Installieren Sie eine Stretch-MetroCluster-Konfiguration

ONTAP MetroCluster

NetApp
April 12, 2024

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

Inhalt

Installieren Sie eine Stretch-MetroCluster-Konfiguration . . . 1
Überblick . . . 1
Bereiten Sie sich auf die MetroCluster Installation vor . . . 1
Auswahl des richtigen Installationsverfahrens für Ihre Konfiguration . . . 6
Verkabeln Sie eine Stretch-MetroCluster-Konfiguration mit zwei SAS-Attached . . . 7
Verkabeln einer Stretch-MetroCluster-Konfiguration mit zwei über Bridge verbundenen Nodes . . . 13
Konfigurieren der MetroCluster-Software in ONTAP . . . 20
Überlegungen zur Verwendung von virtuellem IP- und Border-Gateway-Protokoll mit einer MetroCluster-Konfiguration . . . 59
Testen der MetroCluster-Konfiguration . . . 62
Verbindungen in Stretch-MetroCluster-Konfigurationen mit Array-LUNs . . . 80
Überlegungen beim Entfernen von MetroCluster-Konfigurationen . . . 84
So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring . . . 84
Überlegungen bei der Verwendung von ONTAP in einer MetroCluster-Konfiguration . . . 85
Umstieg von einer Stretch- zu einer Fabric-Attached MetroCluster Konfiguration . . . 95
Wo Sie weitere Informationen finden . . . 96

Installieren Sie eine Stretch-MetroCluster-Konfiguration

Überblick

Um Ihre Stretch MetroCluster Konfiguration zu installieren, müssen Sie eine Reihe von Verfahren in der richtigen Reihenfolge durchführen.

- "Bereiten Sie sich auf die Installation vor und verstehen Sie alle Anforderungen"
- "Wählen Sie das korrekte Installationsverfahren aus"
- Verkabeln Sie die Komponenten
  - "SAS-Attached-Konfiguration mit zwei Nodes"
  - "Konfiguration mit zwei über Bridge verbundenen Nodes"
- "Konfigurieren der Software"
- "Testen Sie die Konfiguration"

Bereiten Sie sich auf die MetroCluster Installation vor

Unterschiede zwischen den ONTAP MetroCluster Konfigurationen

Die verschiedenen MetroCluster Konfigurationen weisen wesentliche Unterschiede in den erforderlichen Komponenten auf.

In allen Konfigurationen ist jeder der beiden MetroCluster-Standorte als ONTAP-Cluster konfiguriert. In einer MetroCluster Konfiguration mit zwei Nodes ist jeder Node als Single-Node-Cluster konfiguriert.

Merkmal	IP-Konfigurationen	Fabric-Attached-Konfigurationen		Stretch-Konfigurationen	
		Vier- oder acht-Knoten	* Zwei Knoten*	* Zwei-Knoten-Brücke-verbunden*	* Zwei-Knoten direkt verbunden*
Anzahl an Controllern	Vier oder acht*	Vier oder acht	Zwei	Zwei	Zwei
Storage Fabric mit FC-Switch	Nein	Ja.	Ja.	Nein	Nein
Verwendet eine IP Switch Storage Fabric	Ja.	Nein	Nein	Nein	Nein
Verwendung von FC-to-SAS-Bridges	Nein	Ja.	Ja.	Ja.	Nein

Nutzung von Direct-Attached SAS Storage	Ja (nur lokal in Verbindung)	Nein	Nein	Nein	Ja.
Unterstützt ADP	Ja (ab ONTAP 9.4)	Nein	Nein	Nein	Nein
Unterstützt lokale HA	Ja.	Ja.	Nein	Nein	Nein
Unterstützt ONTAP Automatic ungeplante Switchover (AUSO)	Nein	Ja.	Ja.	Ja.	Ja.
Unterstützt nicht gespiegelte Aggregate	Ja (ab ONTAP 9.8)	Ja.	Ja.	Ja.	Ja.
Unterstützt Array-LUNs	Nein	Ja.	Ja.	Ja.	Ja.
Unterstützt den ONTAP Mediator	Ja (ab ONTAP 9.7)	Nein	Nein	Nein	Nein
Unterstützung von MetroCluster Tiebreaker	Ja (nicht in Kombination mit ONTAP Mediator)	Ja.	Ja.	Ja.	Ja.
Unterstützt Rein SAN-basierte Arrays	Ja.	Ja.	Ja.	Ja.	Ja.

- Wichtig*

Beachten Sie bei MetroCluster IP-Konfigurationen mit acht Nodes die folgenden Überlegungen:

- Konfigurationen mit acht Nodes werden ab ONTAP 9.9 unterstützt.
- Es werden nur NetApp validierte MetroCluster Switches (bei NetApp bestellt) unterstützt.
- Konfigurationen, die IP-geroutet (Layer 3)-Back-End-Verbindungen verwenden, werden nicht unterstützt.
- Konfigurationen mit gemeinsam genutzten privaten Layer 2-Netzwerken werden nicht unterstützt.
- Konfigurationen mit einem gemeinsamen Cisco 9336C-FX2 Switch werden nicht unterstützt.

Unterstützung für alle SAN-Array-Systeme in MetroCluster Konfigurationen

Einige der All-SAN-Arrays (ASAs) werden in MetroCluster-Konfigurationen unterstützt. In der MetroCluster-

Dokumentation gelten die Informationen zu AFF-Modellen auf das entsprechende ASA-System. Beispielsweise gelten alle Kabel und weitere Informationen zum AFF A400 System auch für das ASA AFF A400 System.

Unterstützte Plattformkonfigurationen sind im aufgeführt "NetApp Hardware Universe".

Cluster-Peering

Jede MetroCluster Website ist als Peer-to-dessen Partner-Website konfiguriert. Sie müssen die Voraussetzungen und Richtlinien für die Konfiguration der Peering-Beziehungen kennen. Dies ist wichtig, wenn Sie entscheiden, ob Sie freigegebene oder dedizierte Ports für diese Beziehungen verwenden möchten.

Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie bestätigen, dass die Verbindungsanforderungen zwischen Port, IP-Adresse, Subnetz, Firewall und Cluster-Benennungsanforderungen erfüllt sind.

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

  Beispielsweise muss in einem Cluster mit vier Nodes das für die Kommunikation zwischen Clustern verwendete Subnetz vier verfügbare IP-Adressen haben.

Jeder Node muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster-LIFs können eine IPv4-Adresse oder eine IPv6-Adresse besitzen.

> ONTAP 9 ermöglicht Ihnen die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem Sie optional zulassen, dass beide Protokolle gleichzeitig auf den Intercluster LIFs vorhanden sind. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

- Alle Ports, die für die Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im gleichen IPspace befinden.

Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die für die Cluster-übergreifende Kommunikation verwendete Broadcast-Domäne muss mindestens zwei Ports pro Node enthalten, sodass eine Cluster-übergreifende Kommunikation von einem Port zu einem anderen Port ausfallen kann.

  Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (iffrps) sein.

- Alle Ports müssen verkabelt sein.
- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

- ICMP-Dienst
- TCP auf die IP-Adressen aller Cluster-LIFs über die Ports 10000, 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

Die standardmäßige Cluster-Firewallrichtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Überlegungen bei der Verwendung von dedizierten Ports

Wenn Sie feststellen, ob die Verwendung eines dedizierten Ports für die Intercluster-Replikation die richtige Intercluster-Netzwerklösung ist, sollten Sie Konfigurationen und Anforderungen wie LAN-Typ, verfügbare WAN-Bandbreite, Replikationsintervall, Änderungsrate und Anzahl der Ports berücksichtigen.

Berücksichtigen Sie die folgenden Aspekte Ihres Netzwerks, um zu ermitteln, ob die Verwendung eines dedizierten Ports die beste Intercluster-Netzwerklösung ist:

- Wenn die verfügbare WAN-Bandbreite der der LAN-Ports ähnelt und das Replizierungsintervall so ist, dass eine Replizierung auftritt, während die normale Client-Aktivität besteht, sollten Sie Ethernet-Ports für die Cluster-übergreifende Replizierung zuweisen, um Konflikte zwischen der Replizierung und den Datenprotokollen zu vermeiden.
- Wenn die durch die Datenprotokolle (CIFS, NFS und iSCSI) generierte Netzwerkauslastung eine über 50%ige Netzwerkauslastung bedeutet, dann dedizierte Ports für die Replizierung, die bei einem Node-Failover die Performance nicht beeinträchtigen.
- Wenn physische 10-GbE- oder schnellere Ports für Daten und Replikation verwendet werden, können Sie VLAN-Ports für die Replikation erstellen und die logischen Ports für die Cluster-übergreifende Replikation zuweisen.

  Die Bandbreite des Ports wird von allen VLANs und dem Basis-Port gemeinsam genutzt.

- Berücksichtigen Sie die Datenänderungsrate und das Replizierungsintervall und ob die Datenmenge, die in jedem Intervall repliziert werden muss, genug Bandbreite erfordert. Dies kann zu Konflikten mit Datenprotokollen führen, wenn Daten-Ports gemeinsam genutzt werden.

Überlegungen bei der Freigabe von Datenports

Wenn Sie feststellen, ob die gemeinsame Nutzung eines Datenports für die Intercluster-Replikation die richtige Intercluster-Netzwerklösung ist, sollten Sie Konfigurationen und Anforderungen wie LAN-Typ, verfügbare WAN-Bandbreite, Replikationsintervall, Änderungsrate und Anzahl der Ports berücksichtigen.

Berücksichtigen Sie die folgenden Aspekte Ihres Netzwerks, um zu ermitteln, ob die gemeinsame Nutzung von Datenports die beste Intercluster-Konnektivitätslösung ist:

- In einem High-Speed-Netzwerk, wie etwa einem 40-Gigabit-Ethernet-Netzwerk (40-GbE), steht möglicherweise ausreichend lokale LAN-Bandbreite zur Verfügung, um eine Replizierung auf denselben 40-GbE-Ports durchzuführen, die für den Datenzugriff verwendet werden.

  In vielen Fällen ist die verfügbare WAN-Bandbreite weit kleiner als die 10 GbE-LAN-Bandbreite.

- Unter Umständen müssen alle Nodes im Cluster Daten replizieren und die verfügbare WAN-Bandbreite gemeinsam nutzen, sodass die gemeinsame Nutzung von Daten-Ports akzeptabel ist.
- Durch die gemeinsame Nutzung von Ports für Daten und Replizierung werden keine zusätzlichen Ports mehr benötigt, die für die Bereitstellung dedizierter Ports für die Replikation benötigt werden.
- Die MTU-Größe (Maximum Transmission Unit) des Replikationsnetzwerks entspricht der Größe des Netzwerks.
- Berücksichtigen Sie die Datenänderungsrate und das Replizierungsintervall und ob die Datenmenge, die in jedem Intervall repliziert werden muss, genug Bandbreite erfordert. Dies kann zu Konflikten mit Datenprotokollen führen, wenn Daten-Ports gemeinsam genutzt werden.
- Wenn Daten-Ports für die Cluster-übergreifende Replizierung gemeinsam genutzt werden, können die Intercluster LIFs zu jedem anderen Cluster-fähigen Port desselben Nodes migriert werden, um den spezifischen Datenport zu steuern, der zur Replizierung verwendet wird.

Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten

Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten

Wenn Ihre Konfiguration nicht gespiegelte Aggregate umfasst, müssen potenzielle Zugriffsprobleme erkennen, die einem Switchover folgen.

Überlegungen für nicht gespiegelte Aggregate bei Wartungsarbeiten, die einen Stromausfall erfordern

Wenn Sie aus Wartungsgründen eine Umschaltung durchführen möchten, die ein standortweites Herunterfahren erfordert, sollten Sie zuerst alle nicht gespiegelten Aggregate des Disaster-Standorts manuell offline schalten.

Wenn Sie keine nicht gespiegelten Aggregate offline schalten, so können Nodes am verbleibenden Standort aufgrund einer „Panik mit mehreren Festplatten“ möglicherweise ausfallen. Wenn die Umschaltung über nicht gespiegelte Aggregate offline erfolgt oder fehlt, ist die Verbindung zum Storage am DR-Standort verloren. Dies ist das Ergebnis eines Power Shutdowns oder eines Verlusts von ISLs.

Überlegungen für nicht gespiegelte Aggregate und hierarchische Namespaces

Wenn Sie hierarchische Namespaces verwenden, sollten Sie den Verbindungspfad so konfigurieren, dass alle Volumes in diesem Pfad sich entweder nur auf gespiegelten Aggregaten oder nur auf nicht gespiegelten Aggregaten befinden. Wenn Sie eine Kombination aus nicht gespiegelten und gespiegelten Aggregaten im Verbindungspfad konfigurieren, ist möglicherweise nach der Umschaltung der Zugriff auf nicht gespiegelte Aggregate verhindert.

Überlegungen für nicht gespiegelte Aggregate und CRS-Metadaten-Volume und Root-Volumes der Daten-SVM

Der Configuration Replication Service (CRS) Metadaten-Volume und Daten-SVM-Root-Volumes müssen sich in einem gespiegelten Aggregat befinden. Sie können diese Volumes nicht in ein nicht gespiegeltes Aggregat verschieben. Wenn sie sich auf einem nicht gespiegelten Aggregat befinden, sind über Switchover und Switchback-Vorgänge verhandelte Vorgänge gegen ein Veto eingelegt. Der Befehl MetroCluster Check gibt eine Warnung aus, wenn dies der Fall ist.

Überlegungen für nicht gespiegelte Aggregate und SVMs

SVMs sollten nur auf gespiegelten Aggregaten oder nur auf nicht gespiegelten Aggregaten konfiguriert werden. Beim Konfigurieren einer Kombination aus nicht gespiegelten und gespiegelten Aggregaten kann ein Switchover von mehr als 120 Sekunden durchgeführt werden. So kann ein Datenausfall auftreten, wenn die nicht gespiegelten Aggregate nicht online geschaltet werden.

Überlegungen für nicht gespiegelte Aggregate und SAN

In älteren Versionen als ONTAP 9.9 sollte sich eine LUN nicht auf einem nicht gespiegelten Aggregat befinden. Das Konfigurieren einer LUN auf einem nicht gespiegelten Aggregat kann zu einem Switchover von mehr als 120 Sekunden bei einem Ausfall der Daten führen.

Firewall-Nutzung an MetroCluster Standorten

Überlegungen zur Firewall-Nutzung an MetroCluster Standorten

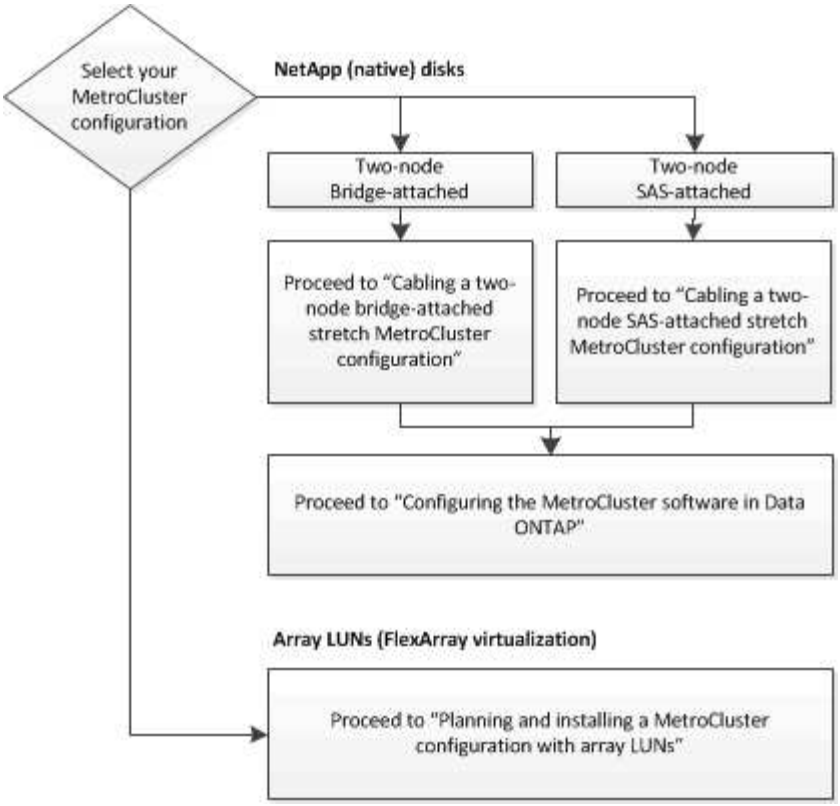
Wenn Sie eine Firewall an einem MetroCluster-Standort verwenden, müssen Sie den Zugriff auf die erforderlichen Ports sicherstellen.

Die folgende Tabelle zeigt die Verwendung von TCP/UDP-Ports in einer externen Firewall, die zwischen zwei MetroCluster-Standorten positioniert ist.

Verkehrstyp	Port/Services
Cluster-Peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP Intercluster LIFs	65200 / TCP 10006 / TCP und UDP
Hardwareunterstützung	4444 / TCP

Auswahl des richtigen Installationsverfahrens für Ihre Konfiguration

Sie müssen die korrekte Installation basierend darauf auswählen, ob Sie FlexArray LUNs verwenden und wie die Storage-Controller mit Storage-Shelfs verbinden.

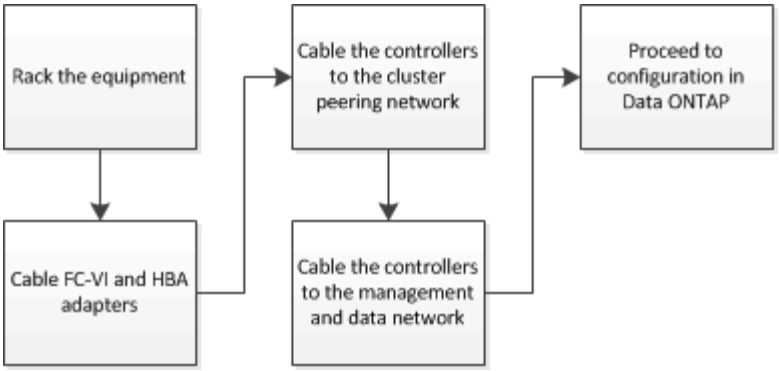


Für diesen Installationstyp…	Verwenden Sie diese Verfahren…
Stretch-Konfiguration mit zwei Nodes und FC-zu-SAS-Bridges	1. "Verkabelung einer Stretch MetroCluster Konfiguration mit zwei über Bridge angebundenen Nodes" 2. "Konfigurieren der MetroCluster-Software in ONTAP"
Stretch-Konfiguration mit zwei Nodes und Direct-Attached SAS-Verkabelung	1. "Verkabelung einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS" 2. "Konfigurieren der MetroCluster-Software in ONTAP"
Installation mit Array LUNs	"Verbindungen in Stretch-MetroCluster-Konfigurationen mit Array-LUNs"

Verkabeln Sie eine Stretch-MetroCluster-Konfiguration mit zwei SAS-Attached

Verkabelung einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS

Die MetroCluster Komponenten müssen an beiden geografischen Standorten physisch installiert, verkabelt und konfiguriert sein. Die Schritte unterscheiden sich für ein System mit nativen Festplatten-Shelfs im Gegensatz zu einem System mit Array-LUNs.



Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS

Die MetroCluster SAS-Attached-Konfiguration mit zwei Nodes erfordert mehrere Teile. Dazu gehören zwei Single-Node-Cluster, in denen die Storage-Controller über SAS-Kabel direkt mit dem Storage verbunden sind.

Die MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage-Controller sind über SAS-Kabel direkt mit dem Storage verbunden.

  Jeder Storage Controller ist als DR-Partner für einen Storage Controller am Standort des Partners konfiguriert.

  - Kupfer-SAS-Kabel können für kürzere Entfernungen verwendet werden.
  - Optische SAS-Kabel können über größere Entfernungen verwendet werden.

  > Bei Systemen mit E-Series Array-LUNs können die Storage-Controller direkt mit den E-Series Storage-Arrays verbunden werden. Bei anderen Array LUNs sind Verbindungen über FC-Switches erforderlich.

