenn ein Volume auf node1 offline ist, stellen Sie sie mit dem folgenden Befehl auf node1 für jedes Volume online:

   ```
   volume online -vserver vserver-name -volume volume-name
   ```

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

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

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

4. Überprüfen Sie, ob auf node2 keine Daten-LIFs mehr vorhanden sind, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

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

Node2 ausmustern

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

Schritte

1. Vorgang fortsetzen:

```
system controller replace resume
```

Der Knoten wird automatisch angehalten.

Nachdem Sie fertig sind

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

Phase 5. Installieren Sie die Ersatz-Systemmodule auf Knoten 2

Überblick

In Phase 5 installieren Sie die neuen Systemmodule, die Sie für den aktualisierten Knoten 2 erhalten haben, und dann Netboot Knoten 2.

Schritte

1. "Installieren Sie die Ersatz-Systemmodule auf Knoten 2"
2. "Netzboot Nr. 2"

Installieren Sie die Ersatz-Systemmodule auf Knoten 2

Installieren Sie die Ersatz-Systemmodule, die Sie für das Upgrade auf Knoten 2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

- Installieren Sie das ASA A150, AFF A150 oder FAS2820 Controller-Modul auf Knoten2
- Installieren Sie ASA A900, AFF A900 oder FAS9500 NVRAM und Controller-Module auf Knoten2

Installieren Sie das Controller-Modul ASA A150, AFF A150 oder FAS2820 auf der Knoten2

Installieren Sie das ASA A150, AFF A150 oder FAS2820 Controller-Modul, das Sie für das Upgrade auf Knoten2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

Bevor Sie beginnen

- Wenn du nicht bereits geerdet bist, beground dich richtig.
- Trennen Sie alle Kabel, einschließlich Konsole, Management, SAS Storage und Datennetzwerkkabel, vom entfernten Controller.

Schritte

1. Richten Sie das Ende des Controller-Moduls an Schacht B im Chassis aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Bay B befindet sich auf dem Chassis unten.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu später beim Verfahren aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem node2-Controller-Modul.

> Da das Chassis bereits eingeschaltet ist, startet node2, sobald es vollständig eingesetzt ist. Um das Booten von node2 zu vermeiden, empfiehlt NetApp, die Konsole und die Managementkabel an das node2-Controller-Modul anzuschließen, bevor Sie das Controller-Modul vollständig in den Steckplatz einsetzen.

3. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt.

   Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist.

> Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DEN AUTOBOOT unterbrochen haben, wird node2 an der LOADER-Eingabeaufforderung angehalten. Wenn SIE DIE AUTOBOOT-Zeit nicht unterbrechen und node2 den Startvorgang startet, warten Sie auf die Eingabeaufforderung und drücken Sie **Strg-C**, um in das Startmenü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, können Sie den Node mit Option 8 neu booten und DEN AUTOBOOT während des Neubootens unterbrechen.

Installieren Sie ASA A900, AFF A900 oder FAS9500 NVRAM und Controller-Module auf Knoten2

Installieren Sie die ASA A900, AFF A900 oder FAS9500 NVRAM- und Controller-Module, die Sie für das Upgrade auf Node2 erhalten haben. Node2 ist Controller B auf der rechten Seite des Chassis, wenn man sich die Controller von der Rückseite des Systems ansieht.

Bei der Installation müssen Sie Folgendes beachten:

- Verschieben Sie alle Leereinfüllmodule in den Steckplätzen 6-1 und 6-2 vom alten NVRAM-Modul in das neue NVRAM-Modul.
- Verschieben Sie das coredump-Gerät NICHT aus dem AFF A700 NVRAM-Modul in das ASA A900- oder AFF A900 NVRAM-Modul.
- Verschieben Sie alle Flash Cache Module, die im FAS9000 NVRAM-Modul installiert sind, auf das FAS9500 NVRAM-Modul.

Bevor Sie beginnen

Wenn du nicht bereits geerdet bist, beground dich richtig.

Installieren Sie das NVRAM-Modul ASA A900, AFF A900 oder FAS9500

Gehen Sie wie folgt vor, um das NVRAM-Modul ASA A900, AFF A900 oder FAS9500 in Steckplatz 6 von Knoten2 zu installieren.

Schritte

1. Richten Sie das NVRAM-Modul an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie das NVRAM-Modul vorsichtig in den Steckplatz, bis der vorletzte und nummerierte E/A-Nockenriegel mit dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVRAM-Moduls.

Installieren Sie das Controller-Modul ASA A900, AFF A900 oder FAS9500 in Knoten2

Gehen Sie wie folgt vor, um das Controller-Modul ASA A900, AFF A900 oder FAS9500 in Knoten2 zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an Schacht B im Chassis aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

   Das Bay-Etikett befindet sich auf dem Chassis direkt über dem Controller-Modul.

   Setzen Sie das Controller-Modul erst dann vollständig in das Chassis ein, wenn Sie dazu später beim Verfahren aufgefordert werden.

