MetroCluster-Dokumentation

ONTAP MetroCluster

NetApp
August 29, 2025

This PDF was generated from https://docs.netapp.com/de-de/ontap-metrocluster/index.html on August 29, 2025. Always check docs.netapp.com for the latest.

Inhalt

MetroCluster-Dokumentation . . . 1
Versionshinweise zu MetroCluster . . . 2
Neuerungen bei MetroCluster . . . 2
Neuerungen bei der MetroCluster IP Plattform und Switch-Unterstützung . . . 7
Plattform-Support . . . 8
Switch-Support . . . 8
Neuerungen bei der MetroCluster FC Plattform und Switch-Unterstützung . . . 9
Plattform-Support . . . 9
Switch-Support . . . 9
Was ist neu in ONTAP Mediator Unterstützung . . . 10
Neuerungen beim MetroCluster Tiebreaker Support . . . 10
Vorgestellt Werden . . . 10
OS Support-Matrix . . . 11
Installieren Sie eine Fabric-Attached MetroCluster . . . 12
Überblick . . . 12
Bereiten Sie sich auf die MetroCluster Installation vor . . . 12
Unterschiede zwischen den ONTAP MetroCluster Konfigurationen . . . 12
Cluster-Peering . . . 13
Überlegungen für ISLs . . . 16
Überlegungen bei der Verwendung von TDM/WDM-Geräten mit Fabric-Attached MetroCluster-Konfigurationen . . . 17
Anforderungen für die Verwendung eines Brocade DCX 8510-8 Switches . . . 19
Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten . . . 20
Firewall-Nutzung an MetroCluster Standorten . . . 21
Fabric-Attached MetroCluster-Konfiguration verkabeln . . . 21
Verkabelung einer Fabric-Attached MetroCluster-Konfiguration . . . 21
Teile einer Fabric-MetroCluster-Konfiguration . . . 22
Erforderliche MetroCluster FC-Komponenten und Namenskonventionen . . . 29
Konfigurationsarbeitsblätter für FC Switches und FC-to-SAS-Bridges . . . 33
Installieren und verkabeln Sie MetroCluster-Komponenten . . . 33
Konfigurieren Sie die FC-Switches . . . 64
Installation von FC-to-SAS-Bridges und SAS-Platten-Shelves . . . 191
Konfigurieren der MetroCluster-Software in ONTAP . . . 207
Sammeln der erforderlichen Informationen . . . 208
Ähnlichkeiten und Unterschiede zwischen Standard-Cluster und MetroCluster Konfigurationen . . . 214
Überprüfen und Konfigurieren des HA-Status von Komponenten im Wartungsmodus . . . 215
Wiederherstellung der Systemstandards und Konfiguration des HBA-Typs auf einem Controller-Modul 217
Konfigurieren von FC-VI-Ports auf einer X1132A-R6 Quad-Port-Karte auf FAS8020 Systemen . . . 219
Überprüfen der Festplattenzuweisung im Wartungsmodus in einer Konfiguration mit acht oder vier Nodes . . . 221
Überprüfen der Festplattenzuweisung im Wartungsmodus in einer Konfiguration mit zwei Nodes . . . 227
Einrichtung von ONTAP . . . 229
Konfigurieren der Cluster in einer MetroCluster-Konfiguration . . . 234

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor . . . 266
Überprüfen des lokalen HA-Vorgangs . . . 266
Überprüfung von Umschaltung, Reparatur und Wechsel zurück . . . 268
Sichern von Backup-Dateien der Konfiguration . . . 268
Überlegungen zur Verwendung von virtuellem IP- und Border-Gateway-Protokoll mit einer MetroCluster-Konfiguration . . . 268
ONTAP-Einschränkungen . . . 270
Richtlinien für die Verwendung dieser Layer-3-Lösung mit einer MetroCluster-Konfiguration . . . 270
Testen der MetroCluster-Konfiguration . . . 271
Überprüfung der ausgehandelten Umschaltung . . . 271
Überprüfung der Heilung und manueller Umkehrschalter . . . 273
Ausfall einer einzelnen FC-to-SAS-Bridge . . . 276
Überprüfung des Betriebs nach Stromunterbrechung . . . 277
Überprüfung des Betriebs nach einem Switch Fabric-Ausfall . . . 278
Überprüfung des Betriebs nach Ausfall eines einzelnen Storage Shelfs . . . 280
MetroCluster-Konfigurationen entfernen . . . 290
So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring . . . 291
Weitere Konfigurations- und Überwachungsfunktionen sind mit dem Active IQ Unified Manager und dem ONTAP System Manager möglich . . . 291
Synchronisieren Sie die Systemzeit mit NTP . . . 291
Überlegungen bei der Verwendung von ONTAP in einer MetroCluster-Konfiguration . . . 292
FlexCache-Unterstützung in einer MetroCluster-Konfiguration . . . 293
FabricPool-Unterstützung in MetroCluster-Konfigurationen . . . 294
FlexGroup-Unterstützung in MetroCluster-Konfigurationen . . . 295
Unterstützung von Konsistenzgruppen in MetroCluster Konfigurationen . . . 295
Job-Zeitpläne in einer MetroCluster-Konfiguration . . . 295
Cluster-Peering vom MetroCluster Standort zu einem dritten Cluster . . . 295
Replikation der LDAP-Client-Konfiguration in einer MetroCluster-Konfiguration . . . 295
Richtlinien zur Erstellung von Networking und LIF für MetroCluster Konfigurationen . . . 295
SVM Disaster Recovery in einer MetroCluster-Konfiguration . . . 301
Die Ausgabe des Befehls „Storage Aggregate Plex show“ ist nach einer MetroCluster Umschaltung nicht bestimmt . . . 304
Ändern von Volumes zum Festlegen des NV-Fehler-Flags bei Umschalten . . . 304
Wo Sie weitere Informationen finden . . . 305
MetroCluster und sonstige Informationen . . . 305
Installieren Sie eine MetroCluster IP-Konfiguration . . . 307
MetroCluster IP-Installationsworkflow . . . 307
Bereiten Sie sich auf die MetroCluster Installation vor . . . 307
Supportmatrix für ONTAP MetroCluster -Konfigurationen . . . 307
Unterschiede zwischen ONTAP Mediator und MetroCluster Tiebreaker . . . 309
Erfahren Sie mehr über Remote-Speicher und MetroCluster IP-Konfigurationen . . . 309
MetroCluster IP-Überlegungen für automatische Laufwerkszuweisung und ADP-Systeme . . . 311
Anforderungen für Cluster-Peering in MetroCluster IP-Konfigurationen . . . 326
ISL-Anforderungen . . . 329

Überlegungen zur Verwendung von MetroCluster-konformen Switches . . . 344
Erfahren Sie mehr über nicht gespiegelte Aggregate in MetroCluster -IP-Konfigurationen . . . 352
Firewall-Portanforderungen für MetroCluster IP-Konfigurationen . . . 354
Erfahren Sie mehr über die Verwendung von virtueller IP und Border Gateway Protocol mit einer MetroCluster -IP-Konfiguration . . . 354
Konfigurieren Sie die Hardwarekomponenten von MetroCluster . . . 357
Erfahren Sie mehr über die Verbindungen von Hardwarekomponenten in einer MetroCluster -IP -Konfiguration . . . 357
Erforderliche MetroCluster IP-Konfigurationskomponenten und Namenskonventionen . . . 361
Rack der MetroCluster IP-Konfigurationshardwarekomponenten . . . 365
MetroCluster IP-Switches verkabeln . . . 366
Verkabeln Sie die ONTAP Controllermodul-Ports in einer MetroCluster IP-Konfiguration . . . 410
Konfigurieren Sie die MetroCluster IP-Switches . . . 411
Überwachen der Integrität des MetroCluster-IP-Switches . . . 468
Konfigurieren Sie die MetroCluster Software in ONTAP . . . 495
Konfigurieren Sie die MetroCluster-Software mithilfe der CLI . . . 496
Konfigurieren Sie die MetroCluster Software mit System Manager . . . 563
Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung . . . 567
Vorbereitung der Installation von ONTAP Mediator in einer MetroCluster -IP-Konfiguration . . . 567
Einrichten des ONTAP Mediators für eine MetroCluster -IP-Konfiguration . . . 569
Entfernen Sie den ONTAP Mediator aus einer MetroCluster -IP-Konfiguration . . . 573
Verbinden Sie eine MetroCluster IP-Konfiguration mit einer anderen ONTAP Mediator-Instanz . . . 574
Wie der ONTAP Mediator automatische ungeplante Switchover in MetroCluster -IP-Konfigurationen unterstützt . . . 574
Verwalten Sie den ONTAP Mediator mit System Manager in MetroCluster -IP-Konfigurationen . . . 576
Testen Sie die ONTAP -Knotenumschaltung für Ihre MetroCluster IP-Konfiguration . . . 577
Überprüfung der ausgehandelten Umschaltung . . . 577
Überprüfung der Heilung und manueller Umkehrschalter . . . 579
Überprüfung des Betriebs nach Stromunterbrechung . . . 582
Überprüfung des Betriebs nach Ausfall eines einzelnen Storage Shelfs . . . 584
MetroCluster-Konfigurationen entfernen . . . 594
Anforderungen und Überlegungen für ONTAP -Operationen mit MetroCluster -IP-Konfigurationen . . . 595
Überlegungen zur Lizenzierung . . . 595
Überlegungen zu SnapMirror . . . 595
MetroCluster-Vorgänge in ONTAP System Manager . . . 595
FlexCache-Unterstützung in einer MetroCluster-Konfiguration . . . 595
FabricPool-Unterstützung in MetroCluster-Konfigurationen . . . 596
FlexGroup-Unterstützung in MetroCluster-Konfigurationen . . . 597
Job-Zeitpläne in einer MetroCluster-Konfiguration . . . 597
Cluster-Peering vom MetroCluster Standort zu einem dritten Cluster . . . 597
Replikation der LDAP-Client-Konfiguration in einer MetroCluster-Konfiguration . . . 597
Richtlinien zur Erstellung von Networking und LIF für MetroCluster Konfigurationen . . . 598
SVM Disaster Recovery in einer MetroCluster-Konfiguration . . . 602
Die Ausgabe des Befehls „Plex show“ für das Storage-Aggregat ist nach einer MetroCluster-Umschaltung nicht bestimmt . . . 605

Ändern von Volumes zum Festlegen des NV-Fehler-Flags bei Umschalten . . . 605
So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring . . . 606
Verwenden Sie den Active IQ Unified Manager und den ONTAP System Manager für die weitere Konfiguration und Überwachung in einer MetroCluster -IP-Konfiguration . . . 606
Synchronisieren Sie die Systemzeit mit NTP in einer MetroCluster -IP-Konfiguration . . . 606
Wo Sie weitere Informationen zu MetroCluster IP finden . . . 607
MetroCluster und sonstige Informationen . . . 607
Installieren Sie eine Stretch-MetroCluster-Konfiguration . . . 610
Überblick . . . 610
Bereiten Sie sich auf die MetroCluster Installation vor . . . 610
Unterschiede zwischen den ONTAP MetroCluster Konfigurationen . . . 610
Cluster-Peering . . . 612
Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten . . . 614
Firewall-Nutzung an MetroCluster Standorten . . . 615
Auswahl des richtigen Installationsverfahrens für Ihre Konfiguration . . . 615
Verkabeln Sie eine Stretch-MetroCluster-Konfiguration mit zwei SAS-Attached . . . 616
Verkabelung einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS . . . 616
Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über SAS . . . 616
Erforderliche MetroCluster Hardwarekomponenten und Benennungsrichtlinien für Stretch-Konfigurationen mit zwei Nodes über SAS . . . 617
MetroCluster-Komponenten für Stretch-Konfigurationen mit zwei Nodes installieren und verkabeln . . . 618
Verkabeln einer Stretch-MetroCluster-Konfiguration mit zwei über Bridge verbundenen Nodes . . . 622
Verkabelung einer Stretch MetroCluster Konfiguration mit zwei über Bridge angebundenen Nodes . . . 622
Teile einer Stretch MetroCluster Konfiguration mit zwei Nodes über eine Bridge . . . 622
Erforderliche MetroCluster Hardwarekomponenten und Namenskonventionen für über Bridge angeschlossene Stretch-Konfigurationen mit zwei Nodes . . . 623
Arbeitsblatt zur Informationssammlung für FC-to-SAS-Bridges . . . 626
Installieren und verkabeln Sie MetroCluster-Komponenten . . . 627
Installation von FC-to-SAS-Bridges und SAS-Platten-Shelves . . . 629
Konfigurieren der MetroCluster-Software in ONTAP . . . 645
Arbeitsblatt für IP-Netzwerkinformationen für Standort A . . . 646
Arbeitsblatt für IP-Netzwerkinformationen für Standort B . . . 648
Ähnlichkeiten und Unterschiede zwischen Standard-Cluster und MetroCluster Konfigurationen . . . 650
Wiederherstellung der Systemstandards und Konfiguration des HBA-Typs auf einem Controller-Modul 651
Konfigurieren von FC-VI-Ports auf einer X1132A-R6 Quad-Port-Karte auf FAS8020 Systemen . . . 653
Überprüfen der Festplattenzuweisung im Wartungsmodus in einer Konfiguration mit zwei Nodes . . . 655
Überprüfen des HA-Status von Komponenten . . . 657
Einrichten von ONTAP in einer MetroCluster Konfiguration mit zwei Nodes . . . 658
Konfigurieren der Cluster in einer MetroCluster-Konfiguration . . . 660
Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor . . . 683
Überprüfung von Umschaltung, Reparatur und Wechsel zurück . . . 683
Sichern von Backup-Dateien der Konfiguration . . . 684
Überlegungen zur Verwendung von virtuellem IP- und Border-Gateway-Protokoll mit einer MetroCluster-Konfiguration . . . 684