  "NetApp Interoperabilitäts-Matrix-Tool"

  Im IMT können Sie im Feld Storage-Lösung die Auswahl Ihrer MetroCluster Lösung verwenden. Sie verwenden den **Komponenten-Explorer**, um die Komponenten und die ONTAP-Version auszuwählen, um Ihre Suche zu verfeinern. Klicken Sie auf **Ergebnisse anzeigen**, um die Liste der unterstützten Konfigurationen anzuzeigen, die den Kriterien entsprechen.

- Cluster-Peering-Netzwerk

  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der SVM-Konfiguration (Storage Virtual Machine). Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.

Erforderliche MetroCluster Hardwarekomponenten und Benennungsrichtlinien für Stretch-Konfigurationen mit zwei Nodes über SAS

Die MetroCluster-Konfiguration erfordert eine Vielzahl von Hardwarekomponenten. Für Einfachheit und Klarheit werden in der gesamten MetroCluster-Dokumentation Standardnamen für Komponenten verwendet. Ein Standort wird als Standort A

bezeichnet, der andere Standort wird als Standort B bezeichnet

Unterstützte Software und Hardware

Hardware und Software müssen für die MetroCluster FC-Konfiguration unterstützt werden.

"NetApp Hardware Universe"

Beim Einsatz von AFF Systemen müssen alle Controller-Module in der MetroCluster Konfiguration als AFF Systeme konfiguriert sein.

Hardwareredundanz in der MetroCluster Konfiguration

Aufgrund der Hardware-Redundanz in der MetroCluster Konfiguration gibt es an jedem Standort zwei jeder Komponenten. Den Standorten werden die Buchstaben A und B willkürlich zugeordnet und den einzelnen Komponenten werden die Zahlen 1 und 2 willkürlich zugeordnet.

ONTAP Cluster mit zwei Single-Node-Clustern

Für die Stretch-MetroCluster Konfiguration über SAS ist zwei Single-Node-ONTAP Cluster erforderlich.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
- Standort B: Cluster_B

Zwei Storage Controller-Module

Die SAS-Attached Stretch MetroCluster Konfiguration erfordert zwei Storage Controller-Module.

- Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.
- Alle Controller-Module in der MetroCluster Konfiguration müssen dieselbe Version von ONTAP ausführen.
- Alle Controller-Module in einer DR-Gruppe müssen aus dem gleichen Modell sein.
- Alle Controller-Module in einer DR-Gruppe müssen dieselbe FC-VI-Konfiguration verwenden.

  Einige Controller Module unterstützen zwei Optionen für FC-VI-Konnektivität:

  - Integrierte FC-VI-Ports
  - Eine FC-VI-Karte in Steckplatz 1

    Ein Mix aus einem Controller-Modul mit integrierten FC-VI-Ports und einem anderen Controller-Modul mit einer zusätzlichen FC-VI-Karte wird nicht unterstützt. Wenn beispielsweise ein Node integrierte FC-VI-Konfiguration verwendet, müssen alle anderen Nodes in der DR-Gruppe auch integrierte FC-VI-Konfigurationen verwenden.

Beispielnamen:

- Standort A: Controller_A_1
- Standort B: Controller_B_1

Mindestens vier SAS-Platten-Shelves (empfohlen)

Bei der SAS-Attached Stretch MetroCluster Konfiguration sind mindestens zwei SAS-Festplatten-Shelfs erforderlich. Wir empfehlen vier SAS-Platten-Shelves.

Es werden zwei Shelves an jedem Standort empfohlen, damit die Festplatteneigentümer pro Shelf sind. Es wird mindestens ein Shelf an jedem Standort unterstützt.

Beispielnamen:

- Standort A:
  - Shelf_A_1_1
  - Shelf_A_1_2
- Standort B:
  - Shelf_B_1_1
  - Shelf_B_1_2

Mischen von IOM12 und IOM 6 Modulen in einem Stack

Ihre Version von ONTAP muss Shelf-Mix unterstützen. Informieren Sie sich im Interoperabilitäts-Matrix-Tool (IMT), ob Ihre Version von ONTAP Shelf-Mischungen unterstützt. "NetApp Interoperabilität"

Weitere Informationen zum Anmischen von Regalen finden Sie unter: "Hot-Adding-Shelfs mit IOM12-Modulen werden in einem Shelf-Stack mit IOM6-Modulen ausgeführt"

MetroCluster-Komponenten für Stretch-Konfigurationen mit zwei Nodes installieren und verkabeln

Installation und Verkabelung von MetroCluster Komponenten für Stretch-Konfigurationen mit zwei Nodes über SAS

Die Storage-Controller müssen mit den Storage-Medien und miteinander verbunden werden. Die Storage-Controller müssen außerdem mit dem Daten- und Management-Netzwerk verbunden sein.

Bevor Sie mit einem Verfahren in diesem Dokument beginnen

Vor Abschluss dieser Aufgabe müssen die folgenden Gesamtanforderungen erfüllt werden:

- Vor der Installation müssen Sie sich zunächst mit Überlegungen und Best Practices zur Installation und Verkabelung von Platten-Shelfs für Ihr Festplatten-Shelf-Modell vertraut machen.
- Alle MetroCluster Komponenten müssen unterstützt werden.

  "NetApp Interoperabilitäts-Matrix-Tool"

  Im IMT können Sie im Feld Storage-Lösung die Auswahl Ihrer MetroCluster Lösung verwenden. Verwenden Sie den * Component Explorer*, um die Komponenten und die ONTAP-Version auszuwählen, um Ihre Suche zu verfeinern. Klicken Sie auf **Ergebnisse anzeigen**, um die Liste der unterstützten Konfigurationen anzuzeigen, die den Kriterien entsprechen.

Über diese Aufgabe

- Die Begriffe Node und Controller werden synonym verwendet.

Die Hardwarekomponenten in den Rack führen

Wenn Sie noch nicht die bereits in den Schränken installierten Geräte erhalten haben, müssen Sie die Komponenten in einem Rack unterbringen.

Dieser Task muss auf beiden MetroCluster-Sites ausgeführt werden.

Schritte

1. Planen Sie die Positionierung der MetroCluster Komponenten.

   Die erforderliche Rack-Fläche hängt vom Plattformmodell der Storage Controller, den Switch-Typen und der Anzahl von Festplatten-Shelf-Stacks in Ihrer Konfiguration ab.

2. Durch die Verwendung von Standardpraktiken in der Werkstatt für die Arbeit mit elektrischen Geräten stellen Sie sicher, dass Sie ordnungsgemäß geerdet sind.
3. Die Storage Controller im Rack oder Schrank einbauen.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Installieren Sie die Festplatten-Shelfs, schalten Sie die Festplatten-Shelfs in den einzelnen Stacks ein, und legen Sie die Shelf-IDs fest.

   Informationen über das Verketten von Platten-Shelfs und das Festlegen von Shelf-IDs finden Sie im entsprechenden Leitfaden für Ihr Festplatten-Shelf-Modell.

   > Shelf-IDs müssen für jedes SAS-Festplatten-Shelf innerhalb jeder MetroCluster DR-Gruppe (einschließlich beider Standorte) eindeutig sein. Wenn Sie Shelf-IDs manuell einstellen, müssen Sie das Festplatten-Shelf aus- und wieder einschalten.

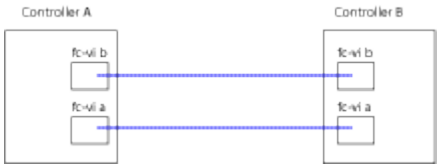
Verkabelung der Controller untereinander und den Storage Shelfs

Die FC-VI-Controller-Adapter müssen direkt miteinander verbunden sein. Die Controller-SAS-Ports müssen sowohl mit den Remote- als auch mit den lokalen Storage-Stacks verbunden werden.

Dieser Vorgang muss an beiden MetroCluster-Standorten durchgeführt werden.

Schritte

1. FC-VI-Ports verkabeln.

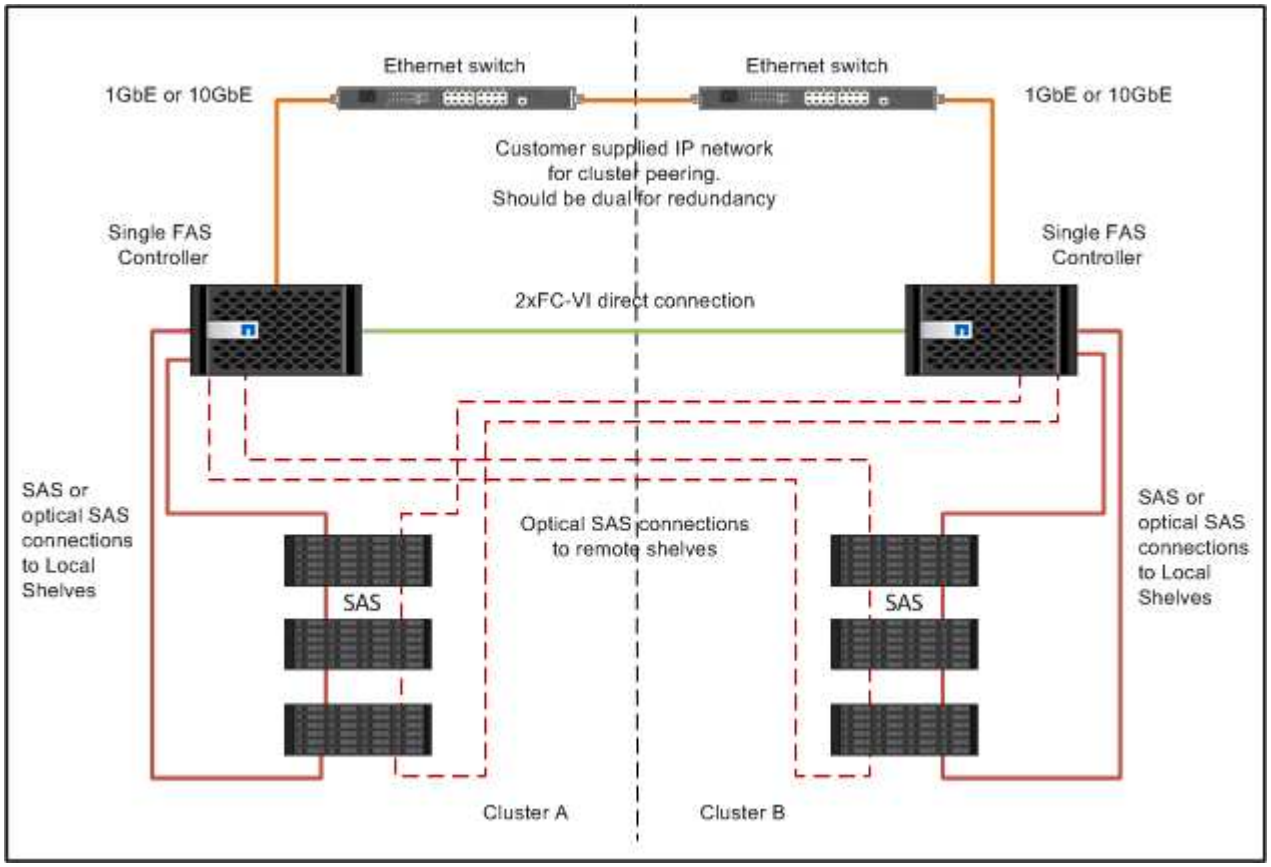
   

   Die obige Abbildung ist ein typischer repräsentativer Kabelanschluss. Die spezifischen FC-VI-Ports variieren je nach Controller-Modul.

- Die Controller-Module FAS8200 und AFF A300 können mit einer der zwei Optionen für FC-VI-Konnektivität bestellt werden:
  - Die Onboard-Ports 0e und 0f sind im FC-VI-Modus konfiguriert.
  - Die Ports 1a und 1b auf einer FC-VI-Karte werden in Steckplatz 1 gespeichert.
- Die Controller-Module des AFF A700 und der FAS9000 Storage-Systeme verwenden jeweils vier FC-VI-Ports.
- Die Controller-Module des AFF A400 und FAS8300 verwenden FC-VI-Ports 2a und 2b.

2. Verkabeln Sie die SAS-Ports.

   Die folgende Abbildung zeigt die Verbindungen. Ihre Port-Verwendung kann sich abhängig von den verfügbaren SAS- und FC-VI-Ports auf dem Controller-Modul unterscheiden.



Verkabeln der Cluster-Peering-Verbindungen

Sie müssen die für Cluster-Peering verwendeten Controller-Modul-Ports verkabeln, damit sie Verbindungen zum Cluster an ihrem Partnerstandort haben.

Diese Aufgabe muss für jedes Controller-Modul der MetroCluster-Konfiguration ausgeführt werden.

Mindestens zwei Ports auf jedem Controller-Modul sollten für Cluster-Peering verwendet werden.

Die empfohlene minimale Bandbreite für die Ports und Netzwerkkonnektivität ist 1 GbE.

Schritte

1. Identifizieren und verkabeln Sie mindestens zwei Ports für Cluster-Peering und vergewissern Sie sich,

dass sie über eine Netzwerkverbindung mit dem Partner-Cluster verfügen.

Cluster-Peering kann auf dedizierten Ports oder auf Daten-Ports durchgeführt werden. Durch den Einsatz von dedizierten Ports wird ein höherer Durchsatz für den Cluster Peering-Datenverkehr erzielt.

"Express-Konfiguration für Cluster und SVM-Peering"

Verkabelung der Management- und Datenverbindungen

Sie müssen die Management- und Daten-Ports in jedem Storage Controller mit den Standortnetzwerken verkabeln.

Diese Aufgabe muss für jeden neuen Controller an beiden MetroCluster Standorten wiederholt werden.

Sie können den Controller und die Cluster Switch Management-Ports mit den vorhandenen Switches im Netzwerk verbinden. Zusätzlich können Sie den Controller mit neuen dedizierten Netzwerk-Switches wie den NetApp CN1601 Cluster-Management-Switches verbinden.

Schritte

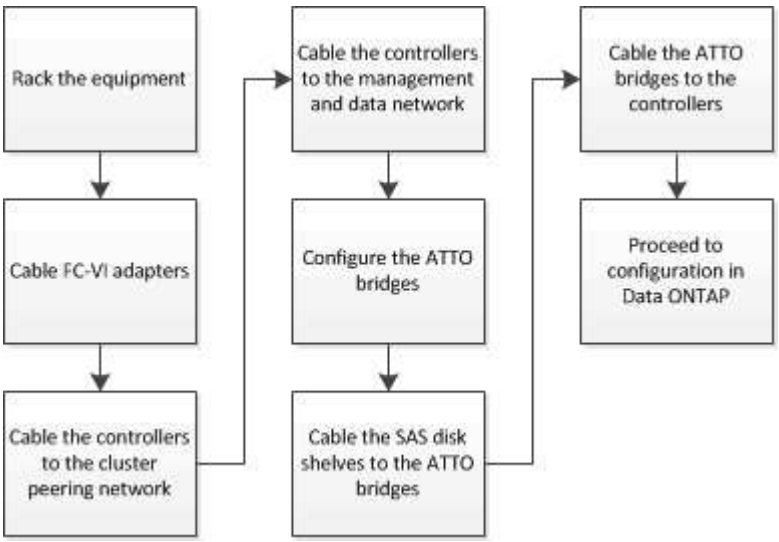
1. Verkabeln Sie die Management- und Daten-Ports des Controllers mit den Management- und Datennetzwerken am lokalen Standort.

   "Dokumentation zu ONTAP Hardwaresystemen"

Verkabeln einer Stretch-MetroCluster-Konfiguration mit zwei über Bridge verbundenen Nodes

Verkabelung einer Stretch MetroCluster Konfiguration mit zwei über Bridge angebundenen Nodes

Die MetroCluster Komponenten müssen an beiden geografischen Standorten physisch installiert, verkabelt und konfiguriert sein. Die Schritte unterscheiden sich für ein System mit nativen Festplatten-Shelfs im Gegensatz zu einem System mit Array-LUNs.



Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über eine Bridge

Bei der Planung der MetroCluster Konfiguration sollten Sie sich mit den einzelnen Komponenten der Konfiguration und deren Zusammenspiel vertraut machen.

Die MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage Controller sind nicht direkt mit dem Storage verbunden, sondern mit FC-to-SAS-Bridges verbunden. Die Storage-Controller sind über FC-Kabel zwischen den FC-VI-Adaptern der einzelnen Controller miteinander verbunden.

  Jeder Storage Controller ist als DR-Partner für einen Storage Controller am Standort des Partners konfiguriert.

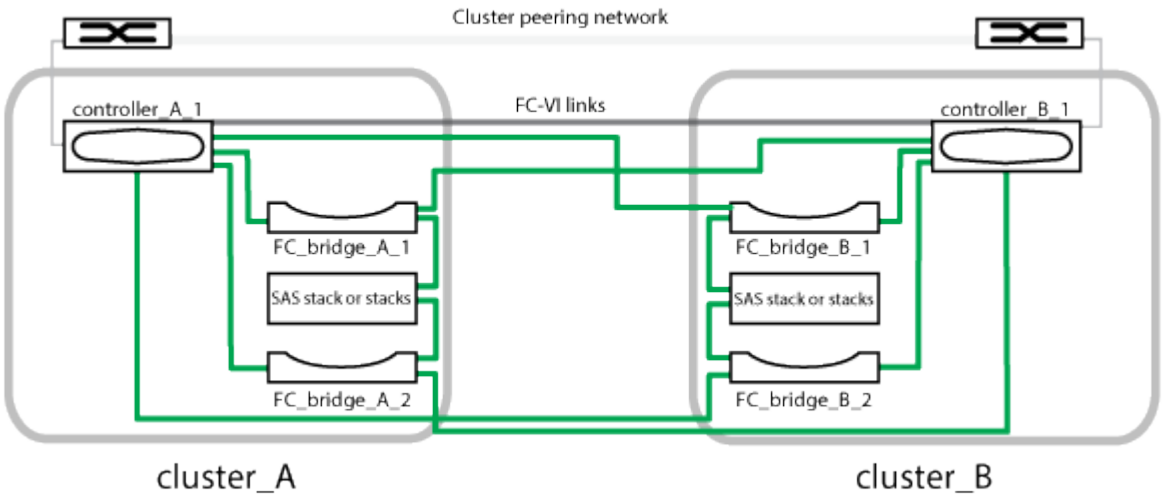
- FC-to-SAS-Bridges

  Die FC-to-SAS-Bridges verbinden die SAS-Storage-Stacks mit den FC-Initiator-Ports auf den Controllern und sorgen somit für den Überbrückung zwischen den beiden Protokollen.

- Cluster-Peering-Netzwerk

  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der SVM-Konfiguration (Storage Virtual Machine). Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.

Die folgende Abbildung zeigt eine vereinfachte Ansicht der MetroCluster Konfiguration. Bei einigen Verbindungen stellt eine einzelne Leitung mehrere redundante Verbindungen zwischen den Komponenten dar. Verbindungen zu Daten und Management-Netzwerken werden nicht angezeigt.



- Die Konfiguration besteht aus zwei Single-Node-Clustern.
- Jeder Standort verfügt über einen oder mehrere SAS-Storage-Stacks.

  SAS-Shelves in MetroCluster-Konfigurationen werden mit ACP-Verkabelung nicht unterstützt.

  Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt.

Erforderliche MetroCluster Hardwarekomponenten und Namenskonventionen für über Bridge angeschlossene Stretch-Konfigurationen mit zwei Nodes

Bei der Planung der MetroCluster-Konfiguration müssen Sie die erforderlichen und unterstützten Hardware- und Software-Komponenten kennen. Für Einfachheit und Klarheit sollten Sie auch die Namenskonventionen verstehen, die für Komponenten in Beispielen in der gesamten Dokumentation verwendet werden. Ein Standort wird beispielsweise als Standort A bezeichnet, der andere Standort wird als Standort B bezeichnet

Unterstützte Software und Hardware

Hardware und Software müssen für die MetroCluster FC-Konfiguration unterstützt werden.

"NetApp Hardware Universe"

Beim Einsatz von AFF Systemen müssen alle Controller-Module in der MetroCluster Konfiguration als AFF Systeme konfiguriert sein.

Hardwareredundanz in der MetroCluster Konfiguration

Aufgrund der Hardware-Redundanz in der MetroCluster Konfiguration gibt es an jedem Standort zwei Komponenten. Den Standorten werden die Buchstaben A und B willkürlich zugeordnet und den einzelnen Komponenten werden die Zahlen 1 und 2 willkürlich zugeordnet.