2. Verkabeln Sie die Management- und Konsolen-Ports mit dem node2-Controller-Modul.

   Da das Chassis bereits eingeschaltet ist, startet node2, sobald es vollständig eingesetzt ist. Um das Booten von node2 zu vermeiden, wird empfohlen, die Konsole und die Managementkabel mit dem node2-Controller-Modul zu verbinden, bevor das Controller-Modul vollständig in den Steckplatz eingesetzt wird.

3. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt.

   Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist.

   Um Schäden an den Anschlüssen zu vermeiden, sollten Sie beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden.

4. Schließen Sie die serielle Konsole an, sobald das Modul eingesetzt ist und bereit ist, DEN AUTOSTART von node1 zu unterbrechen.
5. Nachdem Sie DIE AUTOBOOT-Funktion unterbrochen haben, wird node2 an der LOADER-Eingabeaufforderung angehalten. Wenn SIE DIE AUTOBOOT-Zeit nicht unterbrechen und node2 den Startvorgang startet, warten Sie auf die Eingabeaufforderung und drücken Sie **Strg-C**, um in das Startmenü zu gelangen. Nachdem der Knoten im Startmenü angehalten wurde, verwenden Sie die Option `8` Um den Node neu zu booten und den AUTOBOOT während des Neubootens zu unterbrechen.
6. Legen Sie an der Eingabeaufforderung LOADER> von node2 die Standardumgebungsvariablen fest:

   ```
   set-defaults
   ```

7. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:

   ```
   saveenv
   ```

Netzboot Nr. 2

Nachdem Sie die entsprechenden Node2-Ersatzsystemmodule ausgetauscht haben, müssen Sie sie möglicherweise mit dem Netzboot starten. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Bei der Vorbereitung auf den Netzboot legen Sie eine Kopie des ONTAP 9-Startabbilds auf einen Webserver, auf den das System zugreifen kann.

Es ist nicht möglich, die auf dem Boot-Medium des Ersatz-Controller-Moduls installierte ONTAP-Version zu überprüfen, es sei denn, sie ist in einem Gehäuse installiert und eingeschaltet. Die ONTAP-Version auf dem Ersatz-System-Boot-Medium muss mit der ONTAP-Version auf dem alten System identisch sein, das Sie aktualisieren, und sowohl das primäre als auch das Backup-Boot-Image müssen übereinstimmen. Sie können die Images konfigurieren, indem Sie einen Netzboot gefolgt vom ausführen `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

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

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Laden Sie die für Ihr System erforderlichen Systemdateien und die korrekte Version von ONTAP von *NetApp Support Site* herunter. Siehe "Quellen" Link zur NetApp Support Site_.

Über diese Aufgabe

Sie müssen die neuen Controller als Netzboot ansehen, wenn sie nicht die gleiche Version von ONTAP 9 auf ihnen installiert sind, die auf den ursprünglichen Controllern installiert ist. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Siehe "Quellen" Um eine Verknüpfung zur NetApp Support Site_ zu erhalten, um die Dateien zum Ausführen des Netzboots des Systems herunterzuladen.
2. Laden Sie die entsprechende ONTAP Software im Bereich Software Download der NetApp Support Website herunter, und speichern Sie die `<ontap_version>_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.
4. Ihre Verzeichnisliste sollte enthalten `<ontap_version>_image.tgz`.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie müssen den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