Testen der MetroCluster-Konfiguration . . . 687
Überprüfung der ausgehandelten Umschaltung . . . 687
Überprüfung der Heilung und manueller Umkehrschalter . . . 689
Ausfall einer einzelnen FC-to-SAS-Bridge . . . 691
Überprüfung des Betriebs nach Stromunterbrechung . . . 693
Überprüfung des Betriebs nach Ausfall eines einzelnen Storage Shelfs . . . 694
MetroCluster-Konfigurationen entfernen . . . 705
So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring . . . 706
Weitere Konfigurations- und Überwachungsfunktionen sind mit dem Active IQ Unified Manager und dem ONTAP System Manager möglich . . . 706
Synchronisieren Sie die Systemzeit mit NTP . . . 706
Überlegungen bei der Verwendung von ONTAP in einer MetroCluster-Konfiguration . . . 707
Überlegungen zur Lizenzierung . . . 708
Überlegungen zu SnapMirror . . . 708
FlexCache-Unterstützung in einer MetroCluster-Konfiguration . . . 708
FabricPool-Unterstützung in MetroCluster-Konfigurationen . . . 709
FlexGroup-Unterstützung in MetroCluster-Konfigurationen . . . 709
Job-Zeitpläne in einer MetroCluster-Konfiguration . . . 709
Cluster-Peering vom MetroCluster Standort zu einem dritten Cluster . . . 710
Replikation der LDAP-Client-Konfiguration in einer MetroCluster-Konfiguration . . . 710
Richtlinien zur Erstellung von Networking und LIF für MetroCluster Konfigurationen . . . 710
SVM Disaster Recovery in einer MetroCluster-Konfiguration . . . 714
Ausgabe der show-Befehle für die Storage-Festplatte und des Storage-Shelf zeigen-Befehle in einer Stretch-MetroCluster-Konfiguration mit zwei Nodes . . . 717
Die Ausgabe des Befehls „Plex show“ für das Storage-Aggregat ist nach einer MetroCluster-Umschaltung nicht bestimmt . . . 717
Ändern von Volumes zum Festlegen des NV-Fehler-Flags bei Umschalten . . . 717
Umstieg von einer Stretch- zu einer Fabric-Attached MetroCluster Konfiguration . . . 717
Wo Sie weitere Informationen finden . . . 718
MetroCluster und sonstige Informationen . . . 718
Installation und Konfiguration von MetroCluster Tiebreaker . . . 721
Was ist neu . . . 721
Vorgestellt Werden . . . 721
OS Support-Matrix . . . 721
Überblick über die Tiebreaker Software . . . 722
Erkennen von Ausfällen mit der NetApp MetroCluster Tiebreaker Software . . . 722
Wie die Tiebreaker Software Standortausfällen erkennt . . . 722
So erkennt die Tiebreaker Software Konnektivitätsausfälle zwischen Standorten . . . 723
Auswirkungen verschiedener Ausfalltypen auf die Tiebreaker Software-Erkennungszeit . . . 724
Über die Tiebreaker CLI und die man-Pages . . . 725
Installation der Tiebreaker Software . . . 725
Tiebraker Installations-Workflow . . . 726
Bereiten Sie sich auf die Installation der Tiebreaker Software vor . . . 726
Sicherung der Tiebreaker Host- und Datenbankinstallation . . . 727

Installieren Sie das Tiebreaker Softwarepaket . . . 731
Aktualisieren Sie den Host, auf dem der Tiebreaker Monitor ausgeführt wird . . . 816
Konfigurieren der Tiebreaker Software . . . 816
Starten der Tiebreaker Software-CLI . . . 816
Hinzufügen von MetroCluster Konfigurationen . . . 816
Befehle zum Ändern von MetroCluster Tiebreaker Konfigurationen . . . 817
Entfernen von MetroCluster-Konfigurationen . . . 818
Konfigurieren von SNMP-Einstellungen für Tiebreaker Software . . . 819
Monitoring der MetroCluster-Konfiguration . . . 821
AutoSupport wird konfiguriert . . . 821
Anzeigen des Status von Monitoring-Vorgängen . . . 823
Anzeigen von Informationen über die MetroCluster-Konfiguration . . . 825
Erstellen von Dump-Dateien . . . 825
Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus . . . 826
Firewall-Anforderungen für MetroCluster Tiebreaker . . . 826
Ereignisprotokolldateien für MetroCluster Tiebreaker . . . 827
Wo Sie weitere Informationen finden . . . 828
MetroCluster und sonstige Informationen . . . 828
MetroCluster Datensicherung und Disaster Recovery verstehen . . . 830
MetroCluster Datensicherung und Disaster Recovery verstehen . . . 830
MetroCluster Konfigurationen mit acht oder vier Nodes bieten lokalen Failover und Switchover . . . 830
Durchführen von Daten- und Konfigurations-Replizierung mit MetroCluster Konfigurationen . . . 831
Arten von Disaster- und Recovery-Methoden . . . 838
Unterbrechungsfreiem Betrieb dank MetroCluster Konfiguration mit acht oder vier Nodes . . . 840
Durchführen einer MetroCluster Konfiguration mit zwei Nodes für einen unterbrechungsfreien Betrieb 841
Überblick über den Switchover-Prozess . . . 841
Was geschieht während der Reparatur (MetroCluster FC-Konfigurationen)? . . . 849
Was geschieht während der Reparatur (MetroCluster IP-Konfigurationen)? . . . 849
Automatisches Heilen von Aggregaten in MetroCluster IP-Konfigurationen nach dem Switchover . . . 850
Erstellen von SVMs für eine MetroCluster-Konfiguration . . . 852
Was passiert während eines Switchback . . . 854
Durchführung von Umschaltung, Healing und Switchback . . . 855
Umschaltung für Tests oder Wartung . . . 855
Umschaltung für Tests oder Wartung . . . 855
Einschränkungen, wenn die MetroCluster-Konfiguration umgeschaltet wird . . . 855
Überprüfung, ob das System bereit für eine Umschaltung ist . . . 856
Senden einer individuellen AutoSupport Nachricht vor der ausgehandelten Umschaltung . . . 857
Durchführen einer ausgehandelten Umschaltung . . . 857
Vergewissern Sie sich, dass die SVMs ausgeführt werden und die Aggregate online sind . . . 860
Heilt die Konfiguration . . . 861
Zurückwechseln . . . 865
Überprüfen eines erfolgreichen Umschalttasches . . . 868
Befehle für Umschaltung, Healing und Switchback . . . 869
Verwenden Sie System Manager für Umschaltung und Switchback (nur MetroCluster IP-Konfigurationen). . . . 870

Überblick über Umschaltung und zurückwechseln . . . 870
Verwenden Sie System Manager in ONTAP 9.6 oder 9.7 für Umschaltung und Switchback . . . 871
Verwenden Sie System Manager in ONTAP 9.8 oder höher für die Umschaltung und den Wechsel zurück . . . 871
Monitoring der MetroCluster-Konfiguration . . . 873
Überprüfen der MetroCluster-Konfiguration . . . 873
Befehle zum Prüfen und Überwachen der MetroCluster-Konfiguration . . . 875
Überwachen der Konfiguration über MetroCluster Tiebreaker oder ONTAP Mediator . . . 876
Wie die NetApp MetroCluster Tiebreaker Software Ausfälle erkennt . . . 877
Überwachen und Schützen der Konsistenz des Filesystems mithilfe von NVFAIL . . . 879
Auswirkungen von NV-Fehler auf den Zugriff auf NFS-Volumes oder LUNs . . . 879
Befehle für das Monitoring von Datenverlusten . . . 880
Zugriff auf Volumes im Status „NV-Fehler“ nach einer Umschaltung . . . 881
Die Wiederherstellung von LUNs in NV-Fehler-Status nach dem Switchover erfolgt . . . 881
Wo Sie weitere Informationen finden . . . 882
MetroCluster und sonstige Informationen . . . 882
Warten der MetroCluster-Komponenten . . . 884
Weitere Informationen zur MetroCluster-Wartung . . . 884
Vorbereitung auf Wartungsaufgaben . . . 884
Wartungsverfahren für verschiedene Arten von MetroCluster Konfigurationen . . . 884
Alle anderen Wartungsverfahren . . . 884
Vorbereitung auf die MetroCluster-Wartung . . . 885
Aktivieren Sie die Konsolenprotokollierung, bevor Sie Wartungsaufgaben durchführen . . . 886
Vor der Durchführung von Wartungsarbeiten müssen Sie den ONTAP Mediator oder den Tiebreaker Monitoring entfernen . . . 886
MetroCluster-Fehlerszenarien und Recovery . . . 887
Mit dem Interoperabilitäts-Matrix-Tool finden Sie MetroCluster Informationen . . . 888
Wartungsverfahren für MetroCluster FC-Konfigurationen . . . 889
Ändern Sie eine Switch- oder ATTO Bridge-IP-Adresse für die Statusüberwachung . . . 889
FC-to-SAS-Bridge-Wartung . . . 890
Wartung und Austausch von FC-Switches . . . 952
Unterbrechungsfreier Austausch eines Shelfs in einer Fabric-Attached MetroCluster-Konfiguration . . . 1002
Hot-Add-Storage zu einer MetroCluster-FC-Konfiguration . . . 1007
Hot-Removing Storage aus einer MetroCluster FC-Konfiguration . . . 1030
Schalten Sie einen einzelnen Standort in einer MetroCluster FC-Konfiguration aus und wieder ein . . . 1034
Herunterfahren einer gesamten MetroCluster FC-Konfiguration . . . 1048
Wartungsverfahren für MetroCluster IP-Konfigurationen . . . 1050
Wartung und Austausch von IP-Switches . . . 1050
Identifizierung des Storage in einer MetroCluster IP-Konfiguration . . . 1076
Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von Shared Storage MetroCluster Switches . . . 1080
Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration . . . 1096
Schalten Sie einen einzelnen Standort in einer MetroCluster IP-Konfiguration aus und wieder ein . . . 1100
Ausschalten einer gesamten MetroCluster IP-Konfiguration . . . 1107
Wartungsverfahren für alle MetroCluster Konfigurationen . . . 1109
Unterbrechungsfreies Ersetzen eines Shelfs in einer Stretch-MetroCluster-Konfiguration . . . 1109

Wann werden Root-Volumes zu einem neuen Ziel migriert . . . 1111
Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen . . . 1112
Umbenennen eines Clusters in MetroCluster-Konfigurationen . . . 1115
Überprüfen Sie den Funktionszustand einer MetroCluster-Konfiguration . . . 1117
Wo Sie weitere Informationen finden . . . 1120
Umstellung von MetroCluster FC auf MetroCluster IP . . . 1121
Wählen Sie Ihr Übergangsverfahren . . . 1121
Unterstützte Plattformkombinationen . . . 1121
Wählen Sie Ihr Übergangsverfahren . . . 1123
Unterbrechungsfreier Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration (ONTAP 9.8 und höher) . . . 1124
Unterbrechungsfreier Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration (ONTAP 9.8 und höher) . . . 1124
Vorbereitung auf den Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration . . . 1125
Umstellung von MetroCluster FC- auf MetroCluster IP-Konfigurationen . . . 1136
Senden einer benutzerdefinierten AutoSupport Meldung nach der Wartung . . . 1190
Wiederherstellen der Tiebreaker- oder Mediator-Überwachung . . . 1190
Unterbrechungsfreier Übergang von einer MetroCluster FC Konfiguration mit zwei Nodes auf eine MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher) . . . 1190
Unterbrechungsfreie Umstellung von einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher) . . . 1190
Beispiel für die Benennung in diesem Verfahren . . . 1191
Vorbereitung auf den Umstieg mit FC-to-IP und Störungen . . . 1192
Umstellung der MetroCluster FC Nodes . . . 1201
Anschließen der MetroCluster IP-Controller-Module . . . 1210
Konfiguration der neuen Nodes und Abschluss des Übergangs . . . 1226
Stellt den normalen Betrieb des Systems wieder her . . . 1233
Unterbrechungsfreier Übergang von MetroCluster FC auf MetroCluster IP beim Ausmustern von Storage Shelves (ONTAP 9.8 und höher) . . . 1234
Aktivieren Sie die Konsolenprotokollierung . . . 1235
Anforderungen für den Umstieg beim Ausmustern alter Shelfs . . . 1235
Workflow für Unterbrechungen beim Verschieben von Daten und Aussortieren alter Storage Shelves 1236
Umstellung der Konfiguration . . . 1236
Migration der Root-Aggregate . . . 1237
Und die Daten-Aggregate migrieren . . . 1238
Ausmustern von Shelfs, die von Node_A_1-FC und Node_A_2-FC verschoben wurden . . . 1238
Übergang abschließen . . . 1240
Unterbrechungsfreie Transition, wenn vorhandene Shelfs nicht auf neuen Controllern unterstützt werden (ONTAP 9.8 und höher) . . . 1240
Aktivieren Sie die Konsolenprotokollierung . . . 1240
Anforderungen für den Umstieg, wenn Shelfs auf den neuen Nodes nicht unterstützt werden . . . 1241
Workflow für Unterbrechungen beim Übergang, wenn Shelfs nicht von neuen Controllern unterstützt werden . . . 1242
Vorbereiten der neuen Controller-Module . . . 1242
Anschließen der neuen Platten-Shelfs an die vorhandenen MetroCluster FC-Controller . . . 1243

Migrieren Sie Root-Aggregate und verschieben Sie Daten in die neuen Platten-Shelves . . . 1243
Umstellung der Konfiguration . . . 1249
Verschieben eines FC SAN-Workloads von MetroCluster FC- zu MetroCluster IP-Nodes . . . 1250
Verschieben Sie einen FC SAN-Workload von MetroCluster FC auf MetroCluster IP Nodes . . . 1250
Verschieben Sie Linux iSCSI-Hosts von MetroCluster FC zu MetroCluster IP-Knoten . . . 1257
Schritt 1: Einrichtung neuer iSCSI-Verbindungen . . . 1257
Schritt 2: Fügen Sie die neuen Knoten als Reporting-Knoten . . . 1261
Schritt 3: Entfernen Sie Reporting Nodes und scannen Sie Pfade neu . . . 1266
Wo Sie weitere Informationen finden . . . 1268
MetroCluster und sonstige Informationen . . . 1268
Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration . . . 1271
Beginnen Sie hier - Wählen Sie Ihre Prozedur . . . 1271
Hier starten: Sie haben die Wahl zwischen Controller-Upgrade, Systemaktualisierung oder Erweiterung . . . 1271
Wählen Sie ein Controller-Upgrade-Verfahren . . . 1272
Auswahl der Methode zur Systemaktualisierung . . . 1278
Wählen Sie ein Erweiterungsverfahren aus . . . 1283
Controller-Upgrades in MetroCluster IP mit vier Nodes mithilfe von Switchover und Switchback mit Befehlen, die den System-Controller ersetzen (ONTAP 9.13.1 und höher) . . . 1283
Workflow für das Upgrade von MetroCluster IP-Controllern mithilfe von Befehlen „System Controller Replace“ (ONTAP 9.13.1 oder höher) . . . 1283
Upgrade wird vorbereitet . . . 1284
Upgrade Ihrer Controller . . . 1297
Schließen Sie das MetroCluster IP-Controller-Upgrade ab . . . 1323
Controller-Upgrade in MetroCluster IP durch Switchover und Switchback (ONTAP 9.8 und höher) . . . 1325
Workflow für MetroCluster IP-Controller-Upgrades mithilfe von Switchover und Switchback (ONTAP 9.8 und höher) . . . 1325
Upgrade wird vorbereitet . . . 1326
Upgrade Ihrer Controller . . . 1340
Schließen Sie das MetroCluster IP-Controller-Upgrade ab . . . 1368
Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher) . . . 1370
Aktivieren Sie die Konsolenprotokollierung . . . 1371
Workflow für das Upgrade von Controllern in einer MetroCluster IP-Konfiguration . . . 1372
Bereiten Sie sich auf das Upgrade vor . . . 1372
Wechseln Sie über die MetroCluster-Konfiguration . . . 1378
Entfernen Sie das Controller-Modul der AFF A700 oder FAS9000 Plattform und NVS . . . 1380
Installieren Sie die AFF A900- oder FAS9500 NVS- und Controller-Module . . . 1381
Aktualisieren Sie die RCF-Dateien des Switches, um die neuen Plattformen aufzunehmen . . . 1388
Konfigurieren Sie die neuen Controller . . . 1388
Schalten Sie die MetroCluster-Konfiguration zurück . . . 1397
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration . . . 1399
Aktualisieren Sie die Knoten auf site_A . . . 1400
Stellen Sie die Tiebreaker- oder Mediator-Überwachung wieder her . . . 1400
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung . . . 1401