Bedarf an ONTAP Single-Node Clustern

Für die Stretch-MetroCluster Konfiguration über Bridge sind zwei Single-Node-ONTAP-Cluster erforderlich.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
- Standort B: Cluster_B

Anforderung von zwei Storage Controller-Modulen

Die Bridge-Attached Stretch-MetroCluster-Konfiguration erfordert zwei Storage Controller-Module.

Die Controller müssen die folgenden Anforderungen erfüllen:

- Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.
- Alle Controller-Module in der MetroCluster Konfiguration müssen dieselbe Version von ONTAP ausführen.
- Alle Controller-Module in einer DR-Gruppe müssen aus dem gleichen Modell sein.
- Alle Controller-Module in einer DR-Gruppe müssen dieselbe FC-VI-Konfiguration verwenden.

  Einige Controller Module unterstützen zwei Optionen für FC-VI-Konnektivität:

  - Integrierte FC-VI-Ports
  - Eine FC-VI-Karte in Steckplatz 1

Ein Mix aus einem Controller-Modul mit integrierten FC-VI-Ports und einem anderen Controller-Modul mit einer zusätzlichen FC-VI-Karte wird nicht unterstützt. Wenn beispielsweise ein Node integrierte FC-VI-Konfiguration verwendet, müssen alle anderen Nodes in der DR-Gruppe auch integrierte FC-VI-Konfigurationen verwenden.

Beispielnamen:

- Standort A: Controller_A_1
- Standort B: Controller_B_1

Notwendigkeit für FC-to-SAS-Bridges

Die Stretch MetroCluster-Konfiguration über die Bridge erfordert an jedem Standort zwei oder mehr FC-to-SAS-Bridges.

Diese Brücken verbinden die SAS-Platten-Shelfs mit den Controller-Modulen.

> FibreBridge 6500N-Brücken werden in Konfigurationen mit ONTAP 9.8 und höher nicht unterstützt.

- FibreBridge 7600N und 7500N-Brücken unterstützen bis zu vier SAS-Stacks.
- Jeder Stack kann verschiedene IOM-Modelle verwenden, allerdings müssen alle Shelfs in einem Stack dasselbe Modell verwenden.

  Die unterstützten IOM-Modelle hängen von der ONTAP-Version ab, die Sie ausführen.

- Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Die vorgeschlagenen Namen, die in diesem Verfahren als Beispiele verwendet werden, identifizieren das Controller-Modul, mit dem die Bridge eine Verbindung herstellt, und den Port.

Beispielnamen:

- Standort A:
  - Bridge_A_1_*port-number*
  - Bridge_A_2_*port-number*
- Standort B:
  - Bridge_B_1_*port-number*
  - Bridge_B_2_*port-number*

Anforderung für mindestens vier SAS-Shelves (empfohlen)

Für die Stretch MetroCluster-Konfiguration über Bridge ist mindestens zwei SAS Shelfs erforderlich. Es werden jedoch zwei Shelves an jedem Standort empfohlen, damit die Festplatteneigentümer auf Shelf-Basis ausgeführt werden können, also insgesamt vier SAS Shelfs.

Es wird mindestens ein Shelf an jedem Standort unterstützt.

Beispielnamen:

- Standort A:
  - Shelf_A_1_1
  - Shelf_A_1_2
- Standort B:
  - Shelf_B_1_1
  - Shelf_B_1_2

Mischen von IOM12 und IOM 6 Modulen in einem Stack

Ihre Version von ONTAP muss Shelf-Mix unterstützen. Informieren Sie sich im Interoperabilitäts-Matrix-Tool (IMT), ob Ihre Version von ONTAP Shelf-Mischungen unterstützt. "NetApp Interoperabilität"

Weitere Informationen zum Anmischen von Regalen finden Sie unter: "Hot-Adding-Shelfs mit IOM12-Modulen werden in einem Shelf-Stack mit IOM6-Modulen ausgeführt"

Arbeitsblatt zur Informationssammlung für FC-to-SAS-Bridges

Bevor Sie mit der Konfiguration von MetroCluster-Standorten beginnen, sollten Sie die erforderlichen Konfigurationsinformationen erfassen.

Standort A, FC-to-SAS-Bridge 1 (FC_Bridge_A_1a)

Jeder SAS-Stack benötigt mindestens zwei FC-to-SAS-Bridges.

Jede Bridge stellt eine Verbindung zu Controller_A_1_ her*port-number* Und Controller_B_1_*port-number*.

Standort A	Ihr Wert
Bridge_A_1a-IP-Adresse	
Bridge_A_1a-Benutzername	
Bridge_A_1a-Passwort	

Standort A, FC-to-SAS-Bridge 2 (FC_Bridge_A_1b)

Jeder SAS-Stack benötigt mindestens zwei FC-to-SAS-Bridges.

Jede Bridge stellt eine Verbindung zu Controller_A_1_ her*port-number* Und Controller_B_1_*port-number*.

Standort A	Ihr Wert
Bridge_A_1b IP-Adresse	
Bridge_A_1b Benutzername	
Bridge_A_1b Passwort	

Standort B, FC-to-SAS-Bridge 1 (FC_Bridge_B_1a)

Jeder SAS-Stack benötigt mindestens zwei FC-to-SAS-Bridges.

Jede Bridge stellt eine Verbindung zu Controller_A_1_`*Port-Nummer_*` *und Controller_B_1_*`Port-Nummer__` her.

Standort B	Ihr Wert
Bridge_B_1a-IP-Adresse	
Bridge_B_1a-Benutzername	
Bridge_B_1a-Passwort	

Standort B, FC-to-SAS-Bridge 2 (FC_Bridge_B_1b)

Jeder SAS-Stack benötigt mindestens zwei FC-to-SAS-Bridges.

Jede Bridge stellt eine Verbindung zu Controller_A_1_`*Port-Nummer_*` *und Controller_B_1_*`Port-Nummer__` her.

Standort B	Ihr Wert
Bridge_B_1b IP-Adresse	
Bridge_B_1b Benutzername	
Bridge_B_1b Passwort	

Installieren und verkabeln Sie MetroCluster-Komponenten

Die Hardwarekomponenten in den Rack führen

Wenn Sie noch nicht die bereits in den Schränken installierten Geräte erhalten haben, müssen Sie die Komponenten in einem Rack unterbringen.

Dieser Task muss auf beiden MetroCluster-Sites ausgeführt werden.

Schritte

1. Planen der Positionierung der MetroCluster Komponenten

   Die Rack-Fläche hängt vom Plattformmodell der Storage Controller, den Switch-Typen und der Anzahl der Festplatten-Shelf-Stacks in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Die Storage Controller im Rack oder Schrank einbauen.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Installieren Sie die Festplatten-Shelfs, schalten Sie sie ein und legen Sie die Shelf-IDs fest.
   - Sie müssen jedes Festplatten-Shelf aus- und wieder einschalten.
   - Shelf-IDs müssen für jedes SAS-Festplatten-Shelf innerhalb jeder MetroCluster DR-Gruppe (einschließlich beider Standorte) eindeutig sein.
5. Installieren Sie jede FC-to-SAS Bridge:

   a. Befestigen Sie die „L“-Halterungen an der Vorderseite der Brücke an der Vorderseite des Racks (bündige Montage) mit den vier Schrauben.

      Die Öffnungen in den Brückenhalterungen „L“ sind mit dem Standard-Rack ETA-310-X für 19-Zoll (482.6 mm) Racks kompatibel.

      Weitere Informationen und eine Abbildung der Installation finden Sie im *ATTO FibreBridge Installations- und Bedienungshandbuch für Ihr Bridge-Modell*.

   b. Schließen Sie jede Brücke an eine Stromquelle an, die eine richtige Masse liefert.

   c. Schalten Sie die einzelnen Brücken ein.

      > Für eine maximale Ausfallsicherheit müssen Brücken, die mit demselben Stack an Platten-Shelfs verbunden sind, mit unterschiedlichen Stromquellen verbunden werden.

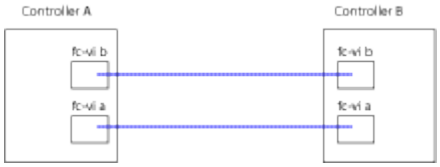
   Die LED „Bridge Ready“ kann bis zu 30 Sekunden in Anspruch nehmen, was darauf hinweist, dass die Bridge ihre Selbsttestsequenz beim Einschalten abgeschlossen hat.

Verkabeln Sie die Controller miteinander

Die FC-VI-Adapter jedes Controllers müssen direkt mit seinem Partner verbunden sein.

Schritte

1. FC-VI-Ports verkabeln.



   Die obige Abbildung ist eine typische Darstellung der erforderlichen Verkabelung. Die spezifischen FC-VI-Ports variieren je nach Controller-Modul.

   - Die Controller-Module AFF A300 und FAS8200 können mit einer der zwei Optionen für die FC-VI-Konnektivität bestellt werden:
     - Die integrierten Ports 0e und 0f sind im FC-VI-Modus konfiguriert.
     - Die Ports 1a und 1b auf einer FC-VI-Karte in Steckplatz 1.
   - Die Controller-Module des AFF A700 und der FAS9000 Storage-Systeme verwenden jeweils vier FC-VI-Ports.

Verkabeln der Cluster-Peering-Verbindungen

Sie müssen die für Cluster-Peering verwendeten Controller-Modul-Ports verkabeln, damit

sie Verbindungen zum Cluster an ihrem Partnerstandort haben.

Diese Aufgabe muss für jedes Controller-Modul der MetroCluster-Konfiguration ausgeführt werden.

Mindestens zwei Ports auf jedem Controller-Modul sollten für Cluster-Peering verwendet werden.

Die empfohlene minimale Bandbreite für die Ports und Netzwerkkonnektivität ist 1 GbE.

Schritte

1. Identifizieren und verkabeln Sie mindestens zwei Ports für Cluster-Peering und vergewissern Sie sich, dass sie über eine Netzwerkverbindung mit dem Partner-Cluster verfügen.

   Cluster-Peering kann auf dedizierten Ports oder auf Daten-Ports durchgeführt werden. Durch den Einsatz von dedizierten Ports wird ein höherer Durchsatz für den Cluster Peering-Datenverkehr erzielt.

   "Express-Konfiguration für Cluster und SVM-Peering"

Verkabelung der Management- und Datenverbindungen

Sie müssen die Management- und Daten-Ports in jedem Storage Controller mit den Standortnetzwerken verkabeln.

Diese Aufgabe muss für jeden neuen Controller an beiden MetroCluster Standorten wiederholt werden.

Sie können den Controller und die Cluster Switch Management-Ports mit den vorhandenen Switches im Netzwerk verbinden. Zusätzlich können Sie den Controller mit neuen dedizierten Netzwerk-Switches wie den NetApp CN1601 Cluster-Management-Switches verbinden.

Schritte

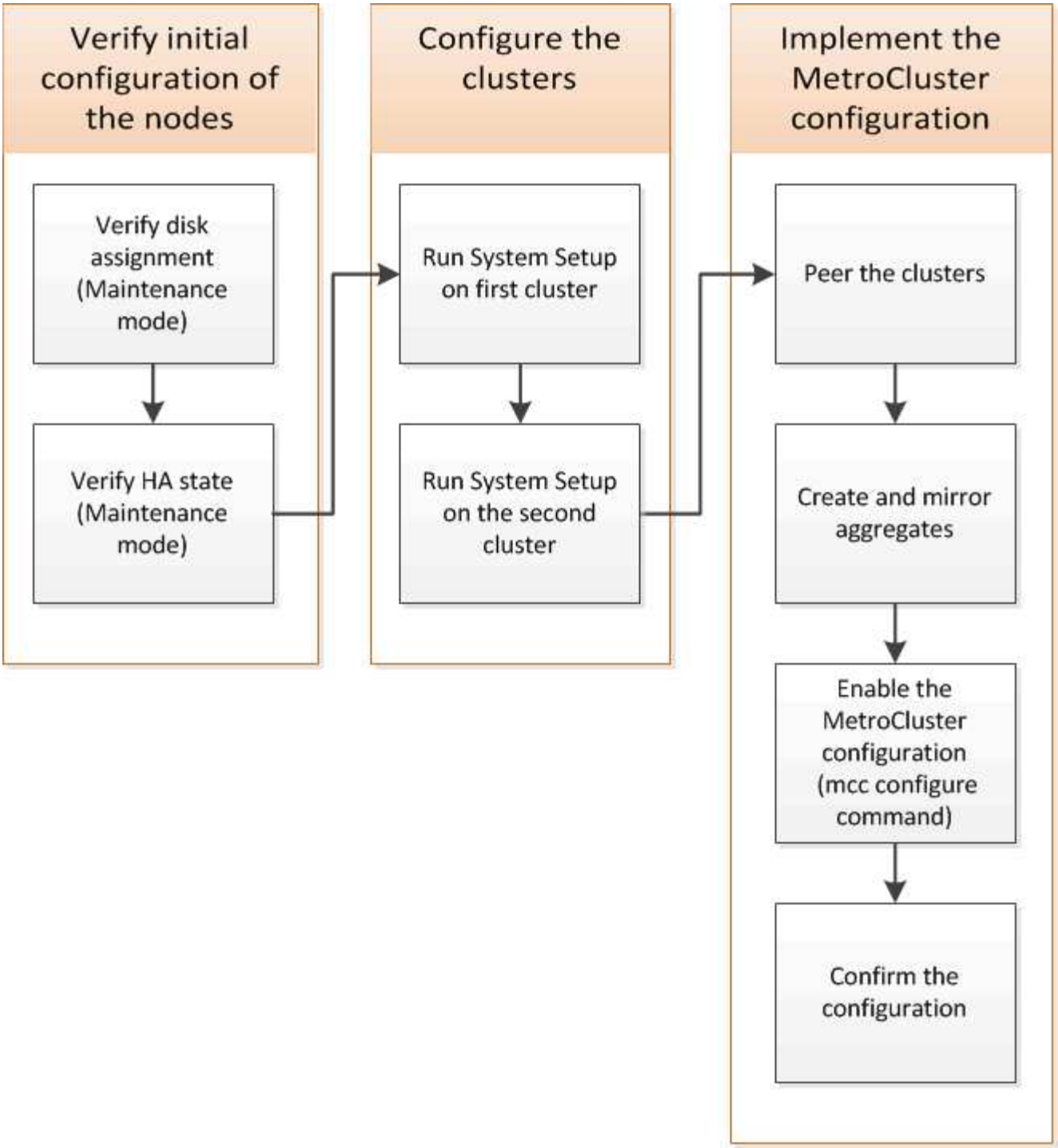
1. Verkabeln Sie die Management- und Daten-Ports des Controllers mit den Management- und Datennetzwerken am lokalen Standort.

   "Dokumentation zu ONTAP Hardwaresystemen"

= :allow-uri-read:

Konfigurieren der MetroCluster-Software in ONTAP

Sie müssen jeden Node in der MetroCluster Konfiguration in ONTAP einrichten, einschließlich der Node-Konfiguration und der Konfiguration der Nodes an zwei Standorten. Sie müssen auch die MetroCluster Beziehung zwischen beiden Standorten implementieren.



Schritte

1. Sammeln Sie die erforderlichen IP-Adressen für die Controller-Module, bevor Sie mit dem Konfigurationsprozess beginnen.
2. Füllen Sie das Arbeitsblatt für IP-Netzwerkinformationen für Standort A aus

Arbeitsblatt für IP-Netzwerkinformationen für Standort A

Vor dem Konfigurieren des Systems müssen Sie IP-Adressen und andere Netzwerkinformationen für den ersten MetroCluster-Standort (Standort A) vom Netzwerkadministrator beziehen.

Informationen zur Cluster-Erstellung von Standort A

Wenn Sie zum ersten Mal das Cluster erstellen, benötigen Sie die folgenden Informationen:

Informationstyp	Ihre Werte
Cluster-Name. Beispiel für diese Information: Site_A	
DNS-Domäne	
DNS-Name-Server	
Standort	
Administratorpasswort	

Node-Informationen zu Standort A

Für jeden Node im Cluster benötigen Sie eine Management-IP-Adresse, eine Netzwerkmaske und ein Standard-Gateway.

Knoten	Port	IP-Adresse	Netzwerkmaske	Standard-Gateway
Knoten 1: Beispiel, das in diesen Informationen verwendet wird: Controller_A_1				
Knoten 2: Nicht erforderlich, wenn eine MetroCluster Konfiguration mit zwei Nodes verwendet wird (ein Node an jedem Standort). Beispiel, das in diesen Informationen verwendet wird: Controller_A_2				

Standort A LIFs und Ports für Cluster-Peering

Sie benötigen für jeden Node im Cluster die IP-Adressen zweier Intercluster-LIFs, einschließlich einer Netzwerkmaske und eines Standard-Gateway. Die Intercluster-LIFs werden verwendet, um die Cluster miteinander zu begleichen.

Knoten	Port	IP-Adresse von Intercluster LIF	Netzwerkmaske	Standard-Gateway
Knoten 1 IC LIF 1				
Knoten 1 IC LIF 2				

Informationen zum Zeitserver an Standort A

Sie müssen die Zeit synchronisieren, die einen oder mehrere NTP-Zeitserver erfordert.

Knoten	Host-Name	IP-Adresse	Netzwerkmaske	Standard-Gateway
NTP-Server 1				
NTP-Server 2				

Standort A nbsp; AutoSupport-Informationen

Sie müssen AutoSupport für jeden Node konfigurieren. Dazu sind folgende Informationen erforderlich:

Informationstyp		Ihre Werte
Von E-Mail-Adresse		Mail-Hosts
IP-Adressen oder Namen		Transportprotokoll
HTTP, HTTPS ODER SMTP		Proxy-Server
	E-Mail-Adressen oder Verteilerlisten des Empfängers	Mitteilungen in voller Länge
	Präzise Nachrichten	

SP-Informationen an Standort A

Sie müssen für die Fehlerbehebung und Wartung den Zugriff auf den Service-Prozessor (SP) jedes Node aktivieren. Hierfür sind für jeden Node die folgenden Netzwerkinformationen erforderlich:

Knoten	IP-Adresse	Netzwerkmaske	Standard-Gateway
Knoten 1			

Arbeitsblatt für IP-Netzwerkinformationen für Standort B

Vor dem Konfigurieren des Systems müssen Sie IP-Adressen und andere Netzwerkinformationen für den zweiten MetroCluster-Standort (Standort B) vom Netzwerkadministrator beziehen.

Informationen zur Cluster-Erstellung von Standort B

Wenn Sie zum ersten Mal das Cluster erstellen, benötigen Sie die folgenden Informationen:

Informationstyp	Ihre Werte
Cluster-Name. Beispiel für diese Information: Site_B	
DNS-Domäne	
DNS-Name-Server	
Standort	
Administratorpasswort	

Node-Informationen zu Standort B

Für jeden Node im Cluster benötigen Sie eine Management-IP-Adresse, eine Netzwerkmaske und ein Standard-Gateway.

Knoten	Port	IP-Adresse	Netzwerkmaske	Standard-Gateway
Knoten 1: Beispiel, das in diesen Informationen verwendet wird: Controller_B_1				
Knoten 2: Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort) Beispiel, das in diesen Informationen verwendet wird: Controller_B_2				

Standort B LIFs und Ports für Cluster-Peering

Sie benötigen für jeden Node im Cluster die IP-Adressen zweier Intercluster-LIFs, einschließlich einer Netzwerkmaske und eines Standard-Gateway. Die Intercluster-LIFs werden verwendet, um die Cluster miteinander zu begleichen.

Knoten	Port	IP-Adresse von Intercluster LIF	Netzwerkmaske	Standard-Gateway
Knoten 1 IC LIF 1				
Knoten 1 IC LIF 2				

Standort B Informationen zum Zeitserver

Sie müssen die Zeit synchronisieren, die einen oder mehrere NTP-Zeitserver erfordert.