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

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

6. Ausführen eines Netzboots auf Knoten 2:

```
netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel
```

Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis node2 jetzt auf dem Ersatz-Controller-Modul ausgeführt wird, um zu starten und die Boot-Menüoptionen anzuzeigen, wie in der folgenden Ausgabe gezeigt:

```
Please choose one of the following:

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

8. Wählen Sie im Startmenü Option `(7) Install new software first`.

   Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

Ignorieren Sie die folgende Meldung:

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

Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades.

> Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen. Das Netzboot wird mit der Option kombiniert `(7) Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

9. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:
   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

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

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

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

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

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

11. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium.
    a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`:

    ```
    This will delete critical system configuration, including cluster
    membership.
    Warning: do not run this option on a HA node that has been taken
    over.
    Are you sure you want to continue?:
    ```

    b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.

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

    ```
    ha-config show
    ```

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

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

14. Wenn Controller und Chassis nicht als konfiguriert wurden `ha`, Verwenden Sie die folgenden Befehle, um die Konfiguration zu korrigieren:

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

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

15. Stopp-Nr. 2:

    ```
    halt
    ```

    Node2 sollte an DER Loader>-Eingabeaufforderung angehalten werden.

16. Überprüfen Sie auf Knoten 1 das Systemdatum, die Uhrzeit und die Zeitzone:

    ```
    date
    ```

17. Überprüfen Sie bei node2 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show date
    ```

18. Legen Sie bei Bedarf das Datum auf node2 fest:

    `set date` *`mm/dd/yyyy`*

    ⓘ Setzen Sie das entsprechende UTC-Datum auf node2.

19. Überprüfen Sie bei node2 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

    ```
    show time
    ```

20. Stellen Sie bei Bedarf die Zeit auf node2 ein:

    `set time` *`hh:mm:ss`*

    ⓘ Legen Sie die entsprechende UTC-Zeit auf node2 fest.

21. Legen Sie die Partner-System-ID auf node2 fest:

    ```
    setenv partner-sysid node1_sysid
    ```

    Für node2, die `partner-sysid` Muss der Knoten 1 sein, den Sie aktualisieren.

    a. Einstellungen speichern:

    ```
    saveenv
    ```

22. Überprüfen Sie in node2 an der LOADER-Eingabeaufforderung den `partner-sysid` Für Knoten 2:

    ```
    printenv partner-sysid
    ```

Phase 6. Starten Sie Knoten2 mit den Ersatz-Systemmodulen

Überblick

In Phase 6 starten Sie Knoten 2 mit aktualisierten Systemmodulen und überprüfen die aktualisierte Installation von Knoten 2. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1-Aggregate und NAS-Daten-LIFs von node1 auf die aktualisierte Node2 verschoben und Sie überprüfen, ob die SAN-LIFs auf node2 vorhanden sind.

1. "Starten Sie Knoten2 mit den Ersatz-Systemmodulen"
2. "Überprüfen Sie die Installation node2"
3. "Wiederherstellen der Key-Manager-Konfiguration auf node2"
4. "Verschieben Sie Aggregate und NAS-Daten-LIFs zurück auf node2"

Starten Sie Knoten2 mit den Ersatz-Systemmodulen

Node2 mit den Ersatzmodulen ist nun startbereit. Bei der Aktualisierung durch Austausch der Systemmodule werden nur die Konsolen- und Managementverbindungen verschoben. In diesem Abschnitt werden die Schritte beschrieben, die zum Starten von Knoten2 mit den Ersatzmodulen für die folgenden Upgrade-Konfigurationen erforderlich sind:

Alter Knoten 2-Controller	Ersatz-Knoten2-Systemmodule
AFF A220 als ASA konfiguriert	Controller-Modul ASA A150
AFF A220 AFF A200 AFF C 190	Controller-Modul AFF A150
FAS2620 FAS2720	FAS2820 Controller-Modul

Alter Knoten 2-Controller	Ersatz-Knoten2-Systemmodule
AFF A700 – als ASA konfiguriert	ASA A900-Controller und NVRAM-Module
AFF A700	AFF A900-Controller und NVRAM-Module
FAS9000	FAS9500 Controller- und NVRAM-Module

Schritte

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

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

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

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

   > FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

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

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

2. Starten Sie den Knoten im Startmenü:

   ```
   boot_ontap menu
   ```

3. Weisen Sie die alten Node2-Festplatten dem Ersatznode2 zu, indem Sie „22/7“ eingeben und die versteckte Option auswählen `boot_after_controller_replacement` Wenn der Node im Boot-Menü angehalten wird.

   Nach einer kurzen Verzögerung werden Sie aufgefordert, den Namen des Node einzugeben, der ersetzt wird. Wenn gemeinsam genutzte Festplatten vorhanden sind (auch Advanced Disk Partitioning (ADP) oder partitionierte Festplatten), werden Sie aufgefordert, den Node-Namen des HA-Partners einzugeben.

   Diese Eingabeaufforderungen sind möglicherweise in den Konsolenmeldungen verborgen. Wenn Sie keinen Node-Namen eingeben oder einen falschen Namen eingeben, werden Sie aufgefordert, den Namen erneut einzugeben.

Wenn `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` Und oder `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` Fehler auftreten, führen Sie die folgenden Schritte aus:

a. Halten Sie den Node an der LOADER-Eingabeaufforderung an.
b. Prüfen und setzen Sie die Storage Encryption Boot-Optionen zurück, die in erwähnt sind Schritt 1.
c. An der Loader-Eingabeaufforderung booten Sie:

```
boot_ontap
```

Das folgende Beispiel kann als Referenz verwendet werden:

Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
.
<output truncated>
.
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

Please choose one of the following:

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

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
```

```
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

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

Die im vorhergehenden Beispiel gezeigten System-IDs sind Beispiel-IDs. Die tatsächlichen System-IDs der Nodes, die Sie aktualisieren, unterscheiden sich.

Zwischen der Eingabe von Node-Namen an der Eingabeaufforderung und der Eingabeaufforderung für die Anmeldung wird der Node mehrmals neu gebootet, um die Umgebungsvariablen wiederherzustellen, die Firmware auf den im System verwendeten Karten zu aktualisieren und für andere ONTAP Updates zu sorgen.

Überprüfen Sie die Installation node2

Sie müssen die Installation von node2 mit den Ersatz-Systemmodulen überprüfen. Da keine Änderung an physischen Ports erfolgt, sind Sie nicht erforderlich, die physischen Ports von der alten node2 auf den Ersatz-Knoten2 zuzuordnen.

Über diese Aufgabe

Nachdem Sie node1 mit dem Ersatz-Systemmodul gestartet haben, überprüfen Sie, ob es richtig installiert ist. Sie müssen warten, bis Node2 dem Quorum Beitritt und dann den Vorgang zum Austausch des Controllers fortsetzen.

An diesem Punkt des Verfahrens wird die Operation angehalten, während node2 dem Quorum beitritt.

Schritte

1. Vergewissern Sie sich, dass node2 dem Quorum beigetreten ist:

   ```
   cluster show -node node2 -fields health
   ```

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

2. Vergewissern Sie sich, dass node2 Teil desselben Clusters wie node1 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

3. Wechseln in den erweiterten Berechtigungsmodus:

   ```
   set advanced
   ```

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

   ```
   system controller replace show
   ```

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

5. Setzen Sie den Austausch des Controllers wieder ein:

   ```
   system controller replace resume
   ```

6. Der Controller-Ersatzvorgang hält für Eingriffe mit der folgenden Meldung an:

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

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


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

In diesem Verfahren wurde der Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node2_ umbenannt.

7. Wenn sich der Controller-Austausch im Status „Pause“ befindet, fahren Sie mit fort Stellen Sie die Netzwerkkonfiguration auf node2 wieder her.

Stellen Sie die Netzwerkkonfiguration auf node2 wieder her

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

Über diese Aufgabe

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

Schritte

1. Listen Sie alle physischen Ports auf Upgrade-Knoten2 auf:

```
network port show -node node2
```

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

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Netzwerk-Port-Erreichbarkeit aller Ports auf node2 auflisten:

```
network port reachability show -node node2
```

Die Ausgabe sollte dem folgenden Beispiel ähnlich sein. Die Port- und Broadcast-Namen variieren.

```
Cluster::*> network port reachability show -node local
Node      Port     Expected Reachability                Reachability
Status
--------- -------- -----------------------------------
---------------------
Node2
          e0M      Default:Mgmt                         no-reachability
          e10a     Default:Default-3                    ok
          e10b     Default:Default-4                    ok
          e11a     Cluster:Cluster                      no-reachability
          e11b     Cluster:Cluster                      no-reachability
          e11c     -                                    no-reachability
          e11d     -                                    no-reachability
          e2a      Default:Default-1                    ok
          e2b      Default:Default-2                    ok
          e9a      Default:Default                      no-reachability
          e9b      Default:Default                      no-reachability
          e9c      Default:Default                      no-reachability
          e9d      Default:Default                      no-reachability
13 entries were displayed.
```

Im vorherigen Beispiel wurde node2 nach dem Austausch des Controllers gestartet und dem Quorum beigetreten. Es verfügt über mehrere Ports, die keine Erreichbarkeit haben und eine Überprüfung der Erreichbarkeit ausstehen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node2 mit einem anderen Status als der Erreichbarkeit `ok` Mit dem folgenden Befehl in der folgenden Reihenfolge:

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

   a. Physische Ports

b. VLAN-Ports

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Eine Warnmeldung, wie im vorhergehenden Beispiel dargestellt, wird für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Erreichbarkeit der Broadcast-Domäne unterscheiden können, in der sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort `y` Oder `n` Je nach Bedarf.

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

```
network port reachability show
```

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

5. Überprüfen der Port-Erreichbarkeit:

```
network port reachability show
```

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

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

```
network port show
```

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

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

8. Stellen Sie die LIF-Home-Ports wieder her und geben Sie ggf. den Vserver und die LIF-Home-Ports an, die Sie mit folgenden Schritten wiederherstellen müssen:

   a. Führen Sie alle vertriebenen LIFs auf:

   ```
   displaced-interface show
   ```

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

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

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

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

Wiederherstellen der Key-Manager-Konfiguration auf node2

Wenn Sie mit NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) Volumes auf dem System, das ein Upgrade ausführt, wird die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert. Wenn Sie den Key-Manager nicht neu synchronisieren, wenn Sie die node2-Aggregate mithilfe von ARL vom aktualisierten Node1 zum aktualisierten Node2 verschieben, können Ausfälle auftreten, da node2 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

Über diese Aufgabe

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

Schritte

1. Führen Sie den folgenden Befehl aus node2:

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

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node2 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK
```

Beispiel

```
::> security key-manager key query -node node2 -fields restored -key
-type SVM-KEK

node     vserver   key-server   key-id
restored
-------- --------- -----------  ----------------------------------------
--------
node2    svm1      ""           00000000000000000200000000000a008a81976
true
                                2190178f9350e071fbb90f00000000000000000
```

Verschieben Sie Aggregate und NAS-Daten-LIFs zurück auf node2

Nachdem Sie die Netzwerkkonfiguration auf Node2 überprüft und bevor Sie Aggregate von Node1 zu Node2 verschieben, überprüfen Sie, ob die NAS-Daten-LIFs, die zu Node2 gehören, die sich derzeit auf Node1 befinden, von Node1 zu Node2 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN LIFs auf Knoten2 vorhanden sind.

Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Nachdem Sie node2 in den Online-Modus versetzt haben, müssen Sie überprüfen, ob sich die LIFs in einem ordnungsgemäßen Zustand und auf den entsprechenden Ports befinden.