Aktualisieren Sie Controller in einer MetroCluster FC Konfiguration mithilfe von Switchover und Switchback . . . 1401
Unterstützte Plattformkombinationen . . . 1401
Über diese Aufgabe . . . 1401
Aktivieren Sie die Konsolenprotokollierung . . . 1402
Bereiten Sie sich auf das Upgrade vor . . . 1403
Wechseln Sie über die MetroCluster-Konfiguration . . . 1409
Vorbereiten der Netzwerkkonfiguration der alten Controller . . . 1411
Entfernen Sie die alten Plattformen . . . 1413
Konfigurieren Sie die neuen Controller . . . 1413
Schalten Sie die MetroCluster-Konfiguration zurück . . . 1425
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration . . . 1427
Aktualisieren Sie die Nodes auf Cluster_A . . . 1428
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung . . . 1428
Wiederherstellung des Tiebreaker Monitoring . . . 1428
Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher) . . . 1428
Aktivieren Sie die Konsolenprotokollierung . . . 1430
Bereiten Sie sich auf das Upgrade vor . . . 1430
Steckplatz 7 am AFF A700 Controller löschen . . . 1430
Wechseln Sie über die MetroCluster-Konfiguration . . . 1437
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul und den NVS an Site_B . . . 1439
Entfernen Sie das Controller-Modul und den NVS von beiden Nodes an Site_B . . . 1439
Installieren Sie das AFF A900 oder FAS9500 NVS und das Controller-Modul . . . 1441
Schalten Sie die MetroCluster-Konfiguration zurück . . . 1454
Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration . . . 1455
Aktualisieren Sie die Knoten auf site_A . . . 1456
Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung . . . 1456
Wiederherstellung des Tiebreaker Monitoring . . . 1457
Aktualisieren Sie Controller in einer MetroCluster FC-Konfiguration mit vier Knoten mithilfe von Switchover und Switchback mit den Befehlen „System Controller Replace“ (ONTAP 9.10.1 und höher). 1457
Unterstützte Plattformkombinationen . . . 1457
Über diese Aufgabe . . . 1457
Aktivieren Sie die Konsolenprotokollierung . . . 1458
Bereiten Sie sich auf das Upgrade vor . . . 1458
Ersetzen Sie die alten Controller, und starten Sie die neuen Controller . . . 1462
Schließen Sie das Upgrade ab . . . 1474
Aktualisieren Sie die Nodes auf Cluster_A . . . 1475
Aktualisieren einer MetroCluster FC-Konfiguration mit vier Nodes . . . 1475
Aktivieren Sie die Konsolenprotokollierung . . . 1475
Führen Sie das Aktualisierungsverfahren durch . . . 1476
Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher) . . . 1478
Aktivieren Sie die Konsolenprotokollierung . . . 1480
Führen Sie das Aktualisierungsverfahren durch . . . 1480
Erweitern Sie eine MetroCluster FC Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes 1489

Erweitern einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes 1489
Aktivieren Sie die Konsolenprotokollierung . . . 1491
Überprüfen des Status der MetroCluster-Konfiguration . . . 1491
Senden einer benutzerdefinierten AutoSupport Meldung, bevor Nodes zur MetroCluster Konfiguration hinzugefügt werden . . . 1493
Zoning für die neuen Controller-Ports beim Hinzufügen eines Controller-Moduls in einer Fabric-Attached MetroCluster-Konfiguration . . . 1494
Fügen Sie jedem Cluster ein neues Controller-Modul hinzu . . . 1494
Aktualisierung der MetroCluster Konfiguration durch neue Controller . . . 1527
Aktivieren von Storage Failover auf beiden Controller-Modulen und Aktivieren von Cluster HA . . . 1530
Starten Sie die SVMs neu . . . 1531
Erweitern Sie eine MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes 1531
Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes 1532
Aktivieren Sie die Konsolenprotokollierung . . . 1534
Bestimmen des neuen Verkabelungslayouts . . . 1534
Die neue Ausrüstung in den Racks zu bringen . . . 1535
Überprüfen des Systemzustands der MetroCluster-Konfiguration . . . 1535
Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor . . . 1537
Senden einer benutzerdefinierten AutoSupport Meldung vor dem Hinzufügen von Nodes zur MetroCluster Konfiguration . . . 1537
Reverkable und Zone A Switch Fabric für die neuen Nodes . . . 1538
Konfigurieren Sie ONTAP auf den neuen Controllern . . . 1539
Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor . . . 1569
Senden einer benutzerdefinierten AutoSupport Meldung nach dem Hinzufügen von Nodes zur MetroCluster Konfiguration . . . 1569
Überprüfung von Umschaltung, Reparatur und Wechsel zurück . . . 1570
Erweitern Sie eine MetroCluster IP-Konfiguration . . . 1570
Aktivieren Sie die Konsolenprotokollierung . . . 1572
Beispiel für die Benennung in diesem Verfahren . . . 1572
Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe . . . 1572
Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung . . . 1575
Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe . . . 1576
Überprüfen des Systemzustands der MetroCluster-Konfiguration . . . 1577
Entfernen der Konfiguration aus Überwachungsanwendungen . . . 1581
Vorbereiten der neuen Controller-Module . . . 1582
RCF-Dateien aktualisieren . . . 1582
Verbinden Sie die neuen Nodes mit den Clustern . . . 1584
Konfigurieren von Intercluster-LIFs, Erstellen der MetroCluster-Schnittstellen und Spiegeln von Root-Aggregaten . . . 1586
Beenden des Hinzufügung der neuen Nodes . . . 1598
Entfernen einer Disaster Recovery-Gruppe . . . 1604
Aktivieren Sie die Konsolenprotokollierung . . . 1605
Entfernen der DR-Gruppen-Nodes aus jedem Cluster . . . 1606
Wo Sie weitere Informationen finden . . . 1609
MetroCluster und sonstige Informationen . . . 1609

Nach einem Ausfall wiederherstellen . . . 1612
Workflow für Disaster Recovery . . . 1612
Durchführen einer erzwungenen Umschaltung nach einem Ausfall . . . 1612
Fechten vor dem Disaster-Standort . . . 1612
Erzwungene Umschaltung durchführen . . . 1613
Die Ausgabe des Befehls „Plex show“ für das Storage-Aggregat ist nach einer MetroCluster-Umschaltung nicht bestimmt . . . 1614
Zugriff auf Volumes im Status „NV-Fehler“ nach einer Umschaltung . . . 1614
Auswahl des richtigen Wiederherstellungsverfahrens . . . 1615
Ausfallszenarien für Controller-Module während der MetroCluster-Installation . . . 1616
Ausfallszenarien für Controller-Module bei der Umstellung von MetroCluster FC zu IP . . . 1616
Szenarien für Controller-Module in MetroCluster Konfigurationen mit acht Nodes . . . 1616
Szenarien für Fehler im Controller-Modul in MetroCluster-Konfigurationen mit zwei Nodes . . . 1620
Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall . . . 1621
Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall . . . 1621
Aktivieren Sie die Konsolenprotokollierung . . . 1622
Ersetzen Sie die Hardware und starten Sie neue Controller . . . 1622
Bereiten Sie den Wechsel zurück in einer MetroCluster IP-Konfiguration vor . . . 1635
Bereiten Sie sich auf den Wechsel zurück in einer MetroCluster FC-Konfiguration vor . . . 1680
Vorbereitung auf den Wechsel zurück in einer heterogenen Konfiguration (Recovery während des Übergangs) . . . 1708
Wiederherstellung abgeschlossen . . . 1711
Wiederherstellung nach einem Ausfall eines Controllers . . . 1725
Aktivieren Sie die Konsolenprotokollierung . . . 1725
Reparatur der Konfiguration in einer MetroCluster-Konfiguration . . . 1726
Überprüfen, ob das System für einen Wechsel bereit ist . . . 1728
Zurückwechseln . . . 1730
Überprüfen eines erfolgreichen Umschalttasches . . . 1732
Löschen von veralteten Aggregat-Auflistungen nach dem Wechsel zurück . . . 1734
Rechtliche Hinweise . . . 1737
Urheberrecht . . . 1737
Marken . . . 1737
Patente . . . 1737
Datenschutzrichtlinie . . . 1737
Sicherheitsinformationen und gesetzliche Hinweise . . . 1737

MetroCluster-Dokumentation

Versionshinweise zu MetroCluster

Neuerungen bei MetroCluster

Jede neue Version der Datenmanagement-Software ONTAP 9 verfügt über neue und erweiterte Funktionen, die die Leistungsfähigkeit, Managebarkeit und Performance von ONTAP MetroCluster Konfigurationen verbessern.

Details zu bekannten Problemen, Einschränkungen und Warnungen zu Upgrades, die ONTAP MetroCluster-Konfigurationen betreffen, finden Sie im "Versionshinweise zu ONTAP 9". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
MetroCluster IP-Unterstützung für End-to-End-Verschlüsselung	Auf den folgenden Systemen wird die End-to-End-Verschlüsselung unterstützt, um Back-End-Datenverkehr, wie z. B. NVlog- und Speicherreplikationsdaten, zwischen den Standorten in einer MetroCluster -IP-Konfiguration zu verschlüsseln. • AFF A800, AFF C800 • AFF A20, AFF A30, AFF C30, AFF A50, AFF C60 • AFF A70, AFF A90, AFF A1K, AFF C80 • FAS50, FAS70 UND FAS90 "Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration"	ONTAP 9.17.1

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
Begrenzung von Änderungen für MetroCluster IP-Konfigurationen	ONTAP 9.17.1 enthält die folgenden Grenzwertaktualisierungen für MetroCluster -IP-Konfigurationen mit vier Knoten: • Für die Systeme AFF C800, AFF A800, AFF A900, AFF A90 und AFF A1K gelten die folgenden aktualisierten Grenzwerte: ◦ FlexVol volume pro Knoten: 1250 ◦ SVM-Limits: 64 SVMs pro Cluster ◦ LIF-Anzahl: 256 LIFs pro Cluster • Für die Systeme AFF A400, AFF C400, ASA A400, ASA C400, AFF C80, AFF A70 und AFF A50 gelten die folgenden aktualisierten Grenzwerte: ◦ FlexVol volume Volumenlimits pro Aggregat (einzeln oder mehrfach): 625 ◦ FlexVol volume pro Knoten: 1250 ◦ FlexVol volume -Limits pro Hochverfügbarkeitspaar (HA): 2500 ◦ FlexVol volume pro Cluster: 5000 ◦ SVM-Limits: 64 SVMs pro Cluster ◦ LIF-Anzahl: 256 LIFs pro Cluster Weitere Informationen finden Sie im "Hardware Universe" für weitere Informationen.	ONTAP 9.17.1
FibreBridge-Firmware-Update mit Anmeldeinformationen	Sie können die Firmware auf FibreBridge-Brücken mithilfe von Anmeldeinformationen aktualisieren, wenn diese vom Server zum Herunterladen des Firmware-Pakets benötigt werden. "Aktualisieren Sie die Firmware auf einer FibreBridge-Bridge"	ONTAP 9.16.1
Unterstützung der SVM-Datenmobilität für die Migration von MetroCluster Konfigurationen	ONTAP unterstützt die folgenden MetroCluster SVM-Migrationen: • Migration einer SVM zwischen einem nicht-MetroCluster HA-Paar und einer MetroCluster IP-Konfiguration • Migrieren einer SVM zwischen zwei MetroCluster IP-Konfigurationen • Migration einer SVM zwischen einer MetroCluster FC-Konfiguration und einer MetroCluster IP-Konfiguration "SVM-Datenmobilität"	ONTAP 9.16.1

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
MD5-Authentifizierungsunterstützung für BGP-Peer-Gruppen	ONTAP unterstützt MD5-Authentifizierung auf BGP-Peer-Gruppen zum Schutz von BGP-Sitzungen. Wenn MD5 aktiviert ist, können BGP-Sitzungen nur unter autorisierten Peers eingerichtet und verarbeitet werden, um mögliche Unterbrechungen der Sitzung durch einen nicht autorisierten Schauspieler zu verhindern. "Konfigurieren Sie Virtual IP (VIP) LIFs"	ONTAP 9.16.1
MetroCluster IP-Unterstützung für End-to-End-Verschlüsselung	Die End-to-End-Verschlüsselung wird auf den Systemen AFF A400, FAS8300 und FAS8700 unterstützt, um den Back-End-Datenverkehr, wie NVLOG- und Storage-Replizierungsdaten, zwischen den Standorten einer MetroCluster IP-Konfiguration zu verschlüsseln. "Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration"	ONTAP 9.15.1
Erhöhung der Volume-Begrenzung bei MetroCluster IP Konfigurationen mit vier Nodes auf AFF A800 und AFF C800 Systemen	In MetroCluster IP-Konfigurationen mit vier Nodes haben die folgenden Volume-Grenzwerte für AFF A800 und AFF C800 Systeme zugenommen: • Die maximale Anzahl von FlexVol Volumes pro Aggregat stieg von 200 auf 625. • Die maximale Anzahl von FlexVol Volumes pro Node stieg von 800 auf 1250. • Die maximale Anzahl von FlexVol -Volumes pro HA-Paar wurde von 1600 auf 2500 erhöht.	ONTAP 9.15.1
MetroCluster IP-Unterstützung für NVMe	Das NVMe/TCP-Front-End-Hostprotokoll wird auf MetroCluster IP-Konfigurationen mit vier Nodes unterstützt. "SAN-Konfigurationen in einer MetroCluster Umgebung"	ONTAP 9.15.1
Erhöhung der Volume-Begrenzung für MetroCluster IP Konfigurationen mit vier Nodes auf AFF A900 Systemen	In MetroCluster IP-Konfigurationen mit vier Nodes haben die folgenden Volume-Einschränkungen für AFF A900-Systeme zugenommen: • Die maximale Anzahl von FlexVol Volumes pro Aggregat stieg von 200 auf 625. • Die maximale Anzahl von FlexVol Volumes pro Node stieg von 800 auf 1250. • Die maximale Anzahl von FlexVol -Volumes pro HA-Paar wurde von 1600 auf 2500 erhöht.	ONTAP 9.14.1