Knoten	Host-Name	IP-Adresse	Netzwerkmaske	Standard-Gateway
NTP-Server 1				
NTP-Server 2				

Standort B nbsp; AutoSupport-Informationen

Sie müssen AutoSupport für jeden Node konfigurieren. Dazu sind folgende Informationen erforderlich:

Informationstyp		Ihre Werte
Von E-Mail-Adresse		Mail-Hosts
IP-Adressen oder Namen		Transportprotokoll
HTTP, HTTPS ODER SMTP		Proxy-Server
	E-Mail-Adressen oder Verteilerlisten des Empfängers	Mitteilungen in voller Länge
	Präzise Nachrichten	

Standort B nbsp; SP-Informationen

Sie müssen den Zugriff auf den Service-Prozessor (SP) jedes Node für die Fehlerbehebung und Wartung aktivieren. Hierfür sind die folgenden Netzwerkinformationen für jeden Node erforderlich:

Knoten	IP-Adresse	Netzwerkmaske	Standard-Gateway
Knoten 1 (Controller_B_1)			

Ähnlichkeiten und Unterschiede zwischen Standard-Cluster und MetroCluster Konfigurationen

Die Konfiguration der Nodes in jedem Cluster in einer MetroCluster-Konfiguration ist ähnlich wie bei den Nodes in einem Standard-Cluster.

Die MetroCluster-Konfiguration basiert auf zwei Standard-Clustern. Physisch muss die Konfiguration symmetrisch sein, wobei jeder Node über dieselbe Hardware-Konfiguration verfügt. Außerdem müssen alle MetroCluster Komponenten verkabelt und konfiguriert werden. Die grundlegende Softwarekonfiguration für Nodes in einer MetroCluster-Konfiguration ist jedoch dieselbe wie für Nodes in einem Standard-Cluster.

Konfigurationsschritt	Standardmäßige Cluster-Konfiguration	MetroCluster-Konfiguration
Konfiguration von Management-, Cluster- und Daten-LIFs auf jedem Node	Gleiches gilt für beide Cluster-Typen	Konfigurieren Sie das Root-Aggregat.
Gleiches gilt für beide Cluster-Typen	Richten Sie das Cluster auf einem Node im Cluster ein.	Gleiches gilt für beide Cluster-Typen
Fügen Sie den anderen Node zum Cluster hinzu.	Gleiches gilt für beide Cluster-Typen	Erstellen Sie ein gespiegeltes Root-Aggregat.
Optional	Erforderlich	Peer-to-Peer-Cluster
Optional	Erforderlich	Aktivieren der MetroCluster-Konfiguration

Wiederherstellung der Systemstandards und Konfiguration des HBA-Typs auf einem Controller-Modul

Um eine erfolgreiche MetroCluster-Installation zu gewährleisten, setzen Sie die Standardeinstellungen auf den Controller-Modulen zurück und stellen sie wieder her.

Wichtig

Dies ist nur für Stretch-Konfigurationen mit FC-to-SAS-Bridges erforderlich.

Schritte

1. Geben Sie an der LOADER-Eingabeaufforderung die Umgebungsvariablen auf ihre Standardeinstellung zurück:

   ```
   set-defaults
   ```

2. Starten Sie den Knoten im Wartungsmodus, und konfigurieren Sie dann die Einstellungen für alle HBAs im System:

   a. Booten in den Wartungsmodus:

      ```
      boot_ontap maint
      ```

   b. Überprüfen Sie die aktuellen Einstellungen der Ports:

      ```
      ucadmin show
      ```

   c. Aktualisieren Sie die Porteinstellungen nach Bedarf.

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

3. Beenden des Wartungsmodus:

   ```
   halt
   ```

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

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

   ```
   boot_ontap maint
   ```

5. Überprüfen Sie die vorgenommenen Änderungen:

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

6. Beenden des Wartungsmodus:

   ```
   halt
   ```

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

7. Starten Sie den Knoten im Startmenü:

   ```
   boot_ontap menu
   ```

   Warten Sie, bis das Boot-Menü angezeigt wird, nachdem Sie den Befehl ausgeführt haben.

8. Löschen Sie die Knotenkonfiguration, indem Sie in der Eingabeaufforderung des Startmenüs „`wipeconfig`“ eingeben und dann die Eingabetaste drücken.

   Auf dem folgenden Bildschirm wird die Eingabeaufforderung des Startmenüs angezeigt:

```
Please choose one of the following:

     (1) Normal Boot.
     (2) Boot without /etc/rc.
     (3) Change password.
     (4) Clean configuration and initialize all disks.
     (5) Maintenance mode boot.
     (6) Update flash from backup config.
     (7) Install new software first.
     (8) Reboot node.
     (9) Configure Advanced Drive Partitioning.
     Selection (1-9)?  wipeconfig
 This option deletes 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?: yes
 Rebooting to finish wipeconfig request.
```

Konfigurieren von FC-VI-Ports auf einer X1132A-R6 Quad-Port-Karte auf FAS8020 Systemen

Wenn Sie die Quad-Port-Karte X1132A-R6 auf einem FAS8020 System verwenden, können Sie in den Wartungsmodus wechseln, um die 1a- und 1b-Ports für die FC-VI- und Initiatorverwendung zu konfigurieren. Dies ist für MetroCluster Systeme, die vom Werk empfangen werden, in denen die Ports für Ihre Konfiguration entsprechend eingestellt sind, nicht erforderlich.

Über diese Aufgabe

Diese Aufgabe muss im Wartungsmodus ausgeführt werden.

> Die Konvertierung eines FC-Ports in einen FC-VI-Port mit dem Befehl ucadmin wird nur auf den Systemen FAS8020 und AFF 8020 unterstützt. Das Konvertieren von FC-Ports in FCVI-Ports wird auf keiner anderen Plattform unterstützt.

Schritte

1. Deaktivieren Sie die Ports:

   ```
   storage disable adapter 1a

   storage disable adapter 1b
   ```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

2. Vergewissern Sie sich, dass die Ports deaktiviert sind:

   `ucadmin show`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

3. Setzen Sie die A- und b-Ports auf den FC-VI-Modus:

   `ucadmin modify -adapter 1a -type fcvi`

   Der Befehl setzt den Modus auf beiden Ports im Port-Paar 1a und 1b (auch wenn im Befehl nur 1a angegeben ist).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

4. Bestätigen Sie, dass die Änderung aussteht:

```
ucadmin show
```

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Fahren Sie den Controller herunter, und starten Sie dann im Wartungsmodus neu.
6. Bestätigen Sie die Konfigurationsänderung:

```
ucadmin show local
```

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

Überprüfen der Festplattenzuweisung im Wartungsmodus in einer Konfiguration mit zwei Nodes

Vor dem vollständigen Booten des Systems zu ONTAP können Sie optional das System im Wartungsmodus booten und die Festplattenzuordnung auf den Nodes überprüfen. Die Festplatten sollten eine vollständig symmetrische Konfiguration erstellen, bei der beide Standorte ihre eigenen Platten-Shelves besitzen und Daten bereitstellen, wobei jedem Knoten und jedem Pool die gleiche Anzahl von gespiegelten Festplatten zugewiesen ist.

Bevor Sie beginnen

Das System muss sich im Wartungsmodus befinden.

Über diese Aufgabe

Neue MetroCluster Systeme haben vor der Auslieferung Festplattenzuordnungen abgeschlossen.

In der folgenden Tabelle sind Beispiele für Pool-Zuweisungen für eine MetroCluster-Konfiguration aufgeführt. Festplatten werden Pools nach Shelf-Basis zugewiesen.

Festplatten-Shelf (*Beispielname*)…	An Standort…	Gehört zu…	Und ist diesem Node zugewiesen…
Festplatten-Shelf 1 (Shelf_A_1_1)	Standort A	Knoten A 1	Pool 0
Festplatten-Shelf 2 (Shelf_A_1_3)	Festplatten-Shelf 3 (Shelf_B_1_1)	Knoten B 1	Pool 1
Festplatten-Shelf 4 (Shelf_B_1_3)	Festplatten-Shelf 9 (Shelf_B_1_2)	Standort B	Knoten B 1
Pool 0	Festplatten-Shelf 10 (Shelf_B_1_4)	Platten-Shelf 11 (Shelf_A_1_2)	Knoten A 1

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs umfasst, sollten Sie die Festplatten anhand der folgenden Richtlinien für jedes Laufwerk mit 12 Festplatten manuell zuweisen:

Diese Festplatten in der Schublade zuweisen…	Zu diesem Knoten und Pool…
1 - 6	Pool des lokalen Node 0
7 - 12	Pool 1 DES DR-Partners

Dieses Muster der Festplattenzuordnung minimiert die Auswirkungen auf ein Aggregat, wenn ein Einschub offline geht.

Schritte

1. Wenn Ihr System vom Werk empfangen wurde, bestätigen Sie die Regalzuordnungen:

   ```
   disk show -v
   ```

2. Bei Bedarf können Sie den entsprechenden Pool explizit Festplatten in den angeschlossenen Platten-Shelfs zuweisen

   ```
   disk assign
   ```

   Festplatten-Shelfs an demselben Standort wie der Node werden Pool 0 zugewiesen, und Festplatten-Shelfs, die sich am Standort des Partners befinden, werden Pool 1 zugewiesen. Sie sollten jedem Pool die gleiche Anzahl von Shelfs zuweisen.

   a. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
   b. Weisen Sie auf dem Knoten vor Ort A systematisch die lokalen Platten-Shelfs dem Pool 0 und den Remote-Festplatten-Shelfs zu, um 1: + zu bündeln `disk assign -shelf *disk_shelf_name* -p *pool*`

      Wenn der Storage Controller Node_A_1 vier Shelfs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

c. Weisen Sie auf dem Knoten am Remote-Standort (Standort B) systematisch seine lokalen Festplatten-Shelfs dem Pool 0 und seinen Remote-Festplatten-Shelfs zu, um Pool 1: + zu bilden `disk assign -shelf` *`disk_shelf_name`* `-p` *`pool`*

   Wenn der Storage Controller Node_B_1 vier Shelfs hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf shelf_B_1_2   -p 0
*> disk assign -shelf shelf_B_1_4  -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
 *> disk assign -shelf shelf_B_1_3 -p 1
```

a. Zeigt die Festplatten-Shelf-IDs und Einschübe für jede Festplatte an:
   `disk show –v`

Überprüfen des HA-Status von Komponenten

In einer Stretch MetroCluster Konfiguration, die werkseitig nicht vorkonfiguriert ist, müssen Sie überprüfen, ob der HA-Zustand der Controller- und Gehäusekomponente auf „`mcc-2n`“ eingestellt ist, damit sie ordnungsgemäß hochfahren. Bei Systemen, die vom Werk empfangen werden, ist dieser Wert vorkonfiguriert, und Sie müssen ihn nicht überprüfen.

Bevor Sie beginnen

Das System muss sich im Wartungsmodus befinden.

Schritte

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

   ```
   ha-config show
   ```

   Das Controller-Modul und das Gehäuse sollten den Wert „`mcc-2n`“ aufweisen.

2. Wenn der angezeigte Systemzustand des Controllers nicht „`mcc-2n`“ lautet, stellen Sie den HA-Status für den Controller ein:

   ```
   ha-config modify controller mcc-2n
   ```

3. Wenn der angezeigte Systemzustand des Gehäuses nicht „`mcc-2n`“ lautet, stellen Sie den HA-Status für das Gehäuse ein:

   ```
   ha-config modify chassis mcc-2n
   ```

Halten Sie den Knoten an.

Warten Sie, bis der Node an der LOADER-Eingabeaufforderung wieder angezeigt wird.

4. Wiederholen Sie diese Schritte auf jedem Knoten der MetroCluster-Konfiguration.

Einrichten von ONTAP in einer MetroCluster Konfiguration mit zwei Nodes

In einer MetroCluster-Konfiguration mit zwei Nodes müssen Sie auf jedem Cluster den Node booten, den Setup-Assistenten für den Cluster beenden und den verwenden `cluster setup` Befehl zum Konfigurieren des Node in einem Single-Node-Cluster.

Bevor Sie beginnen

Sie dürfen den Service Processor nicht konfiguriert haben.

Über diese Aufgabe

Diese Aufgabe gilt für MetroCluster-Konfigurationen mit zwei Nodes, die nativen NetApp Storage verwenden.

Neue MetroCluster Systeme sind vorkonfiguriert. Sie müssen diese Schritte nicht ausführen. Sie sollten jedoch AutoSupport konfigurieren.

Diese Aufgabe muss auf beiden Clustern in der MetroCluster Konfiguration ausgeführt werden.

Weitere allgemeine Informationen zum Einrichten von ONTAP finden Sie im "Einrichtung von ONTAP"

Schritte

1. Schalten Sie den ersten Node ein.

   Sie müssen diesen Schritt auf dem Node am Disaster-Recovery-Standort (DR) wiederholen.

   Der Node bootet. Dann startet der Cluster-Setup-Assistent auf der Konsole, der Sie darüber informiert, dass AutoSupport automatisch aktiviert wird.

```
::> Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

2. Erstellen eines neuen Clusters:

   `create`

3. Wählen Sie, ob der Node als Single Node Cluster verwendet werden soll.

```
Do you intend for this node to be used as a single node cluster? {yes,
no} [yes]:
```

4. Übernehmen Sie die Standardeinstellung „`ja`“, indem Sie die Eingabetaste drücken, oder geben Sie Ihre

eigenen Werte ein, indem Sie „`no`“ eingeben und anschließend die Eingabetaste drücken.

5. Befolgen Sie die Anweisungen, um den Assistenten **Cluster Setup** abzuschließen. Drücken Sie die Eingabetaste, um die Standardwerte zu akzeptieren, oder geben Sie Ihre eigenen Werte ein, und drücken Sie dann die Eingabetaste.

   Die Standardwerte werden automatisch basierend auf Ihrer Plattform und Netzwerkkonfiguration ermittelt.

6. Nachdem Sie den **Cluster Setup**-Assistenten abgeschlossen und beendet haben, überprüfen Sie, ob der Cluster aktiv ist und der erste Knoten ordnungsgemäß ist:

   `cluster show`

   Das folgende Beispiel zeigt ein Cluster, in dem der erste Node (cluster1-01) sich in einem ordnungsgemäßen Zustand befindet und zur Teilnahme berechtigt ist:

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   cluster1-01           true    true
   ```

   Wenn eine der Einstellungen, die Sie für die Admin-SVM oder Node-SVM eingegeben haben, geändert werden muss, können Sie über den auf den Assistenten * Cluster Setup* zugreifen `cluster setup` Befehl.

Konfigurieren der Cluster in einer MetroCluster-Konfiguration

Sie müssen die Cluster Peer, die Root-Aggregate spiegeln, ein gespiegeltes Datenaggregat erstellen und dann den Befehl zum Implementieren der MetroCluster Operationen ausgeben.

Peering der Cluster

Die Cluster in der MetroCluster Konfiguration müssen sich in einer Peer-Beziehung zueinander finden, damit sie kommunizieren und die für MetroCluster Disaster Recovery essentielle Datenspiegelung durchführen können.

Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

"Überlegungen bei der Verwendung von dedizierten Ports"

"Überlegungen bei der Freigabe von Datenports"

Konfigurieren von Intercluster-LIFs

Sie müssen Intercluster-LIFs an Ports erstellen, die für die Kommunikation zwischen den MetroCluster-Partner-Clustern verwendet werden. Sie können dedizierte Ports oder Ports verwenden, die auch Datenverkehr haben.

Konfigurieren von Intercluster-LIFs auf dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare

Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerk-Ports in „`cluster01`“ angezeigt:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   ```
   network interface show -fields home-port,curr-port
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Ports „`e0e`“ und „`e0f`“ nicht zugewiesen:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port

Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Im folgenden Beispiel werden der Failover-Gruppe „`intercluster01`“ die Ports „`e0e`“ und „`e0f`“ auf der System-SVM „`cluster01`“ zugewiesen:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   `network interface failover-groups show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`
ONTAP 9.5 und früher	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „`cluster01_ic01`“ und „`cluster01_ic02`“ in der Failover-Gruppe „`intercluster01`“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface show -service-policy default-intercluster`
ONTAP 9.5 und früher	`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 und früher	`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs „`cluster01_ic01`“ und „`cluster01_ic02`“ auf dem SVM-Port „`e0e`“ an Port „`e0f`“ scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Verwandte Informationen

"Überlegungen bei der Verwendung von dedizierten Ports"

Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerk-Ports in „`cluster01`“ angezeigt:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home -node node -home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
ONTAP 9.5 und früher	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „`cluster01_ic01`“ und „`cluster01_ic02`“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface show -service-policy default-intercluster`
ONTAP 9.5 und früher	`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

ONTAP-Version	Befehl
ONTAP 9.6 und höher	`network interface show –service-policy default-intercluster -failover`

ONTAP 9.5 und früher	`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs „`cluster01_ic01`“ und „`cluster01_ic02`“ am Port „`e0c`“ über den Port „`e0d`“ scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Verwandte Informationen

"Überlegungen bei der Freigabe von Datenports"

Erstellen einer Cluster-Peer-Beziehung

Sie müssen die Cluster-Peer-Beziehung zwischen den MetroCluster Clustern erstellen.

Erstellen einer Cluster-Peer-Beziehung

Sie können das verwenden `cluster peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster. Nachdem die Peer-Beziehung erstellt wurde, können Sie ausführen `cluster peer create` Im Remote-Cluster zur Authentifizierung beim lokalen Cluster.

Bevor Sie beginnen

- Sie müssen auf jedem Node in den Clustern, die Peering durchführen, Intercluster LIFs erstellt haben.
- Die Cluster müssen ONTAP 9.3 oder höher ausführen.

Schritte

1. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Quell-Cluster:

   `cluster peer create -generate-passphrase -offer-expiration` *`MM/DD/YYYY HH:MM:SS`*`|1…7days|1…168hours -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Wenn Sie beides angeben `-generate-passphrase` Und `-peer-addrs`, Nur der Cluster, dessen Intercluster LIFs in angegeben sind `-peer-addrs` Kann das generierte Passwort verwenden.

Sie können die ignorieren `-ipspace` Option, wenn kein benutzerdefinierter IPspace verwendet wird. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung auf einem nicht angegebenen Remote-Cluster erstellt:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Authentifizierung des Quellclusters auf dem Quellcluster beim Ziel-Cluster:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird der lokale Cluster an den Remote-Cluster unter LIF-IP-Adressen 192.140.112.101 und 192.140.112.102 authentifiziert:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

3. Vergewissern Sie sich, dass die Cluster-Peer-Beziehung erstellt wurde:

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                            Cluster Serial Number: 1-80-123456
                   Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                  Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Prüfen Sie die Konnektivität und den Status der Knoten in der Peer-Beziehung:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Erstellen einer Cluster-Peer-Beziehung (ONTAP 9.2 und älter)

Sie können das verwenden `cluster peer create` Befehl zum Initiierung einer Anforderung für eine Peering-Beziehung zwischen einem lokalen und einem Remote-Cluster. Nachdem die Peer-Beziehung vom

lokalen Cluster angefordert wurde, können Sie ausführen `cluster peer create` Auf dem Remote-Cluster, um die Beziehung zu akzeptieren.

Bevor Sie beginnen

- Sie müssen auf jedem Node in den Clustern, die Peering durchführen, Intercluster LIFs erstellt haben.
- Die Clusteradministratoren müssen die Passphrase vereinbart haben, die jedes Cluster verwendet, um sich beim anderen zu authentifizieren.

Schritte

1. Erstellen Sie auf dem Ziel-Cluster für die Datensicherung eine Peer-Beziehung mit dem Quell-Cluster:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Sie können die ignorieren `-ipspace` Option, wenn kein benutzerdefinierter IPspace verwendet wird. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine Cluster-Peer-Beziehung zum Remote-Cluster bei Intercluster LIF IP-Adressen 192.168.2.201 und 192.168.2.202 erstellt:

   ```
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

2. Authentifizieren Sie das Quell-Cluster im Datensicherungs-Quellcluster beim Ziel-Cluster:

   `cluster peer create -peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird der lokale Cluster an den Remote-Cluster unter LIF-IP-Adressen 192.140.112.203 und 192.140.112.204 authentifiziert:

   ```
   cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

3. Vergewissern Sie sich, dass die Cluster-Peer-Beziehung erstellt wurde:

   `cluster peer show –instance`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. Prüfen Sie die Konnektivität und den Status der Knoten in der Peer-Beziehung:

   `cluster peer health show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

Spiegelung der Root-Aggregate

Um Datensicherung zu ermöglichen, müssen Sie die Root-Aggregate spiegeln.

Über diese Aufgabe

Standardmäßig wird das Root-Aggregat als RAID-DP Typ Aggregat erstellt. Sie können das Root-Aggregat von RAID-DP zu einem Aggregat des RAID4-Typs ändern. Mit dem folgenden Befehl wird das Root-Aggregat für das RAID4-Typ-Aggregat modifiziert:

`storage aggregate modify -aggregate` *`aggr_name`* `-raidtype raid4`

Auf Systemen anderer Hersteller kann der RAID-Typ des Aggregats von dem Standard RAID-DP zu RAID4 vor oder nach der Spiegelung des Aggregats geändert werden.

Schritte

1. Root-Aggregat spiegeln:

   `storage aggregate mirror aggr_name`

   Mit dem folgenden Befehl wird das Root-Aggregat für „`Controller_A_1`“ gespiegelt:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

2. Wiederholen Sie den vorherigen Schritt für jeden Node in der MetroCluster-Konfiguration.

Verwandte Informationen

"Logisches Storage-Management"

"ONTAP-Konzepte"

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Bevor Sie beginnen

- Sie sollten wissen, welche Laufwerke oder Array LUNs im neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.

Über diese Aufgabe

- Laufwerke und Array-LUNs sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat Eigentum desselben Node sein, der zum Home Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   `storage disk show -spare -owner node_name`

2. Erstellen Sie das Aggregat:

   `storage aggregate create -mirror true`

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem

Node im Cluster ein Aggregat erstellen. Um sicherzustellen, dass das Aggregat auf einem bestimmten Node erstellt wird, verwenden Sie die `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

Sie können die folgenden Optionen angeben:

- Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
- Liste bestimmter Laufwerke oder Array LUNs, die dem Aggregat hinzugefügt werden sollen
- Anzahl der zu einführenden Laufwerke

> In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

- Prüfsummenstil, den Sie für das Aggregat verwenden möchten
- Typ der zu verwendenden Laufwerke
- Die Größe der zu verwendenden Laufwerke
- Fahrgeschwindigkeit zu verwenden
- RAID-Typ für RAID-Gruppen auf dem Aggregat
- Maximale Anzahl an Laufwerken oder Array-LUNs, die in einer RAID-Gruppe enthalten sein können
- Weitere Informationen zu diesen Optionen finden Sie im, ob Laufwerke mit unterschiedlichen U/min zulässig sind `storage aggregate create` Man-Page.

  Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Erstellen von nicht gespiegelten Datenaggregaten

Optional können Sie nicht gespiegelte Datenaggregate für Daten erstellen, für die keine redundante Spiegelung von MetroCluster-Konfigurationen erforderlich ist.

Bevor Sie beginnen

- Sie sollten wissen, welche Laufwerke oder Array LUNs im neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie überprüfen können, ob der richtige Laufwerkstyp ausgewählt ist.

Beispiel 1. Über diese Aufgabe

ACHTUNG: Bei MetroCluster FC-Konfigurationen sind die nicht gespiegelten Aggregate erst nach einer Umschaltung online, wenn auf die Remote-Festplatten im Aggregat zugegriffen werden kann. Wenn die ISLs ausfallen, kann der lokale Knoten möglicherweise nicht auf die Daten auf den nicht gespiegelten Remote-Festplatten zugreifen. Der Ausfall eines Aggregats kann zu einem Neustart des lokalen Node führen.

Die nicht gespiegelten Aggregate müssen sich lokal an dem Node halten, auf dem sie sich enthalten.

- Laufwerke und Array-LUNs sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat Eigentum desselben Node sein, der zum Home Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- Der "Festplatten- und Aggregatmanagement" Enthält weitere Informationen zur Spiegelung von Aggregaten.

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   `storage disk show -spare -owner node_name`

2. Erstellen Sie das Aggregat:

   `storage aggregate create`

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Node erstellt wird, sollten Sie das verwenden `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste bestimmter Laufwerke oder Array LUNs, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken oder Array-LUNs, die in einer RAID-Gruppe enthalten sein können
   - Weitere Informationen zu diesen Optionen finden Sie im, ob Laufwerke mit unterschiedlichen U/min zulässig sind `storage aggregate create` Man-Page.

     Mit dem folgenden Befehl wird ein nicht gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Implementieren der MetroCluster-Konfiguration

Sie müssen den ausführen `metrocluster configure` Befehl zum Starten der Datensicherung in einer MetroCluster-Konfiguration.

Bevor Sie beginnen

- Es sollten mindestens zwei gespiegelte Datenaggregate ohne Root-Wurzeln auf jedem Cluster vorhanden sein.

  Zusätzliche Datenaggregate können entweder gespiegelt oder nicht gespiegelt werden.

  Überprüfen Sie die Aggregattypen:

  `storage aggregate show`

  > Wenn Sie ein einzelnes gespiegeltes Datenaggregat verwenden möchten, finden Sie weitere Informationen unter "Konfigurieren Sie die MCC Software in ONTAP" Weitere Anweisungen.

- Der HA-Konfigurationsstatus der Controller und des Gehäuses muss „`mcc-2n`“ sein.

Über diese Aufgabe

Sie können die ausgeben `metrocluster configure` Um die MetroCluster-Konfiguration zu aktivieren, aktivieren Sie einmal den Befehl auf einem der Nodes. Sie müssen den Befehl nicht für jede der Standorte oder Nodes ausführen. Es ist nicht von Bedeutung, auf welchem Node oder Standort Sie den Befehl ausgeben möchten.

Schritte

1. Konfigurieren Sie die MetroCluster im folgenden Format:

Wenn Ihre MetroCluster Konfiguration…	Dann tun Sie das…
Mehrere Datenaggregate	Konfigurieren Sie an der Eingabeaufforderung eines beliebigen Nodes MetroCluster: `metrocluster configure` *`node-name`*

Ein einzelnes gespiegeltes Datenaggregat	a. Ändern Sie von der Eingabeaufforderung eines beliebigen Node auf die erweiterte Berechtigungsebene:
	
	`set -privilege advanced`
	
	Sie müssen mit „`y`“ antworten, wenn Sie aufgefordert werden, in den erweiterten Modus zu wechseln, und die Eingabeaufforderung für den erweiterten Modus (*) angezeigt wird.
	
	b. Konfigurieren Sie die MetroCluster mit dem `-allow-with-one -aggregate true` Parameter:
	
	`metrocluster configure -allow-with-one-aggregate true` *`node-name`*
	
	c. Zurück zur Administrator-Berechtigungsebene:
	`set -privilege admin`

> Die Best Practice besteht in der Nutzung mehrerer Datenaggregate. Wenn die erste DR-Gruppe nur ein Aggregat hat und Sie eine DR-Gruppe mit einem Aggregat hinzufügen möchten, müssen Sie das Metadaten-Volume aus dem einzelnen Datenaggregat verschieben. Weitere Informationen zu diesem Verfahren finden Sie unter "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

Mit dem folgenden Befehl wird die MetroCluster-Konfiguration auf allen Nodes in der DR-Gruppe aktiviert, die „`Controller_A_1`“ enthält:

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

   `network port show`

   Im folgenden Beispiel wird die Verwendung von Netzwerkports angezeigt:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000

7 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.
   a. Überprüfen Sie die Konfiguration von Standort A:
      `metrocluster show`

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Überprüfen Sie die Konfiguration von Standort B:
      `metrocluster show`

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

Konfiguration von FC-to-SAS-Bridges für das Monitoring des Systemzustands

Wenn Ihre Konfiguration über FC-to-SAS-Bridges verfügt, müssen Sie bei Systemen mit ONTAP-Versionen vor 9.8 einige besondere Konfigurationsschritte durchführen, um die FC-to-SAS-Bridges in der MetroCluster-Konfiguration zu überwachen.

- SNMP-Überwachungstools anderer Anbieter werden für FibreBridge-Brücken nicht unterstützt.
- Ab ONTAP 9.8 werden FC-to-SAS-Bridges standardmäßig über in-Band-Verbindungen überwacht, keine zusätzliche Konfiguration erforderlich.

> Ab ONTAP 9.8 beginnt der `storage bridge` Befehl wird durch ersetzt `system bridge`. Die folgenden Schritte zeigen das `storage bridge` Befehl, aber wenn Sie ONTAP 9.8 oder höher ausführen, der `system bridge` Befehl ist bevorzugt.

Schritte

1. Fügen Sie von der ONTAP Cluster-Eingabeaufforderung die Bridge zur Statusüberwachung hinzu:

   a. Fügen Sie die Bridge mit dem Befehl für Ihre ONTAP-Version hinzu:

ONTAP-Version	Befehl
ONTAP 9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
ONTAP 9.4 und früher	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   b. Überprüfen Sie, ob die Bridge hinzugefügt und richtig konfiguriert wurde:

   ```
   storage bridge show
   ```

   Es kann wegen des Abrufintervalls bis zu 15 Minuten dauern, alle Daten wiederzugeben. Die ONTAP-Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „`Status`“ „`ok`“ lautet und weitere Informationen, wie der weltweite Name (WWN), angezeigt werden.

Das folgende Beispiel zeigt, dass die FC-to-SAS-Bridges konfiguriert sind:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Überprüfen der MetroCluster-Konfiguration

Sie können überprüfen, ob die Komponenten und Beziehungen in der MetroCluster Konfiguration ordnungsgemäß funktionieren. Nach der Erstkonfiguration und nach sämtlichen Änderungen an der MetroCluster-Konfiguration sollten Sie einen Check durchführen. Sie sollten auch vor einer ausgehandelten (geplanten) Umschaltung oder einem Switchback prüfen.

Wenn der `metrocluster check run` Befehl wird zweimal innerhalb kürzester Zeit auf einem oder beiden Clustern ausgegeben. Ein Konflikt kann auftreten, und der Befehl erfasst möglicherweise nicht alle Daten. Danach `metrocluster check show` Befehle zeigen nicht die erwartete Ausgabe an.

1. Überprüfen Sie die Konfiguration:

   `metrocluster check run`

   Der Befehl wird als Hintergrundjob ausgeführt und wird möglicherweise nicht sofort ausgeführt.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Detailliertere Ergebnisse anzeigen:

   ```
   metrocluster check run

   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

   Der `metrocluster check show` Befehle zeigen die Ergebnisse der letzten `metrocluster check run` Befehl. Sie sollten immer den ausführen `metrocluster check run` Befehl vor Verwendung des `metrocluster check show` Befehle, sodass die angezeigten Informationen aktuell sind.

   Das folgende Beispiel zeigt die `metrocluster check aggregate show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
```

```
                                                    ownership-state
ok
                      controller_A_1_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                      controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

18 entries were displayed.
```

Das folgende Beispiel zeigt die `metrocluster check cluster show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes. Sie zeigt an, dass die Cluster bei Bedarf bereit sind, eine ausgehandelte Umschaltung durchzuführen.

```
Last Checked On: 9/13/2017 20:47:04

Cluster                 Check                            Result
--------------------- -------------------------------- ---------
mccint-fas9000-0102
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
mccint-fas9000-0304
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
10 entries were displayed.
```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

"Netzwerk- und LIF-Management"

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor

Sie können die NetApp Support-Website besuchen und das Config Advisor-Tool herunterladen, um häufige Konfigurationsfehler zu überprüfen.

Config Advisor ist ein Tool zur Konfigurationsvalidierung und Statusüberprüfung. Sie können die Lösung sowohl an sicheren Standorten als auch an nicht sicheren Standorten zur Datenerfassung und Systemanalyse einsetzen.

> Der Support für Config Advisor ist begrenzt und steht nur online zur Verfügung.

1. Rufen Sie die Config Advisor Download-Seite auf und laden Sie das Tool herunter.

   "NetApp Downloads: Config Advisor"

2. Führen Sie Config Advisor aus, überprüfen Sie die Ausgabe des Tools und folgen Sie den Empfehlungen in der Ausgabe, um erkannte Probleme zu beheben.

Überprüfung von Umschaltung, Reparatur und Wechsel zurück

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

1. Verwenden Sie die im genannten Verfahren für die ausgehandelte Umschaltung, die Reparatur und den Wechsel zurück "Nach einem Ausfall wiederherstellen".

Sichern von Backup-Dateien der Konfiguration

Sie können einen zusätzlichen Schutz für die Backup-Dateien der Clusterkonfiguration bieten, indem Sie eine Remote-URL (entweder HTTP oder FTP) angeben, bei der die Backup-Dateien der Konfiguration zusätzlich zu den Standardstandorten im lokalen Cluster hochgeladen werden.

1. Legen Sie die URL des Remote-Ziels für die Backup-Dateien der Konfiguration fest:

   ```
   system configuration backup settings modify URL-of-destination
   ```

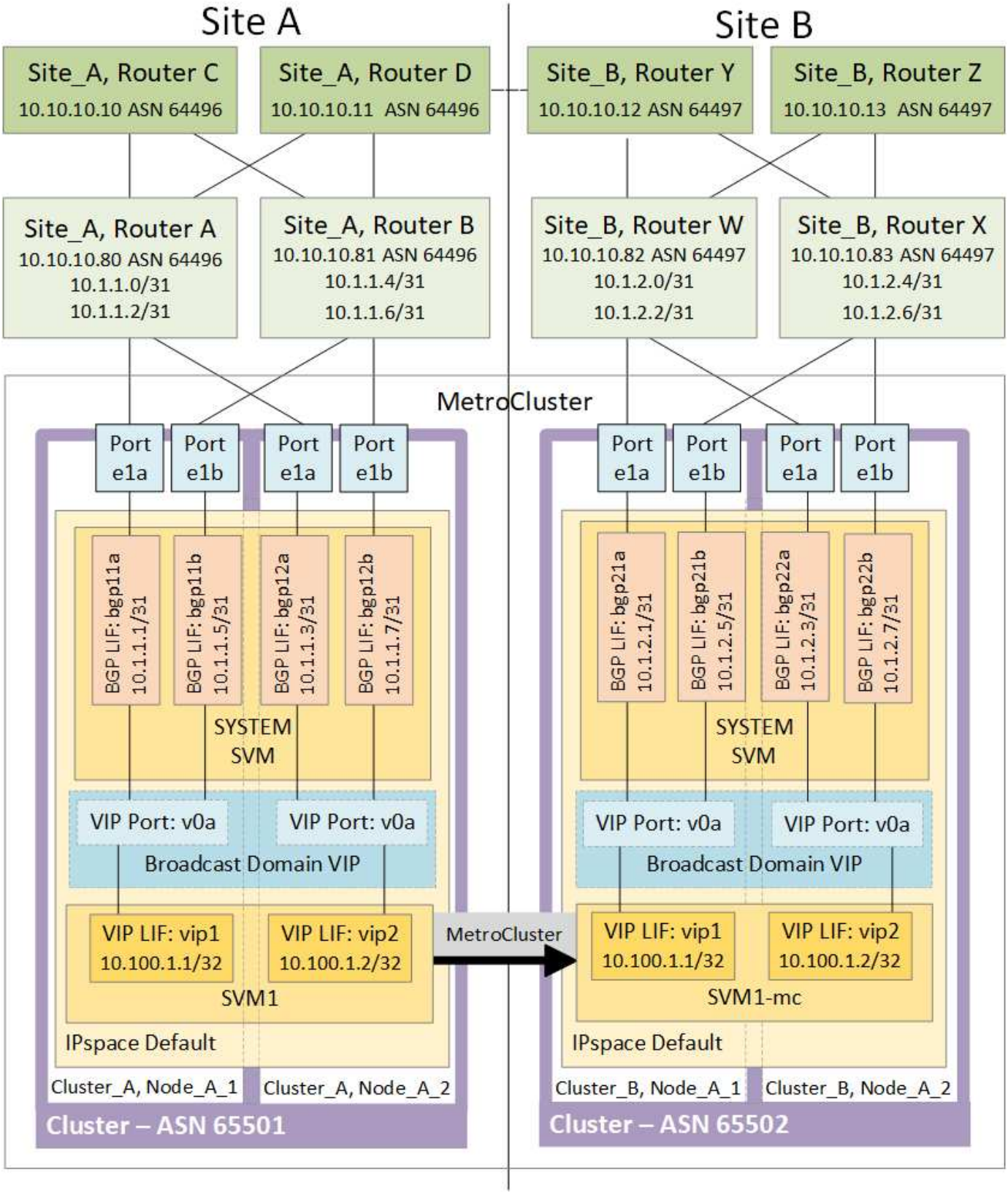
   Der "Cluster-Management mit der CLI" Enthält zusätzliche Informationen unter dem Abschnitt *Verwalten von Konfigurations-Backups*.

Überlegungen zur Verwendung von virtuellem IP- und Border-Gateway-Protokoll mit einer MetroCluster-Konfiguration

Ab ONTAP 9.5 unterstützt ONTAP Layer-3-Konnektivität mithilfe von Virtual IP (VIP) und Border Gateway Protocol (BGP). Die Kombination aus VIP und BGP für Redundanz im Front-End-Netzwerk und der Back-End MetroCluster-Redundanz bietet eine Layer 3 Disaster Recovery-Lösung.

Lesen Sie die folgenden Richtlinien und Illustrationen bei der Planung Ihrer Layer 3-Lösung. Einzelheiten zur Implementierung von VIP und BGP in ONTAP finden Sie im folgenden Abschnitt:

"Konfigurieren der virtuellen IP (VIP)-LIFs"



ONTAP Einschränkungen

ONTAP überprüft nicht automatisch, ob alle Nodes auf beiden Standorten der MetroCluster Konfiguration mit BGP-Peering konfiguriert sind.

ONTAP führt keine Route-Aggregation durch, kündigt aber alle einzelnen virtuellen LIF-IPs jederzeit als

eindeutige Host-Routen an.

ONTAP unterstützt keine True Anycast - nur ein einzelner Node im Cluster weist eine bestimmte virtuelle LIF-IP auf (wird aber von allen physischen Schnittstellen akzeptiert, unabhängig davon, ob es sich um BGP LIFs handelt, vorausgesetzt, der physische Port ist Teil des korrekten IPspace). Verschiedene LIFs können unabhängig voneinander zu unterschiedlichen Hosting-Nodes migriert werden.

Richtlinien für die Verwendung dieser Layer 3-Lösung mit einer MetroCluster-Konfiguration

Sie müssen Ihr BGP und VIP korrekt konfigurieren, um die erforderliche Redundanz zu gewährleisten.

Einfachere Bereitstellungsszenarien werden gegenüber komplexeren Architekturen bevorzugt (beispielsweise ist ein BGP Peering Router über einen zwischengeschalteten, nicht BGP Router erreichbar). ONTAP ist jedoch nicht durch Einschränkungen in Netzwerkdesign oder Topologie eingeschränkt.

VIP LIFs decken nur das Frontend-/Datennetzwerk ab.

Je nach Ihrer Version von ONTAP müssen Sie BGP Peering LIFs in der Node-SVM konfigurieren, nicht jedoch das System oder die Daten-SVM. In ONTAP 9.8 sind die BGP LIFs in der Cluster (System) SVM sichtbar und die Node-SVMs sind nicht mehr vorhanden.

Jede Daten-SVM erfordert die Konfiguration aller potenziellen First-Hop-Gateway-Adressen (normalerweise der BGP-Router, der IP-Adresse Peering), sodass der Return-Datenpfad bei einer LIF-Migration oder einem MetroCluster-Failover verfügbar ist.

BGP LIFs sind Node-spezifisch, ähnlich wie Intercluster LIFs – jeder Node verfügt über eine eindeutige Konfiguration, die nicht auf DR-Standort-Nodes repliziert werden muss.

Die Existenz der v0a (v0b und so weiter.) überprüft kontinuierlich die Konnektivität und garantiert, dass eine LIF-Migration oder ein Failover erfolgreich ist (im Gegensatz zu L2, wo eine defekte Konfiguration nur nach dem Ausfall sichtbar ist).

Ein großer Unterschied in der Architektur besteht darin, dass Clients nicht mehr dasselbe IP Subnetz wie die VIP der Daten-SVMs teilen sollten. Ein L3-Router mit den entsprechenden Resiliency- und Redundanzfunktionen der Enterprise-Klasse (z. B. VRRP/HSRP) sollte sich auf dem Weg zwischen Speicher und Clients befinden, damit der VIP ordnungsgemäß funktioniert.

Der zuverlässige Aktualisierungsprozess von BGP ermöglicht reibungslosere LIF-Migrationen, da sie geringfügig schneller sind und die Wahrscheinlichkeit einer Unterbrechung für einige Clients niedriger ist.

Sie können BGP so konfigurieren, dass einige Klassen von Netzwerk- oder Switch-Fehlverhalten schneller als LACP erkannt werden, wenn diese entsprechend konfiguriert werden.

Externe BGP (EBGP) verwendet unterschiedliche Zahlen als Nummern zwischen ONTAP-Knoten und Peering-Routern und ist die bevorzugte Bereitstellung, um die Routenaggregation und -Umverteilung auf den Routern zu vereinfachen. Interne BGP (IBGP) und die Verwendung von Routenreflektoren ist nicht unmöglich, aber außerhalb des Umfangs einer einfachen VIP-Einrichtung.

Nach der Implementierung müssen Sie prüfen, ob auf die Daten-SVM zugegriffen werden kann, wenn die zugehörige virtuelle LIF zwischen allen Nodes an jedem Standort (einschließlich MetroCluster-Umschaltung) migriert wird. So müssen Sie sicherstellen, dass die korrekte Konfiguration der statischen Routen zu derselben Daten-SVM korrekt ist.

VIP funktioniert für die meisten IP-basierten Protokolle (NFS, SMB, iSCSI).

Testen der MetroCluster-Konfiguration

Sie können Fehlerszenarien testen, um den korrekten Betrieb der MetroCluster-Konfiguration zu bestätigen.

Überprüfung der ausgehandelten Umschaltung

Sie können einen ausgehandelten (geplanten) Switchover-Vorgang testen, um die unterbrechungsfreie Datenverfügbarkeit zu bestätigen.

Dieser Test überprüft, ob sich die Datenverfügbarkeit nicht auf die Protokolle Microsoft Server Message Block (SMB) und Solaris Fibre Channel auswirkt (ausgenommen Microsoft Server Message Block), indem der Cluster in das zweite Rechenzentrum umgeschaltet wird.

Dieser Test dauert etwa 30 Minuten.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Der `metrocluster switchover` Der Befehl gibt eine Warnmeldung an.

  Wenn Sie antworten **`yes`** In der Eingabeaufforderung wechselt der Standort, von dem der Befehl ausgegeben wird, über die Partnerseite.

Für MetroCluster IP-Konfigurationen:

- Für ONTAP 9.4 und früher:
  - Gespiegelte Aggregate werden nach der ausgehandelten Umschaltung herabgestuft.
- Für ONTAP 9.5 und höher:
  - Gespiegelte Aggregate bleiben im normalen Status, wenn auf den Remote-Storage zugegriffen werden kann.
  - Gespiegelte Aggregate werden nach der ausgehandelten Umschaltung herabgesetzt, wenn der Zugriff auf den Remote-Storage verloren geht.
- Für ONTAP 9.8 und höher:
  - Nicht gespiegelte Aggregate, die sich am Disaster-Standort befinden, sind bei einem Ausfall des Remote-Storage nicht verfügbar. Dies kann zu einem Controller-Ausfall führen.

Schritte

1. Vergewissern Sie sich, dass sich alle Nodes im konfigurierten Status und im normalen Modus befinden:

   ```
   metrocluster node show
   ```