Schritte

1. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Aufgaben aus:

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

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

2. Wiederaufnahme des Betriebs der Versetzung:

   ```
   system controller replace resume
   ```

   Das System führt folgende Prüfungen durch:

   - Cluster-Zustandsprüfung
   - LIF-Statusüberprüfung für Cluster

   Nach Durchführung dieser Überprüfungen verlagert das System die nicht-Root-Aggregate und NAS-Daten-LIFs zurück auf node2, das jetzt auf dem Ersatz-Controller ausgeführt wird.

   Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

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

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

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

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

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

Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in node2 wieder her:

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

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

   ```
   system controller replace resume
   ```

   Das System führt die folgenden Nachprüfungen durch:

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

Phase 7: Schließen Sie das Upgrade ab

Überblick

In Phase 7 bestätigen Sie, dass die neuen Nodes ordnungsgemäß eingerichtet wurden. Bei aktivierter Verschlüsselung konfigurieren und einrichten Sie Storage Encryption bzw. NetApp Volume Encryption. Zudem sollten die alten Nodes außer Betrieb gesetzt und der SnapMirror Betrieb fortgesetzt werden.

Schritte

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

Authentifizierungsmanagement mit KMIP-Servern

Ab ONTAP 9.10.1 können Sie KMIP-Server (Key Management Interoperability Protocol) verwenden, um Authentifizierungsschlüssel zu managen.

Schritte

1. Hinzufügen eines neuen Controllers:

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

2. Fügen Sie den Schlüsselmanager hinzu:

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

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

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

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

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

Vergewissern Sie sich, dass die neuen Controller ordnungsgemäß eingerichtet sind

Um die korrekte Einrichtung zu überprüfen, überprüfen Sie, ob das HA-Paar aktiviert ist. Außerdem überprüfen Sie, ob Node 1 und Node 2 auf den Storage zugreifen können und ob keine der Daten-LIFs gehören, die zu anderen Nodes im Cluster gehören. Außerdem überprüfen Sie, ob alle Datenaggregate auf den richtigen Home Nodes vorhanden sind und ob die Volumes für beide Nodes online sind. Wenn einer der neuen Nodes über einen Unified Target Adapter verfügt, müssen Sie alle Port-Konfigurationen wiederherstellen. Darüber hinaus muss die Verwendung des Adapters geändert werden.

Schritte

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

   ```
   storage failover show
   ```

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

   ```
   cluster::> storage failover show
                              Takeover
   Node        Partner        Possible      State Description
   ----------  -----------    ------------  ------------------
   node1       node2          true          Connected to node2
   node2       node1          true          Connected to node1
   ```

3. Vergewissern Sie sich, dass node1 und node2 zum gleichen Cluster gehören, indem Sie den folgenden Befehl verwenden und die Ausgabe überprüfen:

```
cluster show
```

4. Vergewissern Sie sich, dass node1 und node2 über den folgenden Befehl und eine Analyse der Ausgabe auf den Storage des jeweils anderen zugreifen können:

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

5. Vergewissern Sie sich, dass weder node1 noch node2 Eigentümer von Daten-LIFs sind, die im Besitz anderer Nodes im Cluster sind. Verwenden Sie dazu den folgenden Befehl und prüfen Sie die Ausgabe:

   ```
   network interface show
   ```

   Wenn weder Node1 noch node2 Daten-LIFs Eigentümer anderer Nodes im Cluster sind, setzen Sie die Daten-LIFs auf ihren Home-Eigentümer zurück:

   ```
   network interface revert
   ```

6. Vergewissern Sie sich, dass die Aggregate den jeweiligen Home-Nodes gehören.

   ```
   storage aggregate show -owner-name node1
   ```

   ```
   storage aggregate show -owner-name node2
   ```

7. Legen Sie fest, ob Volumes offline sind:

   ```
   volume show -node node1 -state offline
   ```

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

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

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

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

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

   Der Lizenzcode-Parameter akzeptiert eine Liste von 28 alphabetischen Zeichenschlüsseln für Großbuchstaben. Sie können jeweils eine Lizenz hinzufügen, oder Sie können mehrere Lizenzen gleichzeitig hinzufügen, indem Sie jeden Lizenzschlüssel durch ein Komma trennen.

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

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

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

    - Alle abgelaufenen Lizenzen löschen:

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

- Alle nicht verwendeten Lizenzen löschen:

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

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

  ```
  system license delete -serial-number node1_serial_number -package *
  system license delete -serial-number node2_serial_number -package *
  ```

Die folgende Ausgabe wird angezeigt:

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

Eingabe `y` Um alle Pakete zu entfernen.

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

    ```
    system license show
    ```

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

12. Wenn in der Konfiguration selbstverschlüsselnde Laufwerke verwendet werden und Sie den festgelegt haben `kmip.init.maxwait` Variabel auf `off` (Beispiel: In *Boot node2 mit den Ersatz-Systemmodulen* "Schritt 1"), Sie müssen die Einstellung der Variable aufheben:

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

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

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

    Siehe "Quellen" Link zur *Systemverwaltungsreferenz* für Informationen zu den SPs und den Befehlen *ONTAP 9: Manual Page Reference* für detaillierte Informationen zum System `service-processor network modify` Befehl.