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
Unterstützung für S3 Objekt-Storage auf gespiegelten und nicht gespiegelten Aggregaten	Sie können einen S3-Objekt-Storage-Server auf einer SVM in einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster IP- und FC-Konfigurationen aktivieren. "S3-Unterstützung mit MetroCluster"	ONTAP 9.14.1
Unterstützung für die Bereitstellung eines S3-Buckets auf gespiegelten und nicht gespiegelten Aggregaten in einem MetroCluster-Cluster	Sie können einen Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster Konfigurationen erstellen. "Erstellung eines ONTAP S3 Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration"	ONTAP 9.14.1
Wechsel von MetroCluster FC zu MetroCluster IP mit einem Shared Switch für MetroCluster IP und Ethernet Attached Storage	Mit einem Shared Storage Switch können Sie unterbrechungsfrei von einer MetroCluster FC auf eine MetroCluster IP-Konfiguration umstellen. "Unterbrechungsfreier Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration (ONTAP 9.8 und höher)"	ONTAP 9.13.1
Unterbrechungsfreier Wechsel von einer MetroCluster FC Konfiguration mit acht Nodes zu einer MetroCluster IP Konfiguration	Workloads und Daten lassen sich unterbrechungsfrei von einer bestehenden MetroCluster FC Konfiguration mit acht Nodes auf eine neue MetroCluster IP Konfiguration übertragen. "Unterbrechungsfreier Wechsel von einer MetroCluster FC zu einer MetroCluster IP Konfiguration"	ONTAP 9.13.1
Upgrades der MetroCluster IP-Konfiguration mit vier Nodes unter Verwendung von Switchover und Switchback	Sie können Controller in einer MetroCluster IP Konfiguration mit vier Nodes mithilfe von Switchover und Switchback mit aktualisieren `system controller replace` Befehle. "Aktualisieren Sie Controller in einer MetroCluster IP-Konfiguration mit vier Nodes"	ONTAP 9.13.1

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
Die automatische, vom Mediator unterstützte, ungeplante Umschaltung (MAUSO) wird für eine Abschaltung in der Umgebung ausgelöst	Wenn ein Standort aufgrund einer Abschaltung in der Umgebung ordnungsgemäß heruntergefahren wird, wird MAUSO ausgelöst. "Wie der ONTAP Mediator die automatische ungeplante Umschaltung unterstützt"	ONTAP 9.13.1
Unterstützung von MetroCluster IP-Konfigurationen mit acht Nodes	Sie können die Controller und den Speicher in einer MetroCluster IP-Konfiguration mit acht Nodes aktualisieren, indem Sie die Konfiguration auf eine temporäre Konfiguration mit zwölf Nodes erweitern und dann die alten DR-Gruppen entfernen. "Aktualisieren einer MetroCluster IP-Konfiguration mit vier Nodes"	ONTAP 9.13.1
Konvertierung der MetroCluster IP-Konfiguration in eine MetroCluster Switch-Konfiguration für gemeinsam genutzten Storage	Sie können eine MetroCluster IP-Konfiguration in eine MetroCluster Switch-Konfiguration mit gemeinsamem Speicher konvertieren. "Ersetzen Sie einen IP-Switch"	ONTAP 9.13.1
Die automatische Umschaltung von MetroCluster in einer MetroCluster IP-Konfiguration	Sie können die automatische erzwungene Umschaltung von MetroCluster in einer MetroCluster IP-Konfiguration aktivieren. Bei dieser Funktion handelt es sich um eine Erweiterung der MAUSO-Funktion (Mediator-Assisted ungeplante Switchover). "Einschränkungen bei der automatischen Umschaltung"	ONTAP 9.12.1
S3 auf einer SVM auf einem nicht gespiegeltes Aggregat in einer MetroCluster IP-Konfiguration	Sie können einen S3-Objekt-Storage-Server (ONTAP Simple Storage Service) auf einer SVM in einem nicht gespiegeltes Aggregat in einer MetroCluster IP-Konfiguration aktivieren. "S3-Unterstützung mit MetroCluster"	ONTAP 9.12.1
MetroCluster IP-Unterstützung für NVMe	Das NVMe/FC-Protokoll wird auf MetroCluster IP-Konfigurationen mit vier Nodes unterstützt. "SAN-Konfigurationen in einer MetroCluster Umgebung"	ONTAP 9.12.1

Unterstützte Funktionen in der MetroCluster-Konfiguration	Beschreibung und wo man mehr erfahren kann	Verfügbar ab
IPsec-Unterstützung für Front-End-Hostprotokolle in MetroCluster-IP- und MetroCluster-Fabric-Attached-Konfigurationen	IPsec-Unterstützung für das Front-End-Hostprotokoll (wie NFS und iSCSI) ist in MetroCluster IP- und MetroCluster-Fabric-Attached-Konfigurationen verfügbar. "Konfigurieren Sie IP-Sicherheit (IPsec) über die Verschlüsselung über das Netzwerk"	ONTAP 9.12.1
Wechseln Sie von einer MetroCluster FC-Konfiguration zu einer AFF A250- oder FAS500f MetroCluster IP-Konfiguration	Sie können von einer MetroCluster FC Konfiguration auf eine AFF A250 oder FAS500f MetroCluster IP Konfiguration umsteigen. "Verschieben Sie die lokalen Cluster-Verbindungen"	ONTAP 9.11.1
Konsistenzgruppen	Konsistenzgruppen werden in MetroCluster-Konfigurationen unterstützt. "Konsistenzgruppen in MetroCluster Konfigurationen"	ONTAP 9.11.1
Vereinfachtes Controller Upgrade von Nodes in einer MetroCluster FC-Konfiguration	Das Upgrade-Verfahren mit Switchover und Switchback wurde vereinfacht. "Aktualisieren Sie Controller in einer MetroCluster FC Konfiguration mithilfe von Switchover und Switchback"	ONTAP 9.10.1
IP-Unterstützung für gemeinsame Links auf Layer 3	MetroCluster IP-Konfigurationen können mit IP-gerouteten Back-End-Verbindungen (Layer 3) implementiert werden. "Überlegungen für Layer 3-Weitbereichs-Netzwerke"	ONTAP 9.9.1
Unterstützung von MetroCluster Konfigurationen mit acht Nodes	Permanente Cluster mit acht Nodes werden in IP- und Fabric-Attached MetroCluster-Konfigurationen unterstützt. "Installieren und verkabeln Sie MetroCluster-Komponenten"	ONTAP 9.9.1

Neuerungen bei der MetroCluster IP Plattform und Switch-Unterstützung

Informieren Sie sich über die Neuerungen bei der MetroCluster-IP-Plattform und Switch-Unterstützung.

Plattform-Support

Unterstützte Plattformen in MetroCluster IP-Konfigurationen	Verfügbar ab
FAS50	ONTAP 9.16.1GA
AFF A20, AFF A30, AFF A50, AFF C30, AFF C60, AFF C80	ONTAP 9.16.1
FAS70, FAS90	ONTAP 9.15.1P3
AFF A70, AFF A90, AFF A1K	ONTAP 9.15.1
ASA A150, ASA A250, ASA A400, ASA A800, ASA A900 ASA C250, ASA C400, ASA C800	ONTAP 9.14.1
AFF A150	ONTAP 9.13.1 ONTAP 9.12.1P1 ONTAP 9.11.1P8 ONTAP 9.10.1P12
AFF C250, AFF C400, AFF C800	ONTAP 9.12.1P1 ONTAP 9.13.1 GA
AFF A900	ONTAP 9.10.1
AFF A250	ONTAP 9.8
FAS500f	ONTAP 9.8
ASA AFF A220, ASA AFF A250, ASA AFF A400, ASA AFF A700, ASA AFF A800	ONTAP 9.7
AFF A320	ONTAP 9.6P3
AFF A220, FAS2750	ONTAP 9.6
AFF A300, FAS8200	ONTAP 9.5

Switch-Support

Broadcom-IP-Switches	Verfügbar ab
BES-53248	ONTAP 9.6

Cisco IP-Switches	Verfügbar ab
9336C-FX2 (12 Anschlüsse)	ONTAP 9.14.1
9336C-FX2 (36 Anschlüsse)	ONTAP 9.8
3132Q-V	ONTAP 9.6
3232C	ONTAP 9.6

NVIDIA-Switches	Verfügbar ab
Mehrere MetroCluster IP-Konfigurationen auf demselben NVIDIA SN2100-Switch	ONTAP 9.14.1
SN2100	ONTAP 9.12.1

Neuerungen bei der MetroCluster FC Plattform und Switch-Unterstützung

Plattform-Support

In MetroCluster FC-Konfigurationen unterstützte Plattformen	Verfügbar ab
AFF A900	ONTAP 9.10.1
ASA AFF A700 und ASA AFF A400	ONTAP 9.7P5
AFF A400 und FAS8300	ONTAP 9.7
AFF A300 UND FAS8200	ONTAP 9.5

Switch-Support

Brocade FC-Switches	Verfügbar ab
G710	ONTAP 9.17.1
G720	ONTAP 9.8

Brocade FC-Switches	Verfügbar ab
G620-1, G630-1	ONTAP 9.8
G630	ONTAP 9.6

Was ist neu in ONTAP Mediator Unterstützung

Mit jeder Version werden neue Verbesserungen für ONTAP Mediator bereitgestellt. Was ist neu?

Weitere Informationen zur Installation oder Aktualisierung von ONTAP Mediator in Ihrer MetroCluster-Konfiguration finden Sie unter "Vorbereiten der Installation von ONTAP Mediator" .

ONTAP Mediator-Fähigkeit	ONTAP-Version
Bei einer Abschaltung in der Umgebung wird die mediatorgestützte automatische ungeplante Umschaltung (Mediator-Assisted Automatic ungeplante Switchover, MAUSO) unterstützt. Wenn ein Standort aufgrund einer Abschaltung in der Umgebung ordnungsgemäß heruntergefahren wird, wird MAUSO ausgelöst. "So unterstützt ONTAP Mediator automatische ungeplante Switchover"	ONTAP 9.13.1
Erste Unterstützung für ONTAP Mediator in MetroCluster-IP-Konfigurationen	ONTAP 9.7

Neuerungen beim MetroCluster Tiebreaker Support

Jede Version enthält Erweiterungen der MetroCluster Tiebreaker Software. Die aktuellen Versionen von MetroCluster Tiebreak enthalten alle Neuigkeiten.

Vorgestellt Werden

ONTAP Tiebreaker Version	Vorgestellt Werden
1.6P1	• Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.6	• Einfachere Installation • Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.5	• Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit

1.4	• Aktualisierung der unterstützenden Bibliotheken

OS Support-Matrix

Die folgende Tabelle zeigt die unterstützten Betriebssysteme für die einzelnen Versionen von Tiebreaker.

Betriebssystem für Tiebreaker	1.6P1	1.6	1.5	1.4
Rocky Linux 9.4	Ja.	Nein	Nein	Nein
Rocky Linux 9.0	Nein	Ja.	Nein	Nein
Rocky Linux 8.10	Ja.	Nein	Nein	Nein
Red Hat Enterprise Linux (RHEL) 9.5	Ja.	Nein	Nein	Nein
RHEL 9.4	Ja.	Nein	Nein	Nein
RHEL 9.3	Nein	Nein	Nein	Nein
RHEL 9.2	Ja.	Ja.	Nein	Nein
RHEL 9.1	Nein	Ja.	Nein	Nein
RHEL 9.0	Nein	Ja.	Nein	Nein
RHEL 8.11 – 9.0	Nein	Ja.	Nein	Nein
RHEL 8.10	Ja.	Ja.	Nein	Nein
RHEL 8.9	Nein	Ja.	Nein	Nein
RHEL 8.8	Ja.	Ja.	Nein	Nein
RHEL 8.1 – 8.7	Nein	Ja.	Ja.	Ja.
RHEL 7 – 7.9	Nein	Nein	Nein	Ja.
CentOS 7 - 7.9	Nein	Nein	Nein	Ja.

Installieren Sie eine Fabric-Attached MetroCluster

Überblick

Um Ihre Fabric-Attached 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".
- "Verkabeln Sie die Komponenten"
- "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[1]	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 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.

Hinweise

1. Lesen Sie die folgenden Überlegungen für MetroCluster IP-Konfigurationen mit acht Nodes:
    - 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.

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 für ISLs

Sie müssen ermitteln, wie viele ISLs in der MetroCluster Konfiguration für jedes FC Switch Fabric benötigt werden. Ab ONTAP 9.2 können Sie in einigen Fällen nicht mehr FC Switches und ISLs für jede MetroCluster Konfiguration einteilen, sondern dieselben vier Switches teilen.

Überlegungen zur ISL-Freigabe (ONTAP 9.2)

Ab ONTAP 9.2 ist ISL-Freigabe in den folgenden Fällen möglich:

- Ein MetroCluster-Konfigurationen mit zwei und einem Node und vier Nodes
- Zwei separate MetroCluster Konfigurationen mit vier Nodes
- Zwei separate MetroCluster-Konfigurationen mit zwei Nodes
- Zwei DR-Gruppen innerhalb einer MetroCluster Konfiguration mit acht Nodes

Die Anzahl der erforderlichen ISLs zwischen den Shared Switches hängt von der Bandbreite der mit den Shared Switches verbundenen Plattformmodelle ab.

Berücksichtigen Sie die folgenden Aspekte Ihrer Konfiguration, wenn Sie bestimmen, wie viele ISLs Sie benötigen.

- Geräte anderer Anbieter sollten nicht mit einem der FC-Switches verbunden werden, die die Back-End-MetroCluster-Konnektivität bieten.
- ISL-Freigabe wird bei allen Switches unterstützt, mit Ausnahme der Switches Cisco 9250i und Cisco 9148.
- Alle Nodes müssen ONTAP 9.2 oder höher ausführen.
- Die FC-Switch-Verkabelung für ISL-Freigabe entspricht der für die MetroCluster-Verkabelung mit acht Nodes.
- Die RCF-Dateien für ISL-Freigabe entsprechen denen für die MetroCluster-Verkabelung mit acht Nodes.
- Sie sollten überprüfen, ob alle Hardware- und Softwareversionen unterstützt werden.