```
cluster_A::>  metrocluster node show

Cluster                         Configuration State    Mode
------------------------------- ----------------------
------------------------
 Local: cluster_A                configured             normal
Remote: cluster_B                configured             normal
```

2. Starten Sie den Switchover-Vorgang:

   `metrocluster switchover`

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Vergewissern Sie sich, dass sich das lokale Cluster im konfigurierten Zustand befindet und der Switchover-Modus aktiviert ist:

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                         Configuration State    Mode
------------------------------- ----------------------
------------------------
Local: cluster_A                 configured             switchover
Remote: cluster_B                not-reachable          -
              configured             normal
```

4. Bestätigen Sie, dass der Switchover-Vorgang erfolgreich war:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Verwenden Sie die `vserver show` Und `network interface show` Befehle, um zu überprüfen, ob DR-SVMs und LIFs online sind.

Überprüfung der Heilung und manueller Umkehrschalter

Sie können die Healing- und manuellen Switchback-Vorgänge testen, um zu überprüfen, ob die Datenverfügbarkeit nicht beeinträchtigt ist (außer bei SMB- und Solaris-FC-Konfigurationen), indem Sie nach einer ausgehandelten Umschaltung das Cluster wieder zum ursprünglichen Datacenter wechseln.

Dieser Test dauert etwa 30 Minuten.

Das erwartete Ergebnis dieses Verfahrens ist, dass Services zurück auf ihre Home-Knoten geschaltet werden sollten.

Schritte

1. Vergewissern Sie sich, dass die Heilung abgeschlossen ist:

   `metrocluster node show`

   Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

   ```
   cluster_A::> metrocluster node show
   DR                                  Configuration  DR
   Group Cluster Node                  State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   heal roots
   completed
         cluster_B
                 node_B_2         unreachable    -         switched over
   42 entries were displayed.metrocluster operation show
   ```

2. Vergewissern Sie sich, dass alle Aggregate sind `mirrored`:

   `storage aggregate show`

   Das folgende Beispiel zeigt, dass alle Aggregate einen RAID-Status der Spiegelung aufweisen:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. Booten von Nodes vom Disaster-Standort aus
4. Überprüfen Sie den Status der zurückkehrenden Wiederherstellung:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
            node_A_1            configured     enabled   heal roots
completed
      cluster_B
            node_B_2            configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

5. Führen Sie den Wechsel zurück:

   `metrocluster switchback`

   ```
   cluster_A::> metrocluster switchback
   [Job 938] Job succeeded: Switchback is successful.Verify switchback
   ```

6. Status der Knoten bestätigen:

   `metrocluster node show`

   ```
   cluster_A::> metrocluster node show
   DR                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   normal
         cluster_B
                 node_B_2         configured     enabled   normal

   2 entries were displayed.
   ```

7. Bestätigen Sie den Status:

   `metrocluster operation show`

   Die Ausgabe sollte einen erfolgreichen Status aufweisen.

   ```
   cluster_A::> metrocluster operation show
     Operation: switchback
         State: successful
    Start Time: 2/6/2016 13:54:25
      End Time: 2/6/2016 13:56:15
        Errors: -
   ```

Ausfall einer einzelnen FC-to-SAS-Bridge

Sie können den Ausfall einer einzelnen FC-to-SAS-Bridge testen, um sicherzustellen, dass es keinen Single Point of Failure gibt.

Dieser Test dauert etwa 15 Minuten.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Fehler sollten beim Ausschalten der Brücke erzeugt werden.
- Es sollte kein Failover oder Serviceverlust auftreten.
- Es ist nur ein Pfad vom Controller-Modul zu den Laufwerken hinter der Brücke verfügbar.

> Ab ONTAP 9.8 beginnt der `storage bridge` Befehl wird durch ersetzt `system bridge`. Die folgenden Schritte zeigen das `storage bridge` Befehl, aber wenn Sie ONTAP 9.8 oder höher ausführen, der `system bridge` Befehl ist bevorzugt.

Schritte

1. Schalten Sie die Netzteile der Brücke aus.
2. Vergewissern Sie sich, dass die Brückenüberwachung einen Fehler anzeigt:

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                                  Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
   Status
   ---------- ------------- ------- --------- ---------------- ---------
   -------
   ATTO_10.65.57.145
           bridge_A_1    Atto    FibreBridge 6500N
                                             200000108662d46c true
   error
   ```

3. Stellen Sie sicher, dass die Laufwerke hinter der Bridge mit einem einzigen Pfad verfügbar sind:

   `storage disk error show`

```
cluster_A::> storage disk error show
Disk             Error Type        Error Text
---------------- -----------------
---------------------------------------------
1.0.0            onedomain         1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1            onedomain         1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2            onedomain         1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23           onedomain         1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

Überprüfung des Betriebs nach Stromunterbrechung

Sie können die Antwort der MetroCluster-Konfiguration auf den Ausfall einer PDU testen.

Als Best Practice wird empfohlen, dass jede Netzteileinheit (PSU) einer Komponente mit einem separaten Netzteil verbunden wird. Wenn beide Netzteile mit derselben Stromverteilereinheit (Power Distribution Unit, PDU) verbunden sind und eine elektrische Unterbrechung auftritt, kann der Standort ausfallen und ein komplettes Shelf möglicherweise nicht mehr verfügbar sein. Der Ausfall einer Stromleitung wird getestet, um zu bestätigen, dass keine Verkabelungsabweichung besteht, die zu einer Serviceunterbrechung führen kann.

Dieser Test dauert etwa 15 Minuten.

Für diesen Test müssen alle linken PDUs und dann alle rechten PDUs an allen Racks mit den MetroCluster-Komponenten ausgeschaltet werden.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Fehler sollten beim Trennen der PDUs generiert werden.
- Es sollte kein Failover oder Serviceverlust auftreten.

Schritte

1. Schalten Sie die Stromversorgung der PDUs auf der linken Seite des Racks aus, in dem die MetroCluster-Komponenten enthalten sind.
2. Überwachen Sie das Ergebnis auf der Konsole mithilfe der `system environment sensors show -state fault` Und `storage shelf show -errors` Befehle.

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Schalten Sie das Netzteil wieder ein, und schalten Sie es wieder ein.
4. Stellen Sie sicher, dass ONTAP die Fehlerbedingung beseitigt.
5. Wiederholen Sie die vorherigen Schritte mit den rechten PDUs.

Überprüfung des Betriebs nach Ausfall eines einzelnen Storage Shelfs

Sie können den Ausfall eines einzelnen Storage Shelf testen, um sicherzustellen, dass es keinen Single Point of Failure gibt.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Eine Fehlermeldung sollte von der Überwachungssoftware gemeldet werden.
- Es sollte kein Failover oder Serviceverlust auftreten.
- Die Neusynchronisierung der Spiegelung wird automatisch nach Wiederherstellung des Hardwareausfalls gestartet.

Schritte

1. Überprüfen Sie den Status des Storage-Failovers:

```
storage failover show
```

```
cluster_A::> storage failover show

Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       true     Connected to node_A_2
node_A_2       node_A_1       true     Connected to node_A_1
2 entries were displayed.
```

2. Prüfen Sie den Aggregatstatus:

```
storage aggregate show
```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Vergewissern Sie sich, dass alle Data SVMs und Daten-Volumes online sind und Daten bereitstellen:

   `vserver show -type data`

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Ermitteln Sie ein Shelf in Pool 1 für Node Node_A_2, um ein plötzliches Hardware-Versagen zu simulieren:

   `storage aggregate show -r -node node-name !*root`

   Das ausgewählte Shelf muss Laufwerke enthalten, die Teil eines gespiegelten Datenaggregats sind.

   Im folgenden Beispiel ist das Fehlschlagen der Shelf-ID 31 ausgewählt.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                      0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                      1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.3                      1   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     1.31.4                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.5                      1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Schalten Sie das ausgewählte Shelf physisch aus.
6. Überprüfen Sie erneut den Aggregatstatus:

   ```
   storage aggregate

   storage aggregate show -r -node node_A_2 !*root
   ```

   Das Aggregat mit Laufwerken auf dem ausgeschalteten Shelf sollte über den RAID-Status „`degraded`“ verfügen, und Laufwerke auf dem betroffenen Plex sollten den Status „`failed`“ aufweisen, wie im folgenden Beispiel dargestellt:

   ```
   cluster_A::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1data01_mirrored
   ```

```
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                       0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     parity   2.30.4                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                       0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                       -   -          -  827.7GB
-  (failed)
     parity   FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Vergewissern Sie sich, dass die Daten bereitgestellt werden und alle Volumes noch online sind:

   ```
   vserver show -type data
   ```

   ```
   network interface show -fields is-home false
   ```

   ```
   volume show !vol0,!MDV*
   ```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Schalten Sie das Shelf physisch ein.

   Die Neusynchronisierung wird automatisch gestartet.

9. Überprüfen Sie, ob die Neusynchronisierung gestartet wurde:

   ```
   storage aggregate show
   ```

   Das betroffene Aggregat sollte einen RAID-Status „`reSynchronisieren`“ haben, wie im folgenden Beispiel dargestellt:

   ```
   cluster_A::> storage aggregate show
   cluster Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1_data01_mirrored
               4.15TB    3.40TB   18% online       3 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_1_root
              707.7GB   34.29GB   95% online       1 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_2_data01_mirrored
               4.15TB    4.12TB    1% online       2 node_A_2
   raid_dp,

   resyncing
   node_A_2_data02_unmirrored
               2.18TB    2.18TB    0% online       1 node_A_2
   raid_dp,

   normal
   node_A_2_root
              707.7GB   34.27GB   95% online       1 node_A_2
   raid_dp,