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

Nachdem Sie fertig sind

Wenn die Speicherverschlüsselung auf node1 und node2 aktiviert ist, füllen Sie den Abschnitt aus "Richten Sie Storage Encryption auf dem neuen Controller-Modul ein". Andernfalls füllen Sie den Abschnitt aus "Ausmustern des alten Systems".

Richten Sie Storage Encryption auf dem neuen Controller-Modul ein

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

Über diese Aufgabe

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

Schritte

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

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

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

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

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

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

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

      security key-manager external show

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

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

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

      security key-manager external enable

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

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

   security key-manager external restore -node *new_controller_name*

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

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

Über diese Aufgabe

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

Onboard Key Manager

Konfigurieren Sie NVE oder NAE mit dem Onboard Key Manager.

Schritte

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

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

Externes Verschlüsselungsmanagement

Konfigurieren Sie NVE oder NAE mit externem Verschlüsselungsmanagement.

Schritte

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

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

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

   a. Fügen Sie den Schlüsselverwaltungsserver hinzu:

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

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

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

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

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

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

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

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

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

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

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

   Für diesen Befehl ist die OKM-Passphrase erforderlich

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

Nachdem Sie fertig sind

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

Nachdem Sie fertig sind

Überprüfen Sie, ob Volumes offline geschaltet wurden, da Authentifizierungsschlüssel nicht verfügbar waren oder externe Schlüsselverwaltungsserver nicht erreicht werden konnten. Stellen Sie diese Volumes mit der wieder online `volume online` Befehl.

Ausmustern des alten Systems

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

Schritte

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

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

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

   In einer Tabelle werden Cluster-Informationen, einschließlich der Seriennummern, angezeigt.

5. Suchen Sie den Cluster in der Tabelle und wählen Sie im Dropdown-Menü Product Tool Set die Option **Decommission this System** aus.

Setzen Sie den SnapMirror Betrieb fort

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

Schritte

1. Überprüfen Sie den SnapMirror Status auf dem Ziel:

   ```
   snapmirror show
   ```

2. Wiederaufnahme der SnapMirror Beziehung:

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

Fehlerbehebung

Fehlerbehebung

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

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

Fehler bei der Aggregatverschiebung

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

Prüfen Sie, ob Aggregate Relocation Failure vorhanden sind

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

Schritte

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

   ```
   storage aggregate relocation show
   ```

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

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

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

   Ausführliche Informationen zum `storage aggregate relocation start`, `override-vetoes`, und `override-destination-checks` Optionen finden Sie unter "Quellen" Link zu den Befehlen *ONTAP 9: Manual Page Reference*.

Aggregate, die ursprünglich auf node1 verwendet wurden, sind nach Abschluss des Upgrades Eigentum von node2

Beim Ende des Upgrade-Verfahrens sollte die Knoten1 der neue Home-Node von Aggregaten sein, die ursprünglich als Home-Node node1 verwendet wurden. Sie können sie nach dem Upgrade verschieben.

Über diese Aufgabe

Falls Aggregate nicht korrekt verschoben werden können, d. h. Node 2 statt Knoten 1, wird unter den folgenden Umständen als Home Node verwendet:

- In Phase 3, wenn Aggregate von node2 auf node1 verschoben werden.

  Einige der verlagerten Aggregate haben die Nr. 1 als Home-Node. Ein solches Aggregat könnte zum Beispiel „aggr_Node_1“ heißen. Wenn die Verlagerung von aggr_Node_1 während Phase 3 fehlschlägt und eine Verlagerung nicht erzwungen werden kann, dann bleibt das Aggregat auf node2 zurück.

- Nach Phase 4, wenn node2 durch die neuen Systemmodule ersetzt wird.

  Wenn node2 ersetzt wird, kommt aggr_Node_1 mit node1 als Home-Node statt node2 online.

Nach Phase 6 können Sie das falsche Eigentümerproblem beheben, nachdem Sie das Storage-Failover aktiviert haben, indem Sie die folgenden Schritte durchführen:

Schritte

1. Erhalten Sie eine Liste von Aggregaten:

   `storage aggregate show -nodes node2 -is-home true`

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

2. Vergleichen Sie die Ausgabe von Schritt 1 mit der Ausgabe, die Sie für Knoten 1 im Abschnitt aufgenommen haben "Bereiten Sie die Knoten für ein Upgrade vor" Und beachten Sie alle Aggregate, die nicht korrekt verschoben wurden.
3. Verschiebung der Aggregate links hinter Knoten2:

   `storage aggregate relocation start -node node2 -aggr aggr_node_1 -destination node1`

   Verwenden Sie während dieser Verschiebung keinen Parameter für -ndo-Controller-Upgrade.