  "NetApp Hardware Universe"

- Die Geschwindigkeit und die Anzahl der ISLs müssen Größe aufweisen, um die Client-Auslastung auf beiden MetroCluster Systemen zu unterstützen.
- Die Back-End-ISLs und die Back-End-Komponenten müssen ausschließlich der MetroCluster Konfiguration zugewiesen sein.
- Die ISL muss eine der unterstützten Geschwindigkeiten nutzen: 4 Gbit/s, 8 Gbit/s, 16 Gbit/s oder 32 Gbit/s.
- Die ISLs in einem Fabric sollten alle dieselbe Geschwindigkeit und Länge aufweisen.
- Die ISLs in einem Fabric sollten alle dieselbe Topologie haben. Sie sollten beispielsweise alle direkte Links sein, oder wenn Ihr System WDM verwendet, sollten sie alle WDM verwenden.

Plattformspezifische ISL-Überlegungen

Die Anzahl der empfohlenen ISLs ist plattformspezifisch. Die folgende Tabelle zeigt die ISL-Anforderungen für jedes Fabric nach Plattformmodell. Dabei wird davon ausgegangen, dass jede ISL eine Kapazität von 16 Gbit/s hat.

Modell der Plattform	Empfohlene Anzahl von ISLs pro DR-Gruppe mit vier Nodes (pro Switch Fabric)
AFF A900 UND FAS9500	Acht
AFF A700	Sechs
FAS9000	Sechs
8080	Vier
Alle anderen	Zwei

Wenn das Switch-Fabric acht Nodes unterstützt (eines Teils einer MetroCluster-Konfiguration mit acht Nodes oder zwei Konfigurationen mit vier Nodes, die ISLs teilen), wird die empfohlene Gesamtzahl an ISLs für das Fabric die Summe der erforderlichen ISLs für jede DR-Gruppe mit vier Nodes angegeben. Beispiel:

- Enthält die DR-Gruppe 1 vier AFF A700 Systeme, sind sechs ISLs erforderlich.
- Wenn DR-Gruppe 2 vier FAS8200 Systeme enthält, sind zwei ISLs erforderlich.
- Die Gesamtzahl der empfohlenen ISLs für das Switch Fabric beträgt acht.

Überlegungen bei der Verwendung von TDM/WDM-Geräten mit Fabric-Attached MetroCluster-Konfigurationen

Das Hardware Universe-Tool enthält einige Hinweise zu den Anforderungen, die Time Division Multiplexing (TDM) oder Wavelength Division Multiplexing (WDM)-Geräte erfüllen müssen, um mit einer Fabric-Attached MetroCluster-Konfiguration zu arbeiten. Diese Hinweise enthalten auch Informationen zu verschiedenen Konfigurationen, die Ihnen helfen, zu bestimmen, wann in-Order-Lieferung (IOD) von Rahmen oder außerhalb der Bestellung Lieferung (OOD) von Frames.

Ein Beispiel für solche Anforderungen ist, dass die TDM/WDM-Geräte die Funktion Link Aggregation (Trunking) mit Routing-Richtlinien unterstützen müssen. Die Reihenfolge der Lieferung (IOD oder OOD) von

Frames wird innerhalb eines Switch beibehalten und wird durch die in Kraft gehaltene Routing-Policy bestimmt.

"NetApp Hardware Universe"

Die folgende Tabelle enthält die Routing-Richtlinien für Konfigurationen, die Brocade Switches und Cisco Switches enthalten:

Schalter	Konfigurieren von MetroCluster-Konfigurationen für IOD	Konfiguration von MetroCluster-Konfigurationen für OOD
Brocade	• AptPolicy muss auf 1 gesetzt sein • DLS muss auf aus gesetzt werden • Die IOD muss auf ein gesetzt werden	• AptPolicy muss auf 3 festgelegt sein • DLS muss auf ein gesetzt werden • IOD muss auf aus gesetzt werden
Cisco	Richtlinien für das FCVI-designierte VSAN: • Load Balancing Policy: Srcid und dstid • Die IOD muss auf ein gesetzt werden Richtlinien für das vom Storage festgelegte VSAN: • Load Balancing Policy: Srcid, dstid und oxid • In VSAN darf die Option zur Auftragsgarantie nicht festgelegt werden	Keine Angabe

Wann IOD verwendet werden soll

Es ist am besten, IOD zu verwenden, wenn es von den Links unterstützt wird. Die folgenden Konfigurationen unterstützen IOD:

- Ein einzelnes ISL
- Die ISL und der Link (und die Link-Geräte, z. B. TDM/WDM, falls verwendet) unterstützen die Konfiguration für IOD.
- Ein einziger Trunk, die ISLs und die Links (und die Link-Geräte, wie TDM/WDM, falls verwendet) unterstützen die Konfiguration von IOD.

Wann OOD verwendet werden soll

- Sie können OOD für alle Konfigurationen verwenden, die keine IOD unterstützen.
- Sie können OOD für Konfigurationen verwenden, die die Trunking-Funktion nicht unterstützen.

Verwendung von Verschlüsselungsgeräten

Wenn Sie dedizierte Verschlüsselungsgeräte auf der ISL oder Verschlüsselung auf WDM-Geräten in der MetroCluster-Konfiguration verwenden, müssen Sie folgende Anforderungen erfüllen:

- Die externen Verschlüsselungsgeräte oder WDM-Geräte wurden vom Anbieter mit dem entsprechenden FC-Switch selbst zertifiziert.

  Die Selbstzertifizierung sollte den Betriebsmodus (wie Trunking und Verschlüsselung) abdecken.

- Die zusätzliche Latenz aufgrund der Verschlüsselung sollte nicht mehr als 10 Mikrosekunden enthalten.

Anforderungen für die Verwendung eines Brocade DCX 8510-8 Switches

Wenn Sie sich auf die MetroCluster Installation vorbereiten, sollten Sie sich mit der MetroCluster Hardwarearchitektur und den erforderlichen Komponenten vertraut machen.

- Die in MetroCluster-Konfigurationen verwendeten DCX 8510-8-Switches müssen von NetApp erworben werden.
- Für Skalierbarkeit sollte ein Port-Chunk zwischen MetroCluster Konfigurationen belassen werden, wenn nur zwei MetroCluster in 4x48-Port-Modulen verkabelt werden. Dadurch können Sie die Portnutzung in MetroCluster-Konfigurationen erweitern, ohne neu zu konfigurieren.
- Jeder Brocade DCX 8510-8-Switch in der MetroCluster -Konfiguration muss für die ISL-Ports und Speicherverbindungen korrekt konfiguriert sein. Informationen zur Portnutzung finden Sie im folgenden Abschnitt: "Portzuweisungen für FC-Switches" .
- ISLs können nicht gemeinsam genutzt werden und jede MetroCluster benötigt zwei ISLs für jedes Fabric.
- Der für Back-End-MetroCluster-Konnektivität verwendete DCX 8510-8-Switch sollte nicht für andere Verbindungen verwendet werden.

  Geräte, die nicht von MetroCluster sind, sollten nicht mit diesen Switches verbunden werden, und der Verkehr außerhalb von MetroCluster sollte nicht durch DCX 8510-8 Switches fließen.

- Eine Karte kann entweder an ONTAP MetroCluster * oder* ONTAP 7-Mode MetroCluster angeschlossen werden.

> RCF-Dateien sind für diesen Switch nicht verfügbar.

Die folgenden Anforderungen gelten für die Verwendung von zwei Brocade DCX 8510-8-Switches:

- An jedem Standort muss ein DCX 8510-8-Switch vorhanden sein.
- Sie müssen mindestens zwei Blades mit 48 Ports verwenden, die 16 GB SFPs an jedem Switch enthalten.

Die folgenden Anforderungen gelten für die Verwendung von vier DCX 8510-8-Switches an jedem Standort in einer MetroCluster-Konfiguration:

- An jedem Standort müssen zwei DCX 8510-8-Schalter vorhanden sein.
- Sie müssen mindestens ein Blade mit 48 Ports für jeden DCX 8510-8-Switch verwenden.
- Jedes Blade ist über virtuelle Fabrics als virtueller Switch konfiguriert.

Die folgenden NetApp Produkte werden von Brocade DCX 8510-8 Switches nicht unterstützt:

- Config Advisor
- Fabric Health Monitor
- MyAutoSupport (Systemrisiken können falsch positive Ergebnisse zeigen)
- Active IQ Unified Manager (ehemals OnCommand Unified Manager)

> Stellen Sie sicher, dass alle für diese Konfiguration erforderlichen Komponenten im enthalten sind "NetApp Interoperabilitäts-Matrix-Tool". In den Notizen im Interoperabilitäts-Matrix-Tool finden Sie Informationen zu unterstützten Konfigurationen.

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.

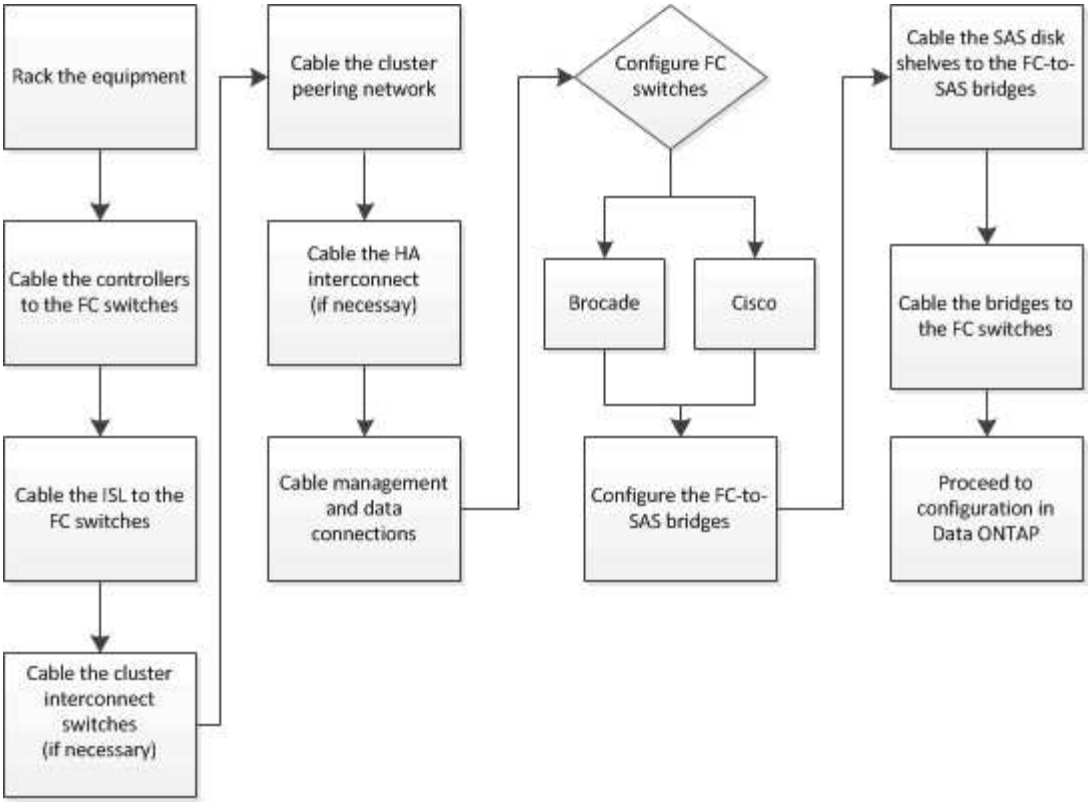
Die folgende Tabelle zeigt die Verwendung von TCP/UDP-Ports in einer externen Firewall, die zwischen zwei MetroCluster-Standorten positioniert ist.

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

Fabric-Attached MetroCluster-Konfiguration verkabeln

Verkabelung einer Fabric-Attached MetroCluster-Konfiguration

Die MetroCluster Komponenten müssen an beiden geografischen Standorten physisch installiert, verkabelt und konfiguriert sein.



Teile einer Fabric-MetroCluster-Konfiguration

Teile einer Fabric-MetroCluster-Konfiguration

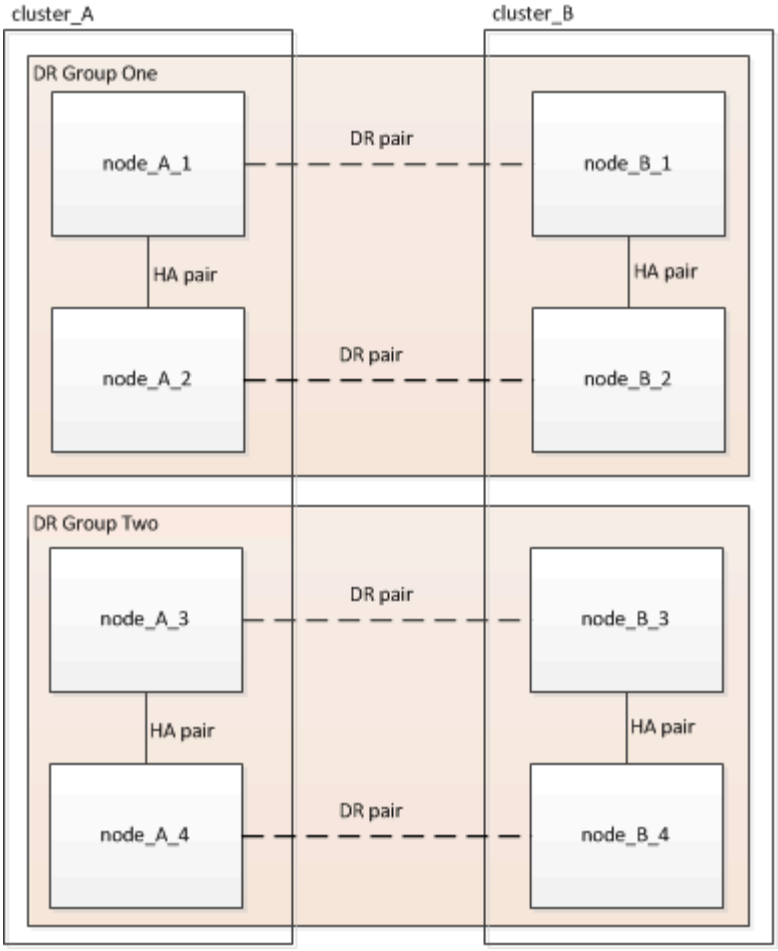
Wenn Sie Ihre MetroCluster Konfiguration planen, sollten Sie sich mit den Hardwarekomponenten und den zugehörigen Interconnects vertraut machen.