   resyncing
   ```

10. Überwachen Sie das Aggregat, um sicherzustellen, dass die Neusynchronisierung abgeschlossen ist:

    ```
    storage aggregate show
    ```

Das betroffene Aggregat sollte einen RAID-Status „`Normal`“ haben, wie im folgenden Beispiel dargestellt:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Verbindungen in Stretch-MetroCluster-Konfigurationen mit Array-LUNs

Verbindungen in Stretch-MetroCluster-Konfigurationen mit Array-LUNs

Bei einer Stretch-MetroCluster-Konfiguration mit Array-LUNs müssen Sie die FC-VI-Ports

über Controller hinweg verbinden. Die direkte Konnektivität zwischen den Controllern und den E-Series Storage-Arrays wird unterstützt. Für alle anderen LUN-Konfigurationen-Arrays müssen Sie in der Konfiguration FC-Switches verwenden.

Sie können auch eine Stretch-MetroCluster-Konfiguration mit Festplatten und Array-LUNs einrichten. In dieser Konfiguration müssen Sie entweder FC-to-SAS-Bridges oder SAS-optische Kabel verwenden, um die Controller mit Festplatten zu verbinden.

Beispiel einer Stretch-MetroCluster-Konfiguration mit Array-LUNs

Bei einer Stretch-MetroCluster-Konfiguration mit Array-LUNs müssen Sie die FC-VI-Ports verkabeln, um die direkte Verbindung zwischen den Controllern zu erreichen. Darüber hinaus müssen Sie jeden Controller-HBA-Port verkabeln, um Switch-Ports auf den entsprechenden FC-Switches zu Switch. Die Verkabelung zu den Array-LUNs erfolgt wie bei einem Fabric-Attached MetroCluster, mit Ausnahme von Array-LUNs der E-Serie, die direkt verbunden werden können.

Die folgende Abbildung zeigt die FC-VI-Ports, die in einer Stretch-MetroCluster-Konfiguration über die Controller A und B hinweg verkabelt sind:

Die FAS9000 Storage-Systeme Controller-Module verwenden jeweils vier FC-VI-Ports.

Bei Konfigurationen mit E-Series Array LUNs können Sie die E-Series LUNs direkt anschließen.

"Direct Attach-Support für Stretch-MetroCluster-Konfiguration mit NetApp E-Series Arrays"

Mit Ausnahme der Verbindung der FC-VI-Ports werden während des weiteren Verfahrens eine MetroCluster-Konfiguration mit den Array-LUNs eingerichtet, die keine LUNs der E-Series verwenden. Dazu müssen FC Switches verwendet werden, die mit den Array-LUNs in Fabric-Attached-Konfigurationen identisch sind.

"Installation und Konfiguration von Fabric-Attached MetroCluster"

Beispiele für Stretch-MetroCluster-Konfigurationen mit zwei Nodes und Festplatten und Array-LUNs

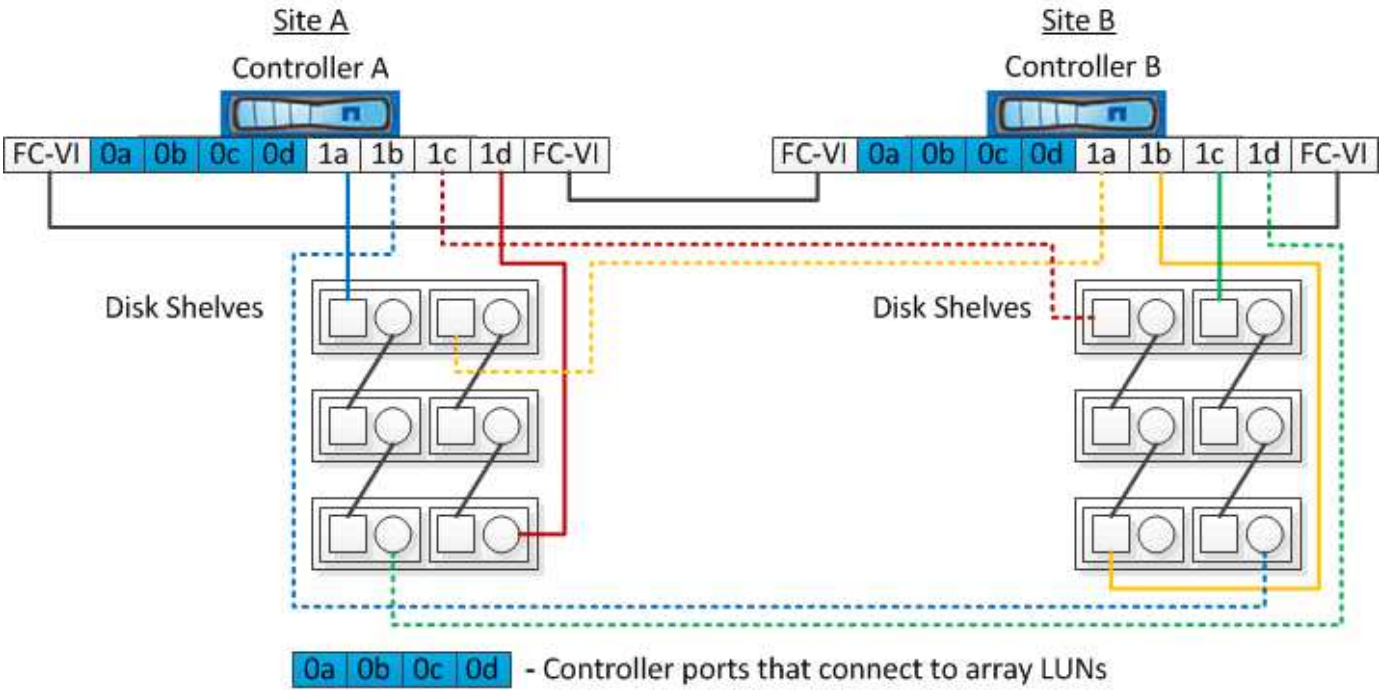
Zum Einrichten einer Stretch-MetroCluster-Konfiguration mit nativen Festplatten und Array-LUNs müssen Sie zum Anschluss der ONTAP Systeme an die Festplatten-Shelfs entweder über FC-to-SAS-Bridges oder über optische SAS-Kabel verfügen. Darüber hinaus müssen FC Switches verwendet werden, um Array-LUNs mit den ONTAP-

Systemen zu verbinden.

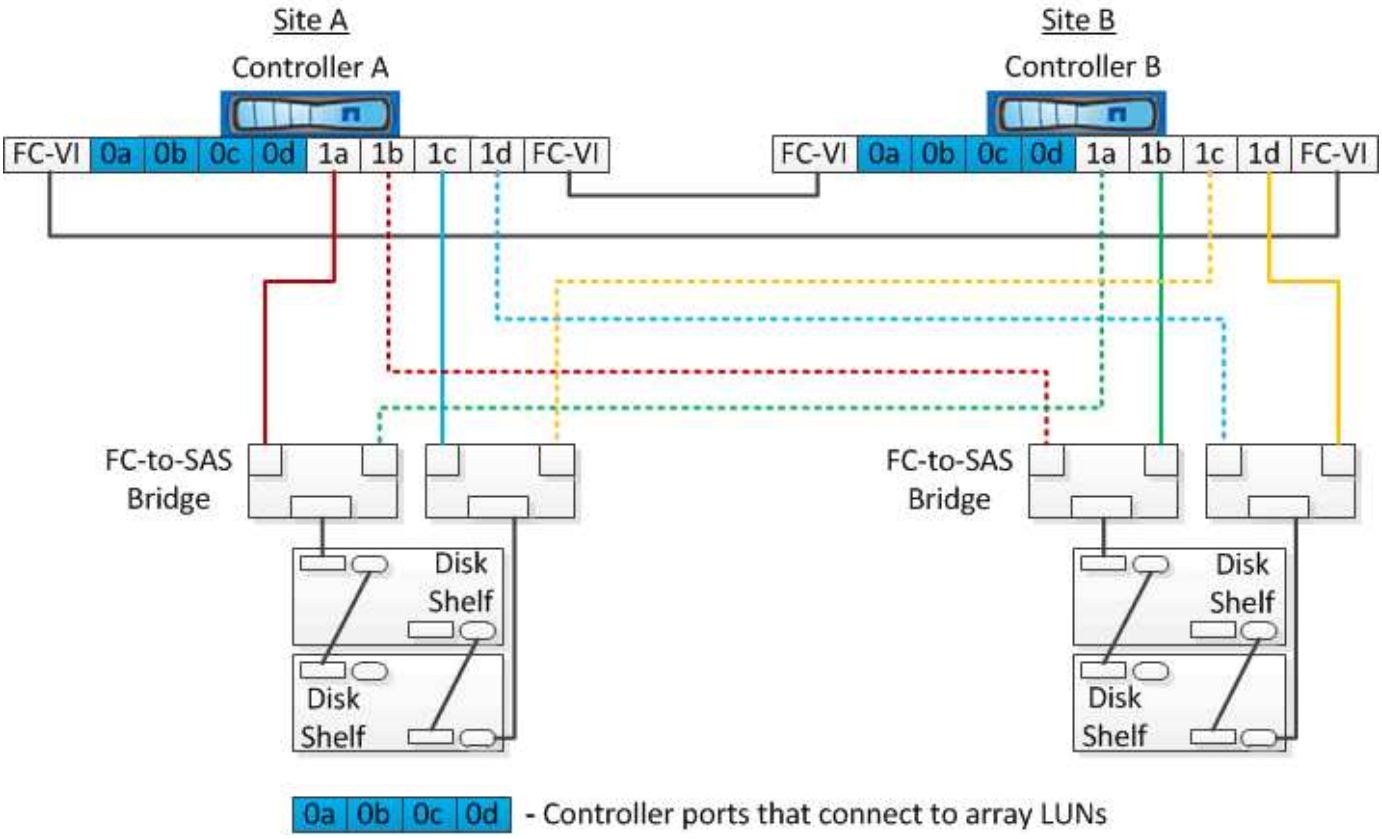
Es sind mindestens acht HBA-Ports erforderlich, damit ein ONTAP-System mit nativen Festplatten und Array-LUNs verbunden werden kann.

In den folgenden Beispielen, die Stretch-MetroCluster-Konfigurationen mit zwei Nodes mit Festplatten und Array-LUNs veranschaulichen, werden HBA-Ports 0a bis 0d zur Verbindung mit Array-LUNs verwendet. Für Verbindungen mit nativen Festplatten werden HBA-Ports 1a bis 1d verwendet.

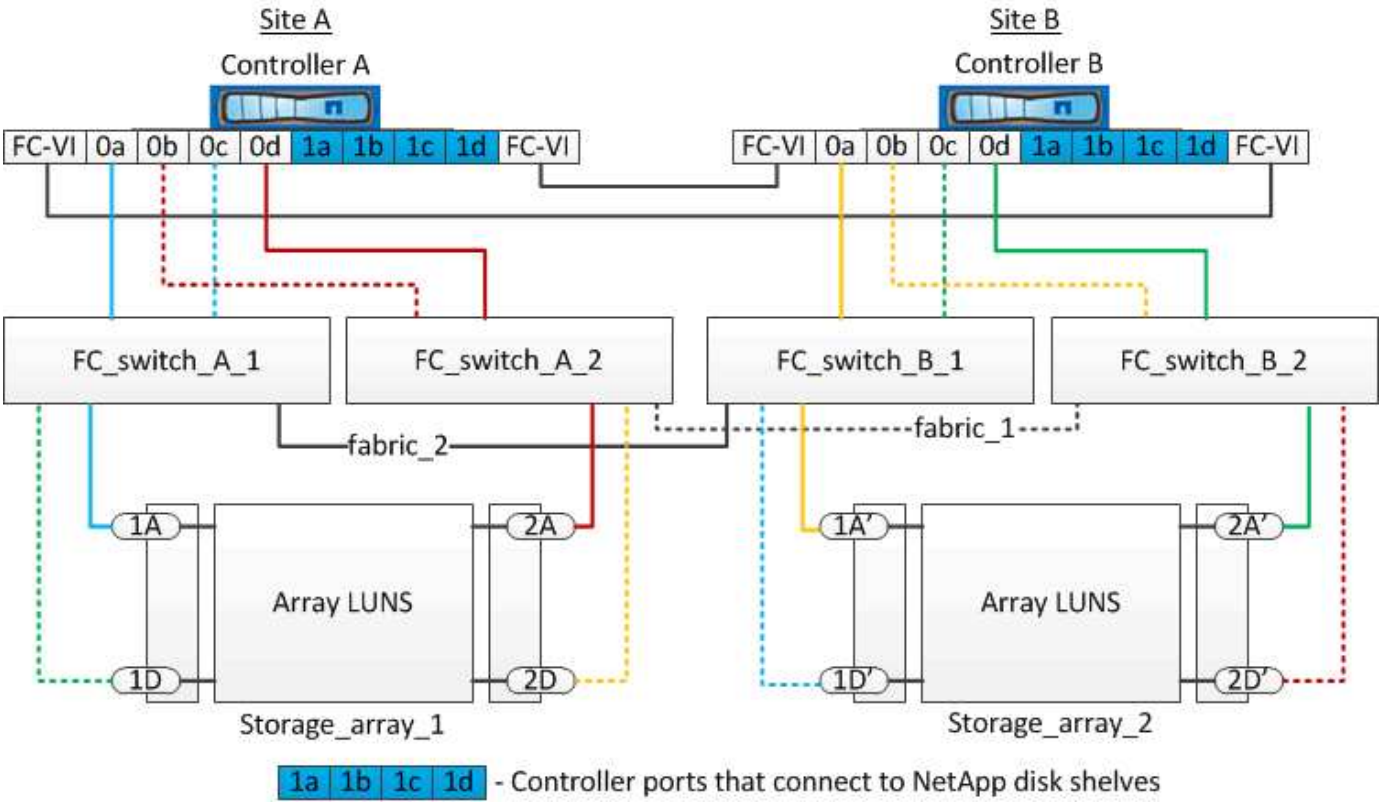
Die folgende Abbildung zeigt eine Stretch-MetroCluster-Konfiguration mit zwei Nodes, in der die nativen Festplatten über optische SAS-Kabel mit den ONTAP-Systemen verbunden sind:



Die folgende Abbildung zeigt eine Stretch-MetroCluster-Konfiguration mit zwei Nodes, bei der die nativen Festplatten über FC-to-SAS-Bridges mit den ONTAP-Systemen verbunden werden:



Die folgende Abbildung zeigt eine Stretch-MetroCluster-Konfiguration mit zwei Nodes mit den Array-LUN-Verbindungen:



Bei Bedarf können Sie auch dieselben FC Switches verwenden, um sowohl native Festplatten als auch die Array-LUNs mit den Controllern in der MetroCluster-Konfiguration zu verbinden.

"Installation und Konfiguration von Fabric-Attached MetroCluster"

Beispiel für eine Stretch-MetroCluster Konfiguration mit E-Series Storage-Arrays

In einer Stretch-MetroCluster Konfiguration mit E-Series Storage Array LUNs können Sie die Storage-Controller und die Storage-Arrays direkt verbinden. Im Gegensatz zu anderen Array LUNs sind FC-Switches nicht erforderlich.

Der "Direct Attach-Support für Stretch-MetroCluster-Konfiguration mit NetApp E-Series Arrays" Der Knowledgebase Artikel enthält Beispiele für Konfigurationen mit E-Series Array-LUNs.

Überlegungen beim Entfernen von MetroCluster-Konfigurationen

Sie können die MetroCluster-Konfiguration von allen Nodes einer Disaster Recovery-Gruppe (DR) entfernen. Nach dem Entfernen der MetroCluster-Konfiguration sollten alle Festplatten-Konnektivität und Interconnects auf einen unterstützten Zustand eingestellt werden. Wenden Sie sich an den technischen Support, wenn Sie die MetroCluster Konfiguration entfernen müssen.

Die Konfiguration von MetroCluster kann nicht rückgängig gemacht werden. Dieses Verfahren sollte nur mit Unterstützung durch den technischen Support erfolgen. Wenden Sie sich an den technischen Support von NetApp und verweisen Sie auf den entsprechenden Leitfaden für Ihre Konfiguration im "Entfernen von Knoten aus einer MetroCluster Konfiguration - Auflösungsleitfaden."

So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring

Mit Active IQ Unified Manager und ONTAP System Manager weitere Konfiguration und Monitoring

Active IQ Unified Manager und ONTAP System Manager können für das GUI-Management der Cluster und für das Monitoring der Konfiguration verwendet werden.

Auf jedem Node ist ONTAP System Manager vorinstalliert. Geben Sie zum Laden von System Manager die LIF-Adresse für das Cluster-Management als URL in einem Webbrowser, der mit dem Node verbunden ist.

Sie können die MetroCluster-Konfiguration auch mit Active IQ Unified Manager überwachen.

Verwandte Informationen

"Active IQ Unified Manager und ONTAP System Manager Dokumentation"

Synchronisieren der Systemzeit mithilfe von NTP

Jedes Cluster benötigt einen eigenen NTP-Server (Network Time Protocol), um die Zeit zwischen den Nodes und ihren Clients zu synchronisieren. Mit dem Dialogfeld DateTime bearbeiten in System Manager können Sie den NTP-Server konfigurieren.

Überprüfen Sie, ob Sie System Manager heruntergeladen und installiert haben. System Manager ist über die NetApp Support Site erhältlich.

- Sie können nach dem Takeover die Zeitzoneneinstellungen für einen ausgefallenen Node oder den Partner-Node nicht ändern.
- Jedes Cluster in der MetroCluster FC-Konfiguration sollte über einen eigenen separaten NTP-Server oder von den Nodes verwendete Server und (falls vorhanden) FC-to-SAS-Bridges an diesem MetroCluster-Standort verfügen.

  Wenn Sie die MetroCluster Tiebreaker Software verwenden, sollte es auch einen eigenen separaten NTP-Server haben.

Schritte

1. Doppelklicken Sie auf der Startseite auf das entsprechende Storage-System.
2. Erweitern Sie die **Cluster** -Hierarchie im linken Navigationsbereich.
3. Klicken Sie im Navigationsbereich auf **Konfiguration Systemwerkzeuge DateTime**.
4. Klicken Sie Auf **Bearbeiten**.
5. Wählen Sie die Zeitzone aus.
6. Geben Sie die IP-Adressen der Zeitserver an, und klicken Sie dann auf **Hinzufügen**.

   Sie müssen einen NTP-Server zur Liste der Zeitserver hinzufügen. Der Domänencontroller kann ein autorisierende Server sein.

7. Klicken Sie auf **OK**.
8. Überprüfen Sie die Änderungen, die Sie an den Datums- und Zeiteinstellungen im Fenster Datum und Uhrzeit vorgenommen haben.

Überlegungen bei der Verwendung von ONTAP in einer MetroCluster-Konfiguration

Wenn Sie ONTAP in einer MetroCluster-Konfiguration verwenden, sollten Sie bestimmte Überlegungen bei der Lizenzierung, beim Peering an Cluster außerhalb der MetroCluster-Konfiguration, bei der Durchführung von Volume-Vorgängen, NVFAIL-Vorgängen und anderen ONTAP-Vorgängen beachten.

Überlegungen zur Lizenzierung

- Beide Standorte sollten für die gleiche Site-lizenzierte Funktionen lizenziert sein.
- Alle Nodes sollten für die gleichen Node-gesperrten Funktionen lizenziert sein.

Überlegungen zu SnapMirror

- Die Disaster Recovery für SnapMirror SVMs wird nur auf MetroCluster Konfigurationen mit Versionen von ONTAP 9.5 oder höher unterstützt.

FlexCache-Unterstützung in einer MetroCluster-Konfiguration

Ab ONTAP 9.7 werden FlexCache Volumes von MetroCluster Konfigurationen unterstützt. Sie sollten die Anforderungen für die manuelle Aufhebung nach dem Switchover oder Switchback-Betrieb kennen.

SVM wird nach der Umschaltung wieder aufgehoben, wenn sich die FlexCache Herkunft und der Cache innerhalb desselben Standorts befinden. MetroCluster

Nach einer vereinbarten oder ungeplanten Umschaltung muss jede SVM-FlexCache-Peering-Beziehung innerhalb des Clusters manuell konfiguriert werden.

Beispielsweise befinden sich SVMs vs1 (Cache) und vs2 (Ursprung) auf Site_A Diese SVMs sind Peering-Punkte.

Nach der Umschaltung werden SVMs vs1-mc und vs2-mc am Partner-Standort (Site_B) aktiviert. Sie müssen manuell aufgehoben werden, damit FlexCache mit dem arbeiten kann `vserver peer repeer` Befehl.

SVM wird nach dem Switchover aufgehoben oder zurückgeschaltet, wenn sich ein FlexCache Ziel auf einem dritten Cluster befindet und sich im getrennten Modus befindet

Bei FlexCache-Beziehungen zu einem Cluster außerhalb der MetroCluster-Konfiguration muss das Peering nach einem Switchover immer manuell neu konfiguriert werden, wenn die betroffenen Cluster während der Umschaltung in einem getrennten Modus sind.

Beispiel:

- Ein Ende der FlexCache (Cache_1 auf vs1) befindet sich auf MetroCluster site_A hat ein Ende der FlexCache
- Das andere Ende der FlexCache (Origin_1 auf vs2) befindet sich auf site_C (nicht in der MetroCluster-Konfiguration)

Wenn die Umschaltung ausgelöst wird und keine Verbindung zwischen Site_A und Site_C besteht, müssen Sie die SVMs On Site_B (das Switchover-Cluster) und Site_C über die manuell aufheben `vserver peer repeer` Befehl nach der Umschaltung.

Wenn ein Wechsel zurück durchgeführt wird, müssen Sie die SVMs on site_A (das ursprüngliche Cluster) und site_C. erneut aufheben

FabricPool-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.7 unterstützen MetroCluster Konfigurationen FabricPool Storage Tiers.

Informationen zur Verwendung von FabricPool finden Sie in "Festplatten- und Aggregatmanagement".

Überlegungen bei der Verwendung von FabricPool

- Die Cluster müssen über FabricPool-Lizenzen mit entsprechenden Kapazitätslimits verfügen.
- Die Cluster müssen IPspaces mit übereinstimmenden Namen haben.

Dies kann der standardmäßige IP-Speicherplatz sein oder ein IP-Speicherplatz, den eine Verwaltung erstellt hat. Dieser IPspace wird für die Konfiguration des FabricPool-Objektspeichers verwendet.

- Für den ausgewählten IPspace muss für jedes Cluster eine Intercluster-LIF definiert sein, die den externen Objektspeicher erreichen kann

Konfigurieren eines Aggregats zur Verwendung in einer gespiegelten FabricPool

> Bevor Sie das Aggregat konfigurieren, müssen Sie in der Objektspeicher einrichten, wie unter „Einrichten von Objektspeichern für FabricPool in einer MetroCluster-Konfiguration“ beschrieben "Festplatten- und Aggregatmanagement".

So konfigurieren Sie ein Aggregat für die Verwendung in einem FabricPool:

1. Erstellen Sie das Aggregat oder wählen Sie ein vorhandenes Aggregat aus.
2. Spiegeln Sie das Aggregat als ein typisches gespiegeltes Aggregat innerhalb der MetroCluster Konfiguration.
3. Erstellen Sie die FabricPool Spiegelung mit dem Aggregat, wie im beschrieben "Festplatten- und Aggregatmanagement":
   a. Hängen Sie einen primären Objektspeicher an.

      Dieser Objektspeicher befindet sich physisch näher am Cluster.

   b. Fügen Sie einen Mirror-Objektspeicher hinzu.

      Dieser Objektspeicher liegt physisch weiter vom Cluster entfernt als der primäre Objektspeicher.

FlexGroup-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.6 unterstützen MetroCluster Konfigurationen FlexGroup Volumes.

Job-Zeitpläne in einer MetroCluster-Konfiguration

In ONTAP 9.3 und höher werden benutzererstellte Job-Zeitpläne automatisch zwischen Clustern in einer MetroCluster Konfiguration repliziert. Wenn Sie einen Job-Zeitplan auf einem Cluster erstellen, ändern oder löschen, wird derselbe Zeitplan automatisch auf dem Partner-Cluster unter Verwendung des Configuration Replication Service (CRS) erstellt.

> Systemerstellte Zeitpläne werden nicht repliziert, und Sie müssen manuell denselben Vorgang auf dem Partner-Cluster durchführen, damit Job-Zeitpläne auf beiden Clustern identisch sind.

Cluster-Peering vom MetroCluster Standort zu einem dritten Cluster

Da die Peering-Konfiguration nicht repliziert wird, müssen Sie auch das Peering auf dem Partner MetroCluster Cluster konfigurieren, wenn Sie eines der Cluster in der MetroCluster Konfiguration zu einem dritten Cluster außerhalb dieser Konfiguration Peer. So bleibt Peering bei einem Switchover erhalten.

Der nicht-MetroCluster Cluster muss ONTAP 8.3 oder höher ausführen. Andernfalls geht Peering verloren, wenn ein Switchover auftritt, selbst wenn Peering für beide MetroCluster-Partner konfiguriert wurde.

Replikation der LDAP-Client-Konfiguration in einer MetroCluster-Konfiguration

Eine auf einer Storage Virtual Machine (SVM) auf einem lokalen Cluster erstellte LDAP-Client-Konfiguration wird auf die Partnerdaten-SVM auf dem Remote-Cluster repliziert. Wenn beispielsweise die LDAP-Client-Konfiguration auf der Admin-SVM auf dem lokalen Cluster erstellt wird, wird sie auf allen Admin-Daten-SVMs im Remote-Cluster repliziert. Diese MetroCluster Funktion ist vorsätzlich, sodass die LDAP-Client-Konfiguration in allen Partner-SVMs des Remote-Clusters aktiv ist.

Richtlinien zur Erstellung von Networking und LIF für MetroCluster Konfigurationen

Sie sollten beachten, wie in einer MetroCluster Konfiguration LIFs erstellt und repliziert werden. Außerdem müssen Sie über die Notwendigkeit der Konsistenz Bescheid wissen, damit Sie bei der Konfiguration Ihres Netzwerks richtige Entscheidungen treffen können.

Verwandte Informationen

"ONTAP-Konzepte"

Anforderungen für die Replikation von IPspace-Objekten und die Subnetz-Konfiguration

Sie sollten die Anforderungen für das Replizieren von IPspace-Objekten in das Partner-Cluster sowie für die Konfiguration von Subnetzen und IPv6 in einer MetroCluster-Konfiguration kennen.

IPspace-Replizierung

Beim Replizieren von IPspace-Objekten in das Partner-Cluster müssen Sie die folgenden Richtlinien berücksichtigen:

- Die IPspace-Namen der beiden Standorte müssen übereinstimmen.
- IPspace-Objekte müssen manuell auf das Partner-Cluster repliziert werden.

  Storage Virtual Machines (SVMs), die vor der Replizierung des IPspaces erstellt und einem IPspace zugewiesen werden, werden nicht zum Partner-Cluster repliziert.

Subnetz-Konfiguration

Beim Konfigurieren von Subnetzen in einer MetroCluster-Konfiguration müssen Sie die folgenden Richtlinien berücksichtigen:

- Beide Cluster der MetroCluster-Konfiguration müssen ein Subnetz im selben IPspace mit demselben Subnetz, Subnetz, Broadcast-Domäne und Gateway aufweisen.
- Der IP-Bereich der beiden Cluster muss unterschiedlich sein.

  Im folgenden Beispiel unterscheiden sich die IP-Bereiche:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                   Avail/
Name      Subnet            Domain    Gateway           Total    Ranges
--------- ---------------- --------- ------------      -------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                   Avail/
Name      Subnet            Domain    Gateway           Total    Ranges
--------- ---------------- --------- ------------     --------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.21-192.168.2.30
```

IPv6-Konfiguration

Wenn IPv6 auf einem Standort konfiguriert ist, muss IPv6 auch auf dem anderen Standort konfiguriert werden.

Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration

Bei der Konfiguration Ihres Netzwerks in einer MetroCluster-Konfiguration sollten Sie die Anforderungen zum Erstellen von LIFs kennen.