4. Vergewissern Sie sich, dass node1 jetzt der Haupteigentümer der Aggregate ist:

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

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

   Aggregate, die nicht den Knoten1 als Hausbesitzer haben, können mit dem gleichen Relocation-Befehl in Schritt 3 auf node1 umgezogen werden.

Neustarts, Panikspiele oder Energiezyklen

Das System kann in verschiedenen Phasen des Upgrades abstürzt, z. B. neu gebootet, Panik oder ein aus- und Wiedereinschalten durchlaufen.

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

Neustarts, Panikzugänge oder Energiezyklen während der Vorprüfphase

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

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

Über diese Aufgabe

Takeover und Giveback können normal fortgesetzt werden.

Schritte

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

Neustarts, Panikzugänge oder Energiezyklen während der ersten Ressourcenfreigabephase

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

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

Über diese Aufgabe

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

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

Schritte

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

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

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

Schritte

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

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

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

Über diese Aufgabe

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

Schritte

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

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

Node1 übernimmt nicht.

Schritte

1. Knoten 2 aufbring.

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

2. Setzen Sie den mit dem Rest des Upgrade-Vorgangs für das Node-Paar fort.

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

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

Node1 übernimmt nicht nach einem Absturz nach node2, da das HA-Paar bereits deaktiviert ist.

Schritte

1. Knoten 2 aufbring.

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

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

Node1 stürzt in der ersten Überprüfungsphase ab, wobei das HA-Paar deaktiviert ist

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

Schritte

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

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

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

Node2 hat einige oder alle seine Aggregate von node1 in node1 verschoben. Node1 liefert Daten von Aggregaten, die verschoben wurden. Das HA-Paar ist deaktiviert und somit gibt es keine Übernahme.

Über diese Aufgabe

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

Schritte

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

Knoten 1 stürzt während der ersten Ressourcen-Wiederholen Phase während der Aggregat-Verschiebung ab

Wenn node1 abstürzt, während node2 Aggregate zu node1 verschoben wird, wird die Aufgabe nach dem Booten von node1 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, aber Aggregate, die bereits in Knoten 1 verlagert wurden, begegnen ein Client-Ausfall, während node1 gebootet wird.

Schritte

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

Neustarts, Panikspiele oder Energiezyklen während der Nachprüfphase

Node1 oder node2 stürzt während der Nachprüfphase ab

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

Schritte

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

Neustarts, Panikzucken oder Energiezyklen während der zweiten Ressourcenfreigabephase

Node1 stürzt während der zweiten Resource-Release-Phase ab

Wenn node1 abstürzt, während node2 Aggregate verschoben wird, wird die Aufgabe nach dem Booten von node1 fortgesetzt.

Über diese Aufgabe

Node2 dient weiterhin verbleibenden Aggregaten, aber Aggregate, die bereits in Node1 verlagert wurden und Node1 eigene Aggregate, begegnen Client-Ausfällen, während node1 gebootet wird.

Schritte

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

Node2 stürzt während der zweiten Resource-Release-Phase ab

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

Über diese Aufgabe

Node1 dient weiterhin den Aggregaten, die verschoben wurden, aber die Aggregate von node2 stoßen auf Client-Ausfälle.

Schritte

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

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

Node1 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node1 abstürzt, wird die Übernahme nicht ausgeführt, da das HA-Paar bereits deaktiviert ist.

Über diese Aufgabe

Es gibt einen Client-Ausfall für alle Aggregate, bis node1 neu gebootet wird.

Schritte

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

Node2 stürzt während der zweiten Verifikationsphase ab

Wenn während dieser Phase node2 abstürzt, wird die Übernahme nicht durchgeführt. Node1 dient Daten aus den Aggregaten.

Über diese Aufgabe

Es gibt einen Ausfall für nicht-Root-Aggregate, die bereits so lange verschoben wurden bis nach einem Neustart von node2.

Schritte

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

Probleme, die in mehreren Phasen des Verfahrens auftreten können

Einige Probleme können in verschiedenen Phasen des Verfahrens auftreten.

Unerwartete Ausgabe des „Storage Failover show“-Befehls

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

Über diese Aufgabe

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

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

```
cluster::> storage failover show

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

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