Disaster-Recovery-Gruppen (DR)

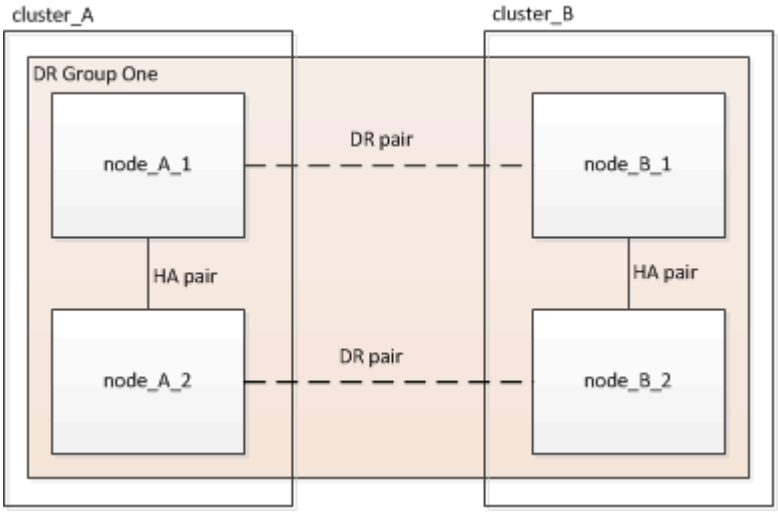
Eine Fabric MetroCluster Konfiguration besteht aus einer oder zwei DR-Gruppen, abhängig von der Anzahl der Nodes in der MetroCluster Konfiguration. Jede DR-Gruppe besteht aus vier Nodes.

- Eine MetroCluster Konfiguration mit acht Nodes besteht aus zwei DR-Gruppen.
- Eine MetroCluster Konfiguration mit vier Nodes besteht aus einer DR-Gruppe.

Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit acht Nodes:



Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit vier Nodes:



Wichtige Hardwarekomponenten

Eine MetroCluster Konfiguration umfasst die folgenden wichtigen Hardware-Elemente:

- Storage Controller

  Die Storage Controller sind nicht direkt mit dem Storage verbunden, sondern mit zwei redundanten FC Switch Fabrics verbunden.

- FC-to-SAS-Bridges

  Die FC-to-SAS-Bridges verbinden die SAS-Storage-Stacks mit den FC-Switches und geben somit die Möglichkeit, die beiden Protokolle zu überbrücken.

- FC Switches

  Die FC-Switches stellen das Langstrecken-Backbone ISL zwischen den beiden Standorten bereit. Die FC Switches stellen die beiden Storage Fabrics bereit, die die Datenspiegelung zu den Remote Storage Pools ermöglichen.

- Cluster-Peering-Netzwerk

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

Fabric MetroCluster Konfiguration mit acht Nodes

Eine Konfiguration mit acht Nodes besteht aus zwei Clustern, eines an jedem geografisch getrennten Standort. „Cluster_A“ befindet sich am ersten MetroCluster-Standort. „Cluster_B“ befindet sich am zweiten MetroCluster-Standort. Jeder Standort verfügt über ein SAS-Storage-Stack. Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt. Die HA-Paare sind als Cluster ohne Switch konfiguriert, ohne Cluster Interconnect Switches. Eine geschaltete Konfiguration wird unterstützt, wird aber nicht angezeigt.

Eine Konfiguration mit acht Nodes umfasst folgende Verbindungen:

- FC-Verbindungen von den HBAs jedes Controllers und FC-VI-Adaptern zu jedem der FC-Switches
- Eine FC-Verbindung von jeder FC-zu-SAS-Bridge zu einem FC-Switch
- SAS-Verbindungen zwischen jedem SAS Shelf und von oben und unten auf jedem Stack zu einer FC-to-SAS-Bridge
- Ein HA Interconnect zwischen jedem Controller im lokalen HA-Paar

  Wenn die Controller ein HA-Paar mit einem Gehäuse unterstützen, ist der HA Interconnect intern, was über die Backplane geschieht, sodass ein externer Interconnect nicht erforderlich ist.

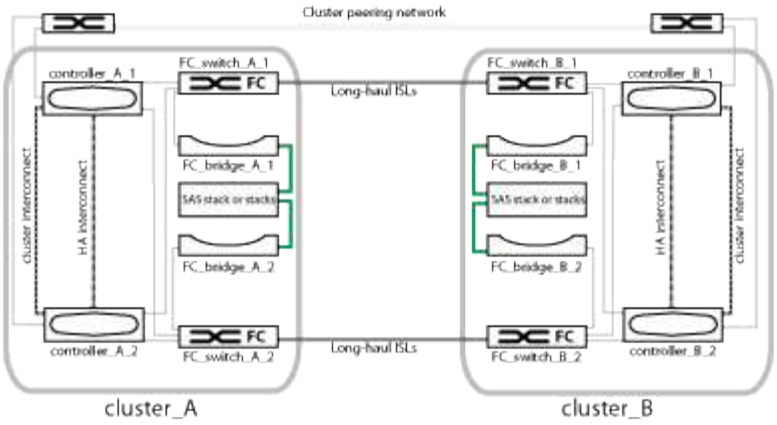
- Ethernet-Verbindungen von den Controllern zu dem vom Kunden bereitgestellten Netzwerk, das für Cluster-Peering verwendet wird

  Die SVM-Konfiguration wird über das Cluster-Peering-Netzwerk repliziert.

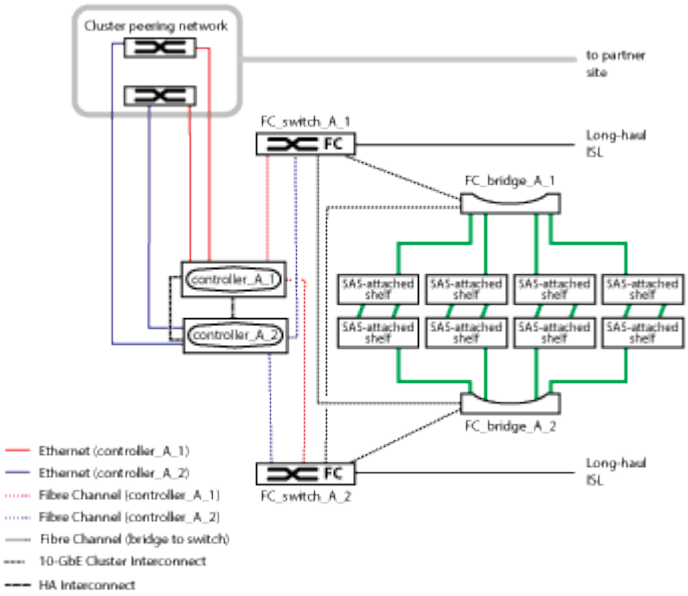
- Ein Cluster-Interconnect zwischen jedem Controller im lokalen Cluster

Fabric MetroCluster Konfiguration mit vier Nodes

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

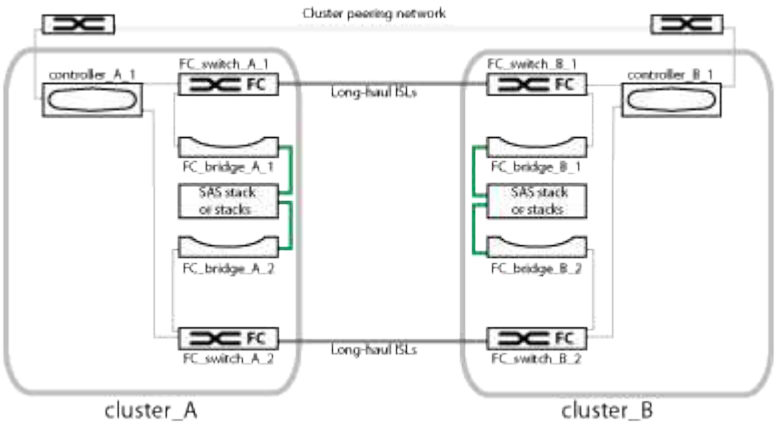


Die folgende Abbildung zeigt eine detailliertere Ansicht der Konnektivität in einem einzelnen MetroCluster Cluster (beide Cluster haben dieselbe Konfiguration):



Fabric MetroCluster Konfiguration mit zwei Nodes

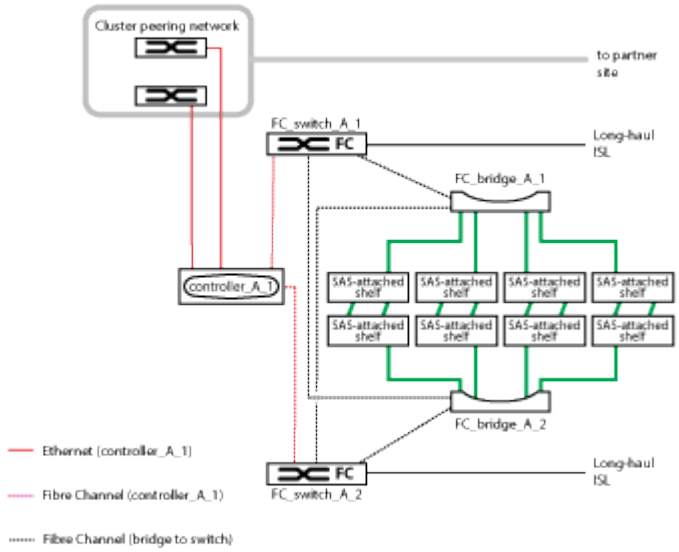
Die folgende Abbildung zeigt eine vereinfachte Ansicht einer Fabric MetroCluster Konfiguration mit zwei Nodes. Bei einigen Verbindungen stellt eine einzelne Leitung mehrere redundante Verbindungen zwischen den Komponenten dar. Verbindungen zu Daten und Management-Netzwerken werden nicht angezeigt.



Eine Konfiguration mit zwei Nodes besteht aus zwei Clustern, eines an jedem geografisch getrennten Standort. „Cluster_A“ befindet sich am ersten MetroCluster-Standort. „Cluster_B“ befindet sich am zweiten MetroCluster-Standort. Jeder Standort verfügt über ein SAS-Storage-Stack. Zusätzliche Storage-Stacks werden unterstützt, aber nur einer wird an jedem Standort angezeigt.

> In einer Konfiguration mit zwei Nodes sind die Nodes nicht als HA-Paar konfiguriert.

Die folgende Abbildung zeigt eine detailliertere Ansicht der Konnektivität in einem einzelnen MetroCluster Cluster (beide Cluster haben dieselbe Konfiguration):



Eine Konfiguration mit zwei Nodes umfasst folgende Verbindungen:

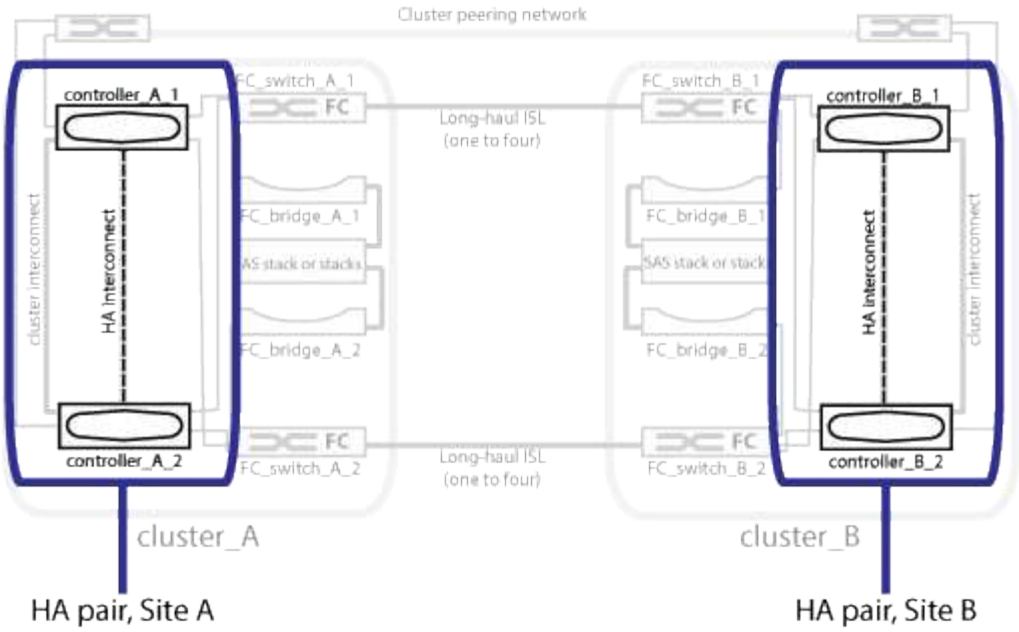
- FC-Verbindungen zwischen dem FC-VI-Adapter auf jedem Controller-Modul
- FC-Verbindungen von den HBAs jedes Controller-Moduls mit der FC-to-SAS Bridge für jeden SAS-Shelf-Stack
- SAS-Verbindungen zwischen jedem SAS Shelf und von oben und unten auf jedem Stack zu einer FC-to-SAS-Bridge
- Ethernet-Verbindungen von den Controllern zu dem vom Kunden bereitgestellten Netzwerk, das für Cluster-Peering verwendet wird

  Die SVM-Konfiguration wird über das Cluster-Peering-Netzwerk repliziert.

Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration

In MetroCluster Konfigurationen mit acht oder vier Nodes besteht jeder Standort aus Storage-Controllern, die als ein oder zwei HA-Paare konfiguriert sind. Dadurch wird lokale Redundanz ermöglicht, sodass der lokale HA-Partner übernimmt, wenn ein Storage Controller ausfällt. Solche Ausfälle können ohne MetroCluster-Switchover-Operation behoben werden.

Lokale HA-Failover- und Giveback-Vorgänge werden mit Storage Failover-Befehlen auf gleiche Weise durchgeführt wie eine andere Konfiguration von MetroCluster.



Verwandte Informationen

"Darstellung redundanter FC-to-SAS-Bridges"

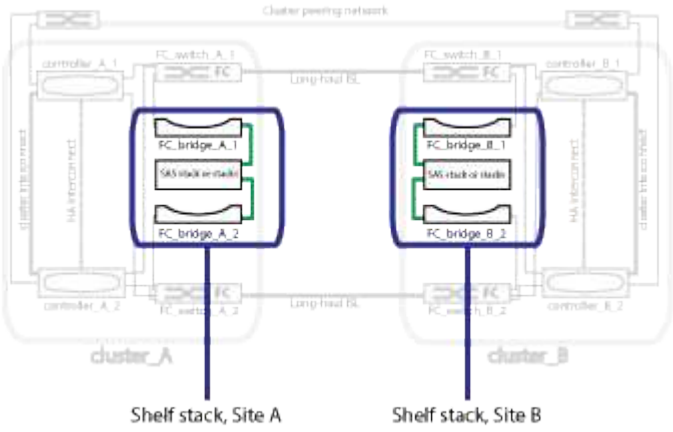
"Redundante FC Switch Fabrics"

"Illustration des Cluster-Peering-Netzwerks"

"ONTAP-Konzepte"

Darstellung redundanter FC-to-SAS-Bridges

FC-to-SAS-Bridges bieten Protokollüberbrückung zwischen SAS-verbundenen Festplatten und der FC Switch Fabric.