Beim Erstellen von LIFs müssen Sie die folgenden Richtlinien beachten:

- Fibre Channel: Sie müssen gestreckte VSAN-Fabrics oder Stretched Fabrics verwenden.
- IP/iSCSI: Sie müssen Layer 2-Strecked-Netzwerk verwenden.
- ARP-Sendungen: Sie müssen ARP-Übertragungen zwischen den beiden Clustern aktivieren.
- Doppelte LIFs: Sie müssen nicht mehrere LIFs mit derselben IP-Adresse (doppelte LIFs) in einem IPspace erstellen.
- NFS- und SAN-Konfigurationen: Es müssen unterschiedliche Storage Virtual Machines (SVMs) sowohl für nicht gespiegelte als auch gespiegelte Aggregate verwendet werden.

Überprüfen Sie die LIF-Erstellung

Sie können die erfolgreiche Erstellung einer logischen Schnittstelle in einer MetroCluster-Konfiguration bestätigen, indem Sie die ausführen `metrocluster check lif show` Befehl. Falls beim Erstellen des LIF Probleme auftreten, können Sie den verwenden `metrocluster check lif repair-placement` Befehl zum Beheben der Probleme.

Anforderungen und Probleme bei der LIF-Replizierung sowie bei der Platzierung

Sie sollten die LIF-Replizierungsanforderungen in einer MetroCluster-Konfiguration kennen. Sie sollten auch wissen, wie eine replizierte LIF auf einem Partner-Cluster platziert ist. Beachten Sie die Probleme, die bei Ausfall der LIF-Replizierung oder der LIF-Platzierung auftreten.

Replizierung von LIFs am Partner-Cluster

Wenn Sie eine LIF auf einem Cluster in einer MetroCluster-Konfiguration erstellen, wird diese LIF im Partner-Cluster repliziert. LIFs werden nicht nach Eins-zu-Eins-Namen platziert. Für die Verfügbarkeit von LIFs nach einem Switchover überprüft der Prozess über die LIF-Platzierung, ob die Ports die LIF auf Basis von Erreichbarkeit und Port-Attributprüfungen hosten können.

Das System muss die folgenden Bedingungen erfüllen, um die replizierten LIFs auf das Partner-Cluster zu platzieren:

Zustand	LIF-Typ: FC	LIF-Typ: IP/iSCSI
Knotenidentifikation	ONTAP versucht, die replizierte LIF auf den Disaster Recovery (DR) Partner des Nodes zu platzieren, auf dem sie erstellt wurde. Falls der DR-Partner nicht verfügbar ist, wird der DR-Hilfspartner zur Platzierung verwendet.	ONTAP versucht, die replizierte LIF auf den DR-Partner des Nodes, auf dem sie erstellt wurde, zu platzieren. Falls der DR-Partner nicht verfügbar ist, wird der DR-Hilfspartner zur Platzierung verwendet.
Port-ID	ONTAP identifiziert die verbundenen FC-Ziel-Ports auf dem DR-Cluster.	Die Ports auf dem DR-Cluster, die sich im gleichen IPspace wie die Quell-LIF befinden, werden für eine Überprüfung der Erreichbarkeit ausgewählt. Wenn im DR-Cluster keine Ports im gleichen IPspace vorhanden sind, kann die LIF nicht platziert werden. Alle Ports im DR-Cluster, die bereits ein LIF im selben IPspace und Subnetz hosten, werden automatisch als erreichbar markiert und können zur Platzierung verwendet werden. Diese Ports sind nicht in der Überprüfung der Erreichbarkeit enthalten.

Erreichbarkeit prüfen	Die Erreichbarkeit ist bestimmt, indem die Konnektivität der Quell-Fabric-WWN auf den Ports im DR-Cluster geprüft wird. Wenn dieselbe Fabric nicht am DR-Standort vorhanden ist, wird diese LIF auf einem zufälligen Port des DR-Partners platziert.	Die Erreichbarkeit wird durch die Antwort auf ein ARP-Protokoll (Address Resolution Protocol) bestimmt, das von jedem zuvor identifizierten Port des DR-Clusters an die Quell-IP-Adresse der zu platzierten LIF gesendet wird. Damit Überprüfungen der Erreichbarkeit erfolgreich sind, müssen ARP-Broadcasts zwischen den beiden Clustern zulässig sein. Jeder Port, der eine Antwort vom Quell-LIF erhält, wird zur Platzierung so markiert.
Portauswahl	ONTAP kategorisiert die Ports anhand von Attributen wie Adaptertyp und -Geschwindigkeit und wählt dann die Ports mit übereinstimmenden Attributen aus. Wenn keine Ports mit übereinstimmenden Attributen gefunden werden, wird das LIF auf einem zufällig verbundenen Port des DR-Partners platziert.	Von den Ports, die während der Überprüfung der Erreichbarkeit als erreichbar markiert sind, bevorzugt ONTAP Ports, die sich in der Broadcast-Domäne befinden, die mit dem Subnetz der logischen Schnittstelle verknüpft sind. Wenn auf dem DR-Cluster keine Netzwerkports verfügbar sind, die sich in der Broadcast-Domäne befinden, die mit dem Subnetz der logischen Schnittstelle verknüpft sind, wählt ONTAP Ports aus, die auf die Quell-LIF Bezug verfügen. Wenn keine Ports mit Reachability zur Quell-LIF vorhanden sind, wird aus der Broadcast-Domäne ein Port ausgewählt, der mit dem Subnetz der Quell-LIF verknüpft ist. Wenn keine solche Broadcast-Domäne vorhanden ist, wird ein zufälliger Port ausgewählt. ONTAP kategorisiert die Ports anhand von Attributen wie Adaptertyp, Schnittstellentyp und Geschwindigkeit und wählt dann die Ports mit übereinstimmenden Attributen aus.

LIF-Platzierung	Über die erreichbaren Ports wählt ONTAP den am wenigsten geladenen Port zur Platzierung aus.	Von den ausgewählten Ports aus wählt ONTAP den am wenigsten geladenen Port zur Platzierung aus.

Platzierung replizierter LIFs, wenn der DR-Partner-Node ausfällt

Wenn auf einem Node, dessen DR-Partner übernommen wurde, eine iSCSI- oder FC-LIF erstellt wird, wird die replizierte LIF auf den zusätzlichen DR-Partner-Knoten platziert. Nach einem nachfolgenden Giveback-Vorgang werden die LIFs nicht automatisch an den DR-Partner übertragen. Dies kann dazu führen, dass sich LIFs auf einen einzelnen Node im Partner-Cluster konzentrieren. Bei einer MetroCluster-Umschaltung versuchen Sie anschließend, die LUNs, die zur SVM (Storage Virtual Machine) gehören, zuzuordnen.

Sie sollten den ausführen `metrocluster check lif show` Befehl nach einem Takeover- oder Giveback-Vorgang, um zu überprüfen, dass die LIF-Platzierung korrekt ist. Wenn Fehler vorhanden sind, können Sie den ausführen `metrocluster check lif repair-placement` Befehl zum Beheben der Probleme.

Fehler beim LIF-Platzierung

Fehler beim LIF-Platzierung, die von angezeigt werden `metrocluster check lif show` Der Befehl bleibt nach einem Switchover-Vorgang erhalten. Wenn der `network interface modify`, `network interface rename`, Oder `network interface delete` Befehl wird für ein LIF mit einem Platzierungsfehler ausgegeben, der Fehler wird entfernt und in der Ausgabe des wird nicht angezeigt `metrocluster check lif show` Befehl.

Fehler bei der LIF-Replizierung

Sie können außerdem prüfen, ob die LIF-Replizierung mithilfe von erfolgreich war `metrocluster check lif show` Befehl. Wenn die LIF-Replikation fehlschlägt, wird eine EMS-Meldung angezeigt.

Sie können einen Replikationsfehler beheben, indem Sie den ausführen `metrocluster check lif repair-placement` Befehl für jedes LIF, das einen korrekten Port nicht findet. Sie sollten alle LIF-Replizierungsfehler so schnell wie möglich beheben, um die Verfügbarkeit von LIF während eines MetroCluster-Switchover-Vorgangs zu überprüfen.

> Selbst wenn die Quell-SVM ausfällt, wird die LIF-Platzierung möglicherweise normal fortgesetzt, wenn in einem Port mit demselben IPspace und Netzwerk in der Ziel-SVM eine LIF zu einer anderen SVM gehört.

Volume-Erstellung auf einem Root-Aggregat

Das System lässt nicht die Erstellung neuer Volumes im Root-Aggregat (ein Aggregat mit einer HA-Richtlinie von CFO) eines Knotens in einer MetroCluster-Konfiguration zu.

Aufgrund dieser Einschränkung können Root-Aggregate mit dem nicht zu einer SVM hinzugefügt werden `vserver add-aggregates` Befehl.

SVM Disaster Recovery in einer MetroCluster-Konfiguration

Ab ONTAP 9.5 können aktive Storage Virtual Machines (SVMs) in einer MetroCluster Konfiguration als Quellen mit der Disaster-Recovery-Funktion der SnapMirror SVM verwendet werden. Ziel-SVM muss sich auf dem dritten Cluster außerhalb der MetroCluster Konfiguration befinden.

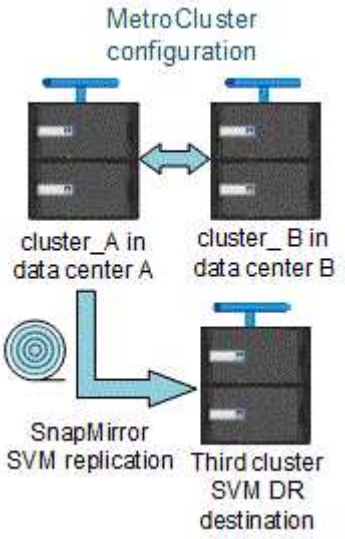
Bei der Verwendung von SVMs mit SnapMirror Disaster Recovery sollten Sie die folgenden Anforderungen und Einschränkungen beachten:

- Nur eine aktive SVM innerhalb einer MetroCluster-Konfiguration kann als Quelle einer SVM Disaster-Recovery-Beziehung verwendet werden.

  Eine Quelle kann eine synchrone Quell-SVM vor der Umschaltung oder eine synchrone Ziel-SVM nach der Umschaltung sein.

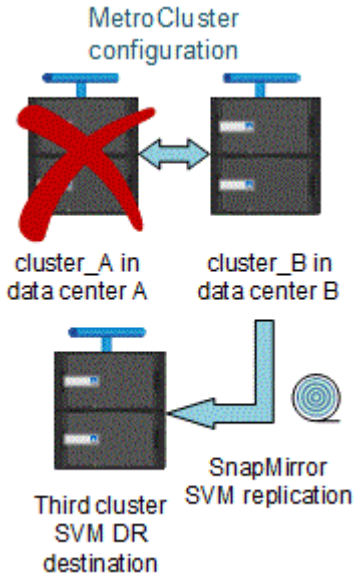
- Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind.

  Das folgende Bild zeigt das Verhalten der SVM Disaster Recovery in einem stabilen Zustand:



- Wenn die synchrone SVM-Quelle die Quelle einer SVM-DR-Beziehung ist, werden die Quell-SVM-DR-Beziehungsinformationen zum MetroCluster Partner repliziert.

  Dadurch können die SVM-DR-Updates nach einer Umschaltung fortgesetzt werden, wie im folgenden Image dargestellt:



- Während der Switchover- und Switchover-Prozesse kann die Replizierung zur SVM-DR-Ziel fehlschlagen.

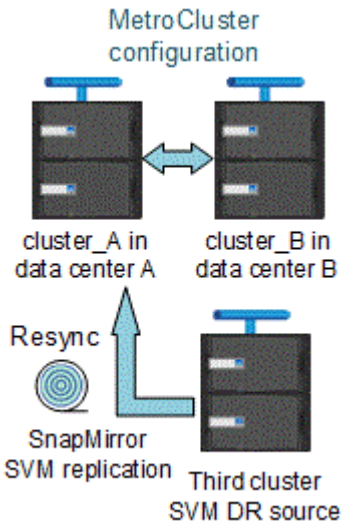
  Nach Abschluss des Switchover- oder Switch-Prozesses werden jedoch die nächsten geplanten SVM-DR-Updates erfolgreich durchgeführt.

Weitere Informationen finden Sie im Abschnitt „`Replizieren der SVM-Konfiguration`“ "Datensicherung mit der CLI" Weitere Informationen zur Konfiguration einer SVM-DR-Beziehung.

Neusynchronisierung der SVM an einem Disaster-Recovery-Standort

Während der Resynchronisierung wird die Disaster-Recovery-Quelle (DR) der Storage Virtual Machines (SVMs) auf der MetroCluster Konfiguration auf der Ziel-SVM auf dem Standort, der nicht von MetroCluster stammt, wiederhergestellt.

Während der Resynchronisierung fungiert die Quell-SVM (Cluster_A) als Ziel-SVM, wie in dem folgenden Image dargestellt:



Wenn während der Neusynchronisierung eine ungeplante Umschaltung erfolgt

Ungeplante Umschalt, die während der Neusynchronisierung auftreten, stoppt die Neusynchronisierung. Wenn eine ungeplante Umschaltung stattfindet, gelten die folgenden Bedingungen:

- Die Ziel-SVM auf dem MetroCluster Standort (als Quell-SVM vor der Resynchronisierung) bleibt als Ziel-SVM erhalten. Der Untertyp der SVM im Partner-Cluster bleibt weiterhin inaktiv.
- Die SnapMirror Beziehung muss manuell und als Ziel mit der SVM für das synchrone Ziel neu erstellt werden.
- Die SnapMirror Beziehung erscheint nicht in der SnapMirror-Ausgabe nach einer Umschaltung am Survivor-Standort, es sei denn, ein SnapMirror Erstellungsvorgang wird ausgeführt.

Während der Neusynchronisierung erfolgt der Wechsel zurück nach einer ungeplanten Umschaltung

Um den Switchback-Prozess erfolgreich durchzuführen, muss die Resynchronisierung-Beziehung gebrochen und gelöscht werden. Der Wechsel zurück ist nicht zulässig, wenn in der MetroCluster Konfiguration SnapMirror DR-Ziel-SVMs vorhanden sind oder wenn der Cluster über eine SVM mit dem Untertyp „`dp-Destination`“ verfügt.

Ausgabe der show-Befehle für die Storage-Festplatte und des Storage-Shelf zeigen-Befehle in einer Stretch-MetroCluster-Konfiguration mit zwei Nodes

In einer Stretch-MetroCluster-Konfiguration mit zwei Nodes wird der -verwendet `is-local-attach` Feld von `storage disk show` Und `storage shelf show` Durch Befehle werden alle Festplatten und Storage Shelfs unabhängig vom Node, mit dem sie verbunden sind, als lokal angezeigt.

Die Ausgabe des Befehls „Plex show“ für das Storage-Aggregat ist nach einer MetroCluster-Umschaltung nicht bestimmt

Wenn Sie den ausführen `storage aggregate plex show` Befehl nach einer MetroCluster-Umschaltung ist der Status von plex0 des Switched über das Root-Aggregat unbestimmt und wird als angezeigt `failed`. Während dieser Zeit wird die umschaltete Root nicht aktualisiert. Der tatsächliche Status dieses Plex kann nur nach der MetroCluster-Heilungsphase ermittelt werden.

Ändern von Volumes zum Festlegen des NV-Fehler-Flags bei Umschalten

Sie können ein Volume so ändern, dass bei einer MetroCluster-Umschaltung das NV-Fehler-Flag auf das Volume gesetzt wird. Das NVFAIL-Flag bewirkt, dass das Volumen von allen Änderungen abgetrennt wird. Dies ist für Volumes erforderlich, die so behandelt werden müssen, als würden bestimmte Schreibvorgänge auf dem Volume nach der Umschaltung verloren gehen.

> In ONTAP-Versionen vor 9.0 wird für jede Umschaltung das NV-Fehler-Flag verwendet. In ONTAP 9.0 und neueren Versionen kommt die ungeplante Umschaltung (USO) zum Einsatz.

Schritte

1. Aktivieren Sie die MetroCluster-Konfiguration, um NVFAIL bei der Umschaltung auszulösen, indem Sie den einstellen `vol -dr-force-nvfail` Parameter zu „`ein`“:

   ```
   vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
   ```

Umstieg von einer Stretch- zu einer Fabric-Attached MetroCluster Konfiguration

In einer Fabric-Attached MetroCluster-Konfiguration sind die Nodes an unterschiedlichen Orten. Dieser geografische Unterschied erhöht den Katastrophenschutz. Für den Übergang von einer Stretch- zu einer Fabric-Attached MetroCluster-Konfiguration müssen Sie FC Switches und gegebenenfalls FC-zu-SAS-Bridges hinzufügen.

- Sie müssen die automatische Umschaltung auf beiden Clustern deaktivieren, indem Sie den ausführen `metrocluster modify -auto-switchover-failure-domain auto-disabled` Befehl.
- Sie müssen die Nodes herunterfahren.

  Dieser Vorgang ist störend.

Die MetroCluster Konfiguration muss an beiden Standorten umgestellt werden. Nach einem Upgrade der MetroCluster Konfiguration müssen Sie die automatische Umschaltung auf beide Cluster aktivieren. Sie müssen die Konfiguration auch validieren, indem Sie den ausführen `metrocluster check run` Befehl.

Dieses Verfahren gibt einen Überblick über die erforderlichen Schritte. Detaillierte Schritte finden Sie in bestimmten Abschnitten im "Installation und Konfiguration von Fabric-Attached MetroCluster". Sie müssen keine vollständige Installation und Konfiguration durchführen.

Schritte

1. Bereiten Sie sich auf das Upgrade vor, indem Sie den Abschnitt „Vorbereitungen für die MetroCluster Installation“ in der sorgfältig prüfen "Installation und Konfiguration von Fabric-Attached MetroCluster".
2. Die erforderlichen Switches und FC-to-SAS-Bridges installieren, verkabeln und konfigurieren.

   > Verwenden Sie die Verfahren im Abschnitt „Verkabelung einer Fabric-Attached MetroCluster-Konfiguration“ der "Installation und Konfiguration von Fabric-Attached MetroCluster".

3. Aktualisieren Sie die MetroCluster-Konfiguration mit den folgenden Schritten.

   Verwenden Sie nicht die Verfahren im Abschnitt „Konfigurieren der MetroCluster-Software in ONTAP“, die im Link: Fabric-attached MetroCluster-Installation und -Konfiguration zu finden sind.

   a. Rufen Sie den erweiterten Berechtigungsmodus auf:
      `set -privilege advanced`

   b. Aktualisieren Sie die MetroCluster-Konfiguration:
      `metrocluster configure -refresh true`

      Mit dem folgenden Befehl wird die MetroCluster-Konfiguration auf allen Nodes in der DR-Gruppe aktualisiert, die Controller_A_1 enthält:

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

   a. Zurück zum Admin-Berechtigungsmodus:
      `set -privilege admin`

4. Überprüfen Sie die MetroCluster Konfiguration auf Fehler und überprüfen Sie, ob sie funktionsfähig ist.

   Sie sollten die Verfahren in den folgenden Abschnitten des verwenden "Installation und Konfiguration von Fabric-Attached MetroCluster":

   - Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor
   - Überprüfen des lokalen HA-Vorgangs
   - Überprüfung von Umschaltung, Reparatur und Wechsel zurück

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und dem Betrieb von MetroCluster.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff

"ONTAP 9-Dokumentation"	• Alle MetroCluster-Leitfäden
	• Technische Übersicht über Konfiguration und Betrieb von MetroCluster FC • Best Practices für die MetroCluster FC-Konfiguration.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"MetroCluster IP-Installation und -Konfiguration: Unterschiede zwischen den ONTAP MetroCluster-Konfigurationen"	• MetroCluster IP Architektur • Verkabelung der Konfiguration • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management und Disaster Recovery"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln • Disaster Recovery (DR)
"Warten von MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Austausch oder Upgrade von Hardware: Verfahren zum Firmware-Upgrade für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Recovery-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes

"Umstellung von MetroCluster FC auf MetroCluster IP" "MetroCluster Upgrade- und Erweiterungsleitfaden"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"Installation und Konfiguration der MetroCluster Tiebreaker Software"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
Active IQ Unified Manager-Dokumentation "NetApp Dokumentation: Produktleitfäden und Ressourcen"	• Monitoring der MetroCluster Konfiguration und Performance
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.