```
cluster::> storage failover show

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

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

Schritte

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

Fehler bei der LIF-Migration

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

Schritte

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

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

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

Quellen

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

- Referenzinhalt
- Referenzstandorte

Referenzinhalt

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

Inhalt	Beschreibung
"Administrationsübersicht mit der CLI"	Beschreibt das Verwalten von ONTAP Systemen, zeigt die Verwendung der CLI-Schnittstelle, den Zugriff auf das Cluster, das Managen von Nodes und vieles mehr.
"Entscheiden Sie, ob Sie System Manager oder die ONTAP CLI für das Cluster-Setup verwenden möchten"	Beschreibt die Einrichtung und Konfiguration von ONTAP.
"Festplatten- und Aggregatmanagement mit CLI"	Beschreibt das Verwalten von physischem ONTAP Storage mit der CLI. Hier erfahren Sie, wie Sie Aggregate erstellen, erweitern und managen, wie Sie mit Flash Pool Aggregaten arbeiten, Festplatten managen und RAID-Richtlinien managen.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	Beschreibt die Installation und Konfiguration der MetroCluster Hardware- und Softwarekomponenten in einer Fabric-Konfiguration.
"Installationsanforderungen für die FlexArray Virtualisierung und Referenz"	Enthält Verkabelungsanweisungen und andere Informationen für FlexArray-Virtualisierungssysteme.
"Hochverfügbarkeits-Management"	Beschreibt die Installation und das Management von hochverfügbaren geclusterten Konfigurationen, einschließlich Storage Failover und Takeover/Giveback.
"Logisches Storage-Management mit der CLI"	Beschreibt, wie Sie Ihre logischen Storage-Ressourcen mithilfe von Volumes, FlexClone Volumes, Dateien und LUNs effizient managen FlexCache Volumes, Deduplizierung, Komprimierung, qtrees und Quotas.
"MetroCluster Management und Disaster Recovery"	Beschreibt die Durchführung von MetroCluster-Switchover- und Switchback-Vorgängen sowohl bei geplanten Wartungsvorgängen als auch bei einem Notfall.
"MetroCluster Upgrade und Erweiterung"	Bietet Verfahren zum Upgrade von Controller- und Storage-Modellen in der MetroCluster Konfiguration, zum Wechsel von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration und zum erweitern der MetroCluster-Konfiguration durch Hinzufügen weiterer Nodes
"Netzwerkmanagement"	Beschreibt die Konfiguration und das Management von physischen und virtuellen Netzwerk-Ports (VLANs und Schnittstellengruppen), LIFs, Routing- und Host-Resolution-Services in Clustern; Optimierung des Netzwerk-Traffic durch Lastenausgleich; und Überwachung des Clusters mit SNMP
"ONTAP 9.0-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.0-Befehle.

Inhalt	Beschreibung
"ONTAP 9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.1-Befehle.
"ONTAP 9.2-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.2-Befehle.
"ONTAP 9.3-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.3-Befehle.
"ONTAP 9.4-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.4-Befehle.
"ONTAP 9.5-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.5-Befehle.
"ONTAP 9.6-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.6-Befehle.
"ONTAP 9.7-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.7-Befehle.
"ONTAP 9.8-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.8-Befehle.
"ONTAP 9.9.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.9.1-Befehle.
"ONTAP 9.10.1-Befehle: Manuelle Seitenreferenz"	Beschreibt die Syntax und die Verwendung der unterstützten ONTAP 9.10.1-Befehle.
"SAN-Management mit CLI"	In wird beschrieben, wie LUNs, Initiatorgruppen und Ziele mithilfe der iSCSI- und FC-Protokolle sowie Namespaces und Subsysteme mit dem NVMe/FC-Protokoll konfiguriert und gemanagt werden.
"Referenz zur SAN-Konfiguration"	Hier finden Sie Informationen zu FC- und iSCSI-Topologien sowie Kabelschemata.
"Upgrade durch Verschieben von Volumes oder Storage"	Beschreibt das schnelle Upgrade von Controller Hardware in einem Cluster durch Verschieben von Storage oder Volumes. Beschreibt zudem, wie ein unterstütztes Modell in ein Festplatten-Shelf konvertiert wird.
"Upgrade von ONTAP"	Die Anleitungen zum Herunterladen und Aktualisieren von ONTAP.
"Aktualisieren Sie Controller-Modelle im selben Chassis mit Befehlen „System-Controller ersetzen“"	Beschreibt die Verfahren zur Aggregatverschiebung, die für ein unterbrechungsfreies Upgrade eines Systems erforderlich sind, wobei das alte System-Chassis und die alten Festplatten erhalten bleiben.
"Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um Controller, die ONTAP 9.8 ausführen, durch den „System-Controller-Austausch“-Befehl unterbrechungsfrei zu aktualisieren.

Inhalt	Beschreibung
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.8 oder höher durchzuführen"	Beschreibt das Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.8 oder höher durchzuführen.
"Verwenden Sie „System Controller Replace“-Befehle, um Controller Hardware mit ONTAP 9.5 auf ONTAP 9.7 zu aktualisieren"	Beschreibt die Verfahren für Aggregatverschiebung, die nötig sind, um ein unterbrechungsfreies Upgrade der Controller, die ONTAP 9.5 auf ONTAP 9.7 mithilfe von Befehlen zum Austausch des System-Controllers durchführen, durchzuführen.
"Nutzen Sie die Aggregatverschiebung, um manuell ein Upgrade der Controller-Hardware mit ONTAP 9.7 oder einer älteren Version durchzuführen"	Beschreibt die Verfahren für die Aggregatverschiebung, die erforderlich sind, um manuelle, unterbrechungsfreie Controller-Upgrades mit ONTAP 9.7 oder früher durchzuführen.

Referenzstandorte

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

Datenzugriff "ONTAP 9-Dokumentation".

Auf das zugreifen "Active IQ Config Advisor" Werkzeug.