Verwandte Informationen

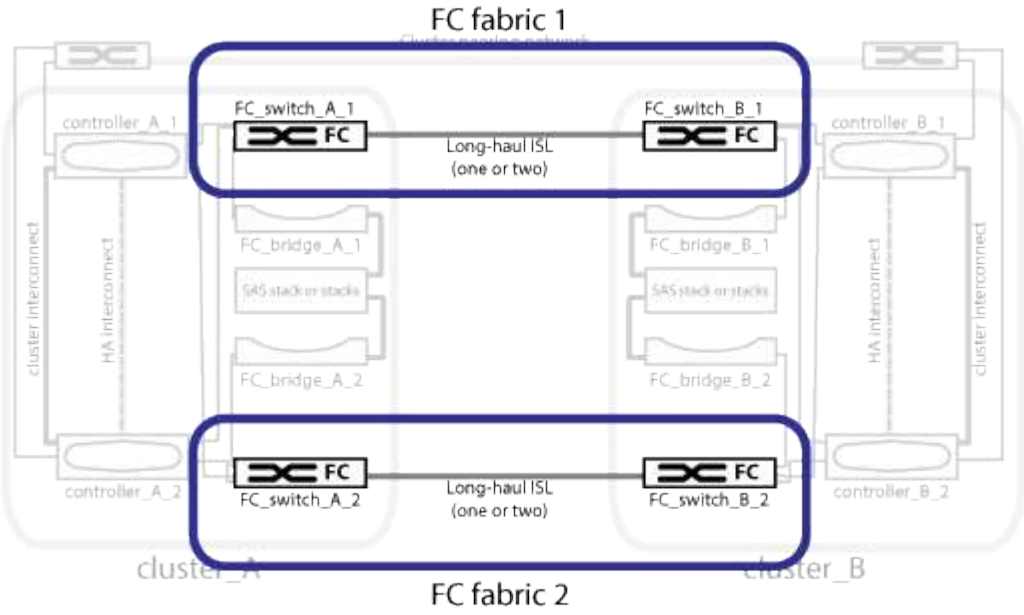
"Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration"

"Redundante FC Switch Fabrics"

"Illustration des Cluster-Peering-Netzwerks"

Redundante FC Switch Fabrics

Jede Switch Fabric umfasst Inter-Switch-Links (ISLs), die die Standorte verbinden. Die Daten werden von Standort zu Standort über ISL repliziert. Um die Redundanz zu gewährleisten, muss sich jede Switch Fabric auf unterschiedlichen physischen Pfaden befinden.



Verwandte Informationen

"Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration"

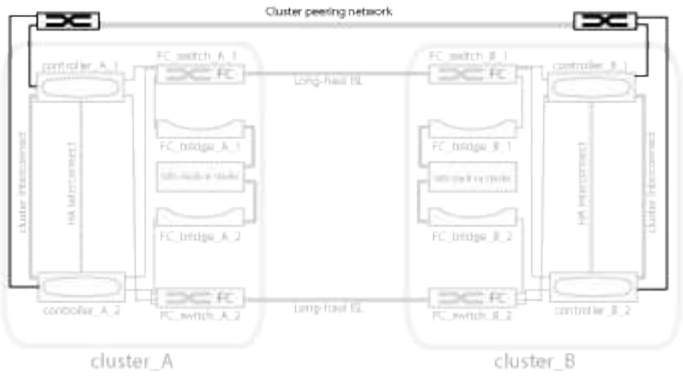
"Darstellung redundanter FC-to-SAS-Bridges"

"Illustration des Cluster-Peering-Netzwerks"

Illustration des Cluster-Peering-Netzwerks

Die beiden Cluster in der MetroCluster Konfiguration werden über ein vom Kunden bereitgestellter Cluster-Peering-Netzwerk Peering Peering durchgeführt. Cluster Peering unterstützt die synchrone Spiegelung von Storage Virtual Machines (SVMs, früher Vserver genannt) zwischen den Standorten.

Intercluster-LIFs müssen auf jedem Node in der MetroCluster-Konfiguration konfiguriert werden, und die Cluster müssen für Peering konfiguriert sein. Die Ports mit den Intercluster-LIFs sind mit dem vom Kunden bereitgestellten Cluster-Peering-Netzwerk verbunden. Die Replizierung der SVM-Konfiguration erfolgt über dieses Netzwerk über den Configuration Replication Service.



Verwandte Informationen

"Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration"

"Darstellung redundanter FC-to-SAS-Bridges"

"Redundante FC Switch Fabrics"

"Express-Konfiguration für Cluster und SVM-Peering"

"Überlegungen für die Konfiguration von Cluster-Peering"

"Verkabeln der Cluster-Peering-Verbindungen"

"Peering der Cluster"

Erforderliche MetroCluster FC-Komponenten und Namenskonventionen

Wenn Sie Ihre MetroCluster FC-Konfiguration planen, müssen Sie die erforderlichen und unterstützten Hardware- und Softwarekomponenten 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.

> Langwierige SFPs werden von den MetroCluster Storage-Switches nicht unterstützt. Eine Tabelle der unterstützten SPFs finden Sie im technischen Bericht von MetroCluster.

Hardwareredundanz in der MetroCluster FC Konfiguration

Aufgrund der Hardware-Redundanz in der MetroCluster FC-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.

Notwendigkeit für zwei ONTAP Cluster

Die Fabric-Attached MetroCluster FC-Konfiguration erfordert zwei ONTAP Cluster, einen an jedem MetroCluster Standort.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
- Standort B: Cluster_B

Anforderung für vier FC Switches

Für die Fabric-Attached MetroCluster FC-Konfiguration sind vier FC-Switches erforderlich (unterstützte Brocade oder Cisco Modelle).

Die vier Switches bilden zwei Switch-Storage-Fabrics, die in der MetroCluster-FC-Konfiguration zwischen jedem der Cluster die ISL bereitstellen.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Anforderungen für zwei, vier oder acht Controller-Module

Die Fabric-Attached MetroCluster FC Konfiguration erfordert zwei, vier oder acht Controller-Module.

In einer MetroCluster Konfiguration mit vier oder acht Nodes bilden die Controller-Module an jedem Standort ein oder zwei HA-Paare. Jedes Controller-Modul besitzt einen DR-Partner am anderen Standort.

Die Controller-Module 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.

  Bei Konfigurationen mit zwei DR-Gruppen kann jede DR-Gruppe jedoch aus verschiedenen Controller-Modulmodellen bestehen.

- 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 wird nicht unterstützt, Wobei ein Mix aus einem Controller-Modul mit integrierten FC-VI-Ports und einer weiteren Karte mit zusätzlicher FC-VI-Karte verwendet wird. 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

Anforderung für vier Cluster Interconnect Switches

Für die Fabric-Attached MetroCluster FC-Konfiguration sind vier Cluster Interconnect Switches erforderlich (wenn Sie keine 2-Node-Cluster ohne Switch verwenden).

Diese Switches sorgen für eine Cluster-Kommunikation zwischen den Controller-Modulen in jedem Cluster. Die Switches sind nicht erforderlich, wenn die Controller-Module an jedem Standort als 2-Node-Cluster ohne Switches konfiguriert sind.

Notwendigkeit für FC-to-SAS-Bridges

Bei der Fabric-Attached MetroCluster FC-Konfiguration sind für jede SAS-Stapelgruppe ein Paar FC-to-SAS-Bridges erforderlich.

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

- FibreBridge 7600N oder 7500N-Brücken unterstützen bis zu vier SAS-Stacks.
- Jeder Stack kann verschiedene IOM-Modelle verwenden.

  Eine Kombination aus IOM12-Modulen und IOM3-Modulen wird im selben Storage-Stack nicht unterstützt. Wenn auf dem System eine unterstützte Version von ONTAP ausgeführt wird, wird im selben Storage Stack eine Kombination aus IOM12-Modulen und IOM6-Modulen unterstützt.

  Unterstützte IOM-Module hängen von der Version der ONTAP ab, die Sie ausführen.

- Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Die als Beispiele in dieser Dokumentation vorgeschlagenen Namen identifizieren das Controller-Modul und den Stack, mit dem die Bridge verbunden ist, wie unten gezeigt.

Pool- und Festplattenanforderungen (mindestens unterstützt)

Es werden acht SAS-Platten-Shelves empfohlen (vier Shelfs an jedem Standort), damit sich die Anschaffung von Festplatten pro Shelf zulässt.

Die MetroCluster-Konfiguration erfordert die Minimalkonfiguration an jedem Standort:

- Jeder Node hat mindestens einen lokalen Pool und einen Remote-Pool am Standort.

  Bei einer MetroCluster-Konfiguration mit vier Nodes und zwei Nodes an jedem Standort sind beispielsweise an jedem Standort vier Pools erforderlich.

- Mindestens sieben Laufwerke pro Pool.

  In einer MetroCluster-Konfiguration mit vier Nodes und einem einzelnen gespiegelten Datenaggregat pro Node sind für die Minimalkonfiguration 24 Festplatten am Standort erforderlich.

In einer minimal unterstützten Konfiguration verfügt jeder Pool über das folgende Laufwerkslayout:

- Drei Root-Laufwerke
- Drei Datenlaufwerke
- Ein Ersatzlaufwerk

Bei einer unterstützten Minimalkonfiguration ist pro Standort mindestens ein Shelf erforderlich.

MetroCluster-Konfigurationen unterstützen RAID-DP und RAID4.

Überlegungen zum Speicherort von Laufwerken für teilweise bestückte Shelfs

Die Laufwerke sollten sich in den Steckplätzen 0-5 und 18-23 befinden, um Laufwerke bei Verwendung von Shelfs, die halb bestückt sind (12 Laufwerke in einem Shelf mit 24 Laufwerken), automatisch zuweisen.

Bei einer Konfiguration mit einem teilweise bestückten Shelf müssen die Laufwerke gleichmäßig in die vier Quadranten des Shelfs verteilt werden.

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. "IMT"

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

Namenskonventionen für Bridge

Die Brücken verwenden das folgende Beispiel:

```
bridge_site_stack grouplocation in pair
```

Dieser Teil des Namens…	Identifiziert…	Mögliche Werte…
Standort	Standort, auf dem sich das Brückenpaar physisch befindet.	A oder B
Stapelgruppe	Nummer der Stapelgruppe, mit der das Brückenpaar verbunden ist. FibreBridge 7600N oder 7500N-Brücken unterstützen bis zu vier Stapel in der Stapelgruppe. Die Stack-Gruppe kann maximal 10 Storage Shelves enthalten.	1, 2, usw.
Position in Paar	Brücke innerhalb des Brückenpaares.Ein Paar Brücken verbinden sich mit einer bestimmten Stapelgruppe.	A oder b

Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

- Bridge_A_1a
- Bridge_A_1b
- Bridge_B_1a

- Bridge_B_1b

Konfigurationsarbeitsblätter für FC Switches und FC-to-SAS-Bridges

Bevor Sie mit der Konfiguration der MetroCluster-Standorte beginnen, können Sie die folgenden Worksheets verwenden, um Ihre Standortinformationen aufzuzeichnen:

"Arbeitsblatt für Standort A"

"Arbeitsblatt für Standort B"

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.

Über diese Aufgabe

Dieser Task muss auf beiden MetroCluster-Sites ausgeführt werden.

Schritte

1. Planen der Positionierung der MetroCluster Komponenten

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

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Installieren Sie die FC-Switches im Rack oder Schrank.
5. 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.
6. 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.

      Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihr Bridge-Modell enthält weitere Informationen und eine Abbildung der Installation.

> Für einen ausreichenden Zugriff auf Port-Speicherplatz und FRU-Wartungsfreundlichkeit müssen Sie 1U-Platz unter dem Brückenpaar lassen und diesen Platz mit einem werkzeuglosen Blindpanel abdecken.

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.

Verkabelung der FC-VI- und HBA-Ports des neuen Controller-Moduls an die FC-Switches

Die FC-VI-Ports und HBAs (Host Bus Adapter) müssen mit den FC-Switches am Standort an jedem Controller-Modul in der MetroCluster-Konfiguration verbunden sein.

Schritte

1. Verkabeln Sie die FC-VI-Ports und HBA-Ports mit der Tabelle für Ihre Konfiguration und Ihr Switch-Modell.
   - "Portzuweisungen für FC-Switches"

Verkabelung der ISLs zwischen MetroCluster Standorten

Sie müssen die FC-Switches an jedem Standort über die ISLs (Fiber-Optic Inter-Switch Links) verbinden, um die Switch Fabrics zu bilden, die die MetroCluster Komponenten verbinden.

Über diese Aufgabe

Dies muss für beide Switch Fabrics geschehen.

Schritte

1. Verbinden Sie die FC Switches an jedem Standort mit allen ISLs. Verwenden Sie dabei die Verkabelung in der Tabelle, die Ihrer Konfiguration und dem Switch-Modell entspricht.
   - "Portzuweisungen für FC-Switches"

Verwandte Informationen

"Überlegungen für ISLs"

Portzuweisungen für FC-Switches

Portzuweisungen für MetroCluster FC-Switches

Sie müssen beim Verkabeln der FC-Switches sicherstellen, dass Sie die angegebenen Portzuweisungen verwenden.

Sie können Ports, die nicht zum Anschließen von Initiator-Ports, FC-VI-Ports oder ISLs verwendet werden, als Speicher-Ports neu konfigurieren. Wenn Sie jedoch die unterstützten RCFs verwenden, müssen Sie die Zoneneinteilung entsprechend ändern.

Wenn Sie die unterstützten RCFs verwenden, stellen ISL-Ports möglicherweise keine Verbindung zu denselben angezeigten Ports her und müssen möglicherweise manuell neu konfiguriert werden.

Wenn Sie Ihre Switches mit den Portzuweisungen für ONTAP 9 konfiguriert haben, können Sie die älteren Zuweisungen weiterhin verwenden. Neue Konfigurationen mit ONTAP 9.1 oder höher sollten jedoch die hier gezeigten Portzuweisungen verwenden.

Allgemeine Verkabelungsrichtlinien

Beachten Sie bei der Verwendung der Verkabelungstabellen die folgenden Richtlinien:

- Brocade- und Cisco-Switches verwenden unterschiedliche Port-Nummerierung:
  - Bei Brocade Switches wird der erste Port mit der Nummer 0 nummeriert.
  - Bei Cisco Switches wird der erste Port mit der Nummer 1 nummeriert.
- Für jeden FC-Switch im Switch Fabric ist die Verkabelung identisch.
- Sie können AFF A300 und FAS8200 Storage-Systeme über eine der zwei Optionen für FC-VI-Konnektivität bestellen:
  - 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.
- Für die AFF A700 und FAS9000 Storage-Systeme sind vier FC-VI-Ports erforderlich. Die folgenden Tabellen zeigen die Verkabelung für die FC Switches mit vier FC-VI-Ports an jedem Controller, außer für den Cisco 9250i Switch.

  Verwenden Sie für andere Storage-Systeme die in den Tabellen gezeigten Kabel, ignorieren Sie jedoch die Verkabelung für FC-VI-Ports c und d.

  Sie können diese Ports leer lassen.
- Die Storage-Systeme der AFF A400 und FAS8300 verwenden die Ports 2a und 2b für FC-VI-Konnektivität.
- Wenn zwei MetroCluster-Konfigurationen ISLs gemeinsam nutzen, verwenden Sie für eine MetroCluster-Verkabelung mit acht Nodes die gleichen Port-Zuweisungen wie diese.
- Die Anzahl der von Ihnen verkabelten ISLs kann je nach den Anforderungen des Standorts variieren.
- Weitere Informationen zu den Überlegungen zu ISL finden Sie im Abschnitt.

  "Überlegungen für ISLs"

AFF A900 und FAS9500 Verkabelungsrichtlinien

- Für AFF A900 oder FAS9500 Storage-Systeme sind acht FC-VI-Ports erforderlich. Wenn Sie ein AFF A900 oder FAS9500 verwenden, müssen Sie die Konfiguration mit acht Ports verwenden. Wenn die Konfiguration die anderen Modelle des Storage-Systems umfasst, verwenden Sie die in den Tabellen dargestellte Verkabelung, ignorieren Sie jedoch die Verkabelung für nicht benötigte FC-VI-Ports.

Port-Zuweisungen für Systeme mit zwei Initiator-Ports

Sie können FAS8200 und AFF A300 -Systeme mit einem einzelnen Initiator-Port für jede Fabric und zwei Initiator-Ports für jeden Controller konfigurieren.

Sie können die Verkabelung für die FibreBridge 7600N-Bridge mit nur einem FC-Port (FC1 oder FC2)

durchführen. Schließen Sie statt vier Initiatoren nur zwei an und lassen Sie die beiden anderen, die mit dem Switch-Port verbunden sind, leer.

Bei manueller Zoneneinteilung folgen Sie der Zoneneinteilung für eine FibreBridge 7600N-Bridge mit einem FC-Port (FC1 oder FC2). In diesem Szenario wird jedem Zonenmitglied pro Fabric ein Initiator-Port (statt zwei) hinzugefügt.

Sie können das Zoning ändern oder ein Upgrade von einer FibreBridge 6500N auf eine FibreBridge 7500N durchführen. Gehen Sie dazu wie unter beschrieben vor "Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke".

Die folgende Tabelle zeigt die Portzuweisungen für Brocade FC-Switches bei Verwendung eines einzelnen Initiator-Ports für jedes Fabric und zweier Initiator-Ports für jeden Controller.

Konfigurationen mit FibreBridge 7500N oder 7600N mit nur einem FC-Port (FC1 oder FC2)			
MetroCluster 1 oder DR Gruppe 1	• Komponente*	**Port**	**6505, 6510, 6520, 7840, G620, G630, G610, G710, G720, G730 und DCX 8510-8**
Anschluss an FC-Switch…	**Verbindet den Switch-Port…**	Controller_x_1	FC-VI-Port A
1	0	FC-VI-Port b	2
0	FC-VI-Port c	1	1
FC-VI-Port d	2	1	HBA-Port A
1	2	HBA-Port b	2
2	HBA-Port c	-	-
HBA-Port d	-	-	Stack 1
Bridge_x_1a	1	8	Bridge_x_1b
2	8	Stapel Y	Bridge_x_ya
1	11	Bridge_x_yb	2

Brocade -Port-Nutzung für Controller in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die erforderlichen Portzuweisungen zum Verkabeln von Brocade FC-Switches mit Ihren Controllern.

Die folgenden Tabellen zeigen die maximal unterstützte Konfiguration mit vier Controllermodulen pro DR-Gruppe. Bei kleineren Konfigurationen ignorieren Sie die Zeilen für die zusätzlichen Controllermodule. Beachten Sie, dass acht ISLs nur auf den Switches Brocade 6510, Brocade DCX 8510-8, G620, G630, G620-

1, G630-1, G720 und G730 unterstützt werden.

Lesen Sie die folgenden Informationen, bevor Sie diese Tabellen verwenden:

- Die Portnutzung der Brocade 6505-, G610- und G710-Switches in einer MetroCluster Konfiguration mit acht Knoten wird nicht angezeigt. Aufgrund der begrenzten Anzahl an Ports müssen die Portzuweisungen je nach Controllermodulmodell und Anzahl der verwendeten ISLs und Bridge-Paare standortbezogen erfolgen.
- Der Brocade DCX 8510-8 Switch kann dasselbe Portlayout verwenden wie der 6510 Switch ***or*** des 7840 Switch.
- Brocade 6520-, 7810- und 7840-Switches werden auf Systemen, die acht FC-VI-Ports verwenden (AFF A900 und FAS9500 -Systeme), nicht unterstützt.
- Brocade 7810-Switches unterstützen nur eine DR-Gruppe.

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 1 oder DR-Gruppe 1 auf Brocade -Switches.

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Controller_x_1	FC-VI-Port A	1	0	0	0	0	0	0	0
FC-VI-Port b	2	0	0	0	0	0	0	0	FC-VI-Port c
1	1	1	1	1	1	1	1	FC-VI-Port d	2
1	1	1	1	1	1	1	FC-VI-2-Port A	1	16
20	n/a	n/a	n/a	16	2	FC-VI-2-Port b	2	16	20
n/a	n/a	n/a	16	2	FC-VI-2-Port c	1	17	21	n/a
n/a	n/a	17	3	FC-VI-2-Port d	2	17	21	n/a	n/a
n/a	17	3	HBA-Port A	1	2	2	2	2	2

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
2	8	HBA-Port b	2	2	2	2	2	2	2
8	HBA-Port c	1	3	3	3	3	3	3	9
HBA-Port d	2	3	3	3	3	3	3	9	Controller_x_2
FC-VI-Port A	1	4	4	4	4	4	4	4	FC-VI-Port b
2	4	4	4	4	4	4	4	FC-VI-Port c	1
5	5	5	5	5	5	5	FC-VI-Port d	2	5
5	5	5	5	5	5	FC-VI-2-Port A	1	18	22
n/a	n/a	n/a	20	6	FC-VI-2-Port b	2	18	22	n/a
n/a	n/a	20	6	FC-VI-2-Port c	1	19	23	n/a	n/a
n/a	21	7	FC-VI-2-Port d	2	19	23	n/a	n/a	n/a
21	7	HBA-Port A	1	6	6	6	6	6	6
12	HBA-Port b	2	6	6	6	6	6	6	12
HBA-Port c	1	7	7	7	7	7	7	13	HBA-Port d

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 2 oder DR-Gruppe 2 auf Brocade -Switches.

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Controller_x_3	FC-VI-Port A	1	n/a	24	48	n/a	12	18	18
FC-VI-Port b	2	n/a	24	48	n/a	12	18	18	FC-VI-Port c
1	n/a	25	49	n/a	13	19	19	FC-VI-Port d	2
n/a	25	49	n/a	13	19	19	FC-VI-2-Port A	1	n/a
36	n/a	n/a	n/a	36	24	FC-VI-2-Port b	2	n/a	36
n/a	n/a	n/a	36	24	FC-VI-2-Port c	1	n/a	37	n/a
n/a	n/a	37	25	FC-VI-2-Port d	2	n/a	37	n/a	n/a
n/a	37	25	HBA-Port A	1	n/a	26	50	n/a	14
24	26	HBA-Port b	2	n/a	26	50	n/a	14	24
26	HBA-Port c	1	n/a	27	51	n/a	15	25	27
HBA-Port d	2	n/a	27	51	n/a	15	25	27	Controller_x_4
FC-VI-Port A	1	n/a	28	52	n/a	16	22	22	FC-VI-Port b

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
2	n/a	28	52	n/a	16	22	22	FC-VI-Port c	1
n/a	29	53	n/a	17	23	23	FC-VI-Port d	2	n/a
29	53	n/a	17	23	23	FC-VI-2-Port A	1	n/a	38
n/a	n/a	n/a	38	28	FC-VI-2-Port b	2	n/a	38	n/a
n/a	n/a	38	28	FC-VI-2-Port c	1	n/a	39	n/a	n/a
n/a	39	29	FC-VI-2-Port d	2	n/a	39	n/a	n/a	n/a
39	29	HBA-Port A	1	n/a	30	54	n/a	18	28
30	HBA-Port b	2	n/a	30	54	n/a	18	28	30
HBA-Port c	1	n/a	31	55	n/a	19	29	31	HBA-Port d

MetroCluster 3 oder DR-Gruppe 3

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 3 oder DR-Gruppe 3 auf Brocade -Switches.

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Controller_x_5	FC-VI-Port A	1	48	48
FC-VI-Port b	2	48	48	FC-VI-Port c
1	49	49	FC-VI-Port d	2

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
49	49	FC-VI-2-Port A	1	64
50	FC-VI-2-Port b	2	64	50
FC-VI-2-Port c	1	65	51	FC-VI-2-Port d
2	65	51	HBA-Port A	1
50	56	HBA-Port b	2	50
56	HBA-Port c	1	51	57
HBA-Port d	2	51	57	Controller_x_6
FC-VI-Port A	1	52	52	FC-VI-Port b
2	52	52	FC-VI-Port c	1
53	53	FC-VI-Port d	2	53
53	FC-VI-2-Port A	1	68	54
FC-VI-2-Port b	2	68	54	FC-VI-2-Port c
1	69	55	FC-VI-2-Port d	2
69	55	HBA-Port A	1	54
60	HBA-Port b	2	54	60
HBA-Port c	1	55	61	HBA-Port d

MetroCluster 4 oder DR-Gruppe 4

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 4 oder DR-Gruppe 4 auf Brocade -Switches.

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Controller_x_7	FC-VI-Port A	1	66	66
FC-VI-Port b	2	66	66	FC-VI-Port c

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
1	67	67	FC-VI-Port d	2
67	67	FC-VI-2-Port A	1	84
72	FC-VI-2-Port b	2	84	72
FC-VI-2-Port c	1	85	73	FC-VI-2-Port d
2	85	73	HBA-Port A	1
72	74	HBA-Port b	2	72
74	HBA-Port c	1	73	75
HBA-Port d	2	73	75	Controller_x_8
FC-VI-Port A	1	70	70	FC-VI-Port b
2	70	70	FC-VI-Port c	1
71	71	FC-VI-Port d	2	71
71	FC-VI-2-Port A	1	86	76
FC-VI-2-Port b	2	86	76	FC-VI-2-Port c
1	87	77	FC-VI-2-Port d	2
87	77	HBA-Port A	1	76
78	HBA-Port b	2	76	78
HBA-Port c	1	77	79	HBA-Port d

Brocade -Port-Nutzung für FC-zu-SAS-Brücken in einer MetroCluster FC-Konfiguration

Erfahren Sie mehr über die erforderlichen Portzuweisungen für die Verkabelung von Brocade FC-Switches mit FC-zu-SAS-Brücken. Die Portzuweisungen variieren je nachdem, ob die Brücken einen oder zwei FC-Ports verwenden.

Brocade 7810-Switches unterstützen nur eine DR-Gruppe.

Shelf-Konfigurationen mit FibreBridge 7500N- oder 7600N-Brücken unter Verwendung beider FC-Ports (FC1 und FC2)

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 1 oder DR-Gruppe 1 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Brocade Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei den Switches Brocade 6505, G610, G710, G620, G620-1, G630 und G630-1 können Sie zusätzliche Bridges an die Ports 12–15 anschließen.
- Bei Brocade 6510- und DCX 8510-8-Switches können Sie zusätzliche Bridges an die Ports 12–19 anschließen.
- Bei Brocade 6520-Switches können Sie zusätzliche Bridges an die Ports 12–21 und 24–45 anschließen.
- Auf Brocade 7810- und 7840-Switches unterstützt MetroCluster 1 oder DR-Gruppe 1 nur zwei Bridge-Stacks.
- Bei Brocade G720- und G730-Switches können Sie zusätzliche Bridges an die Ports 16–21 anschließen.

* Komponente*		Port	Anschluss an FC-Switch …	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Stack 1	Bridge_x_1a	FC1	1	8	8	8	8	8	8	10
FC2	2	8	8	8	8	8	8	10	Bridge_x_1b	FC1
1	9	9	9	9	9	9	11	FC2	2	9
9	9	9	9	9	11	Stack 2	Bridge_x_2a	FC1	1	10
10	10	10	10	10	14	FC2	2	10	10	10
10	10	10	14	Bridge_x_2b	FC1	1	11	11	11	11
11	11	15	FC2	2	11	11	11	11	11	11

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 2 oder DR-Gruppe 2 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Brocade Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Auf den Switches Brocade 6510, DCX 8510-8 und 7840 unterstützt MetroCluster 2 oder DR-Gruppe 2 nur zwei Bridge-Stacks.
- Bei Brocade 6520-Switches können Sie zusätzliche Bridges an die Ports 60–69 und 72–93 anschließen.
- Bei den Switches Brocade G620, G620-1, G630 und G630-1 können Sie zusätzliche Bridges an die Ports 32–35 anschließen.
- Bei Brocade G720- und G730-Switches können Sie zusätzliche Bridges an die Ports 36–39 anschließen.
- Die Portnutzung für die Brocade 6505-, G610- und G710-Switches in einer MetroCluster Konfiguration mit acht Knoten wird nicht angezeigt. Aufgrund der begrenzten Anzahl von Ports weisen Sie die Ports je nach Controllermodell und Anzahl der verwendeten ISLs und Bridge-Paare Site für Site zu.

* Komponente*		Port	Anschluss an FC-Switch …	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Stack 1	Bridge_x_1a	FC1	1	n/a	32	56	n/a	20	26	32
FC2	2	n/a	32	56	n/a	20	26	32	Bridge_x_1b	FC1
1	n/a	33	57	n/a	21	27	33	FC2	2	n/a
33	57	n/a	21	27	33	Stack 2	Bridge_x_2a	FC1	1	n/a
34	58	n/a	22	30	34	FC2	2	n/a	34	58
n/a	22	30	34	Bridge_x_2b	FC1	1	n/a	35	59	n/a
23	31	35	FC2	2	n/a	35	59	n/a	23	31

MetroCluster 3 oder DR-Gruppe 3

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 3 oder DR-Gruppe 3 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Brocade Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei Brocade G630- und G630-1-Switches können Sie zusätzliche Bridges an die Ports 60–63 anschließen.
- Bei Brocade G730-Switches können Sie zusätzliche Bridges an die Ports 64, 65, 68 und 69 anschließen.

* Komponente*		Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Stack 1	Bridge_x_1a	FC1	1	56	58

* Komponente*		Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
FC2	2	56	58	Bridge_x_1b	FC1
1	57	59	FC2	2	57
59	Stack 2	Bridge_x_2a	FC1	1	58
62	FC2	2	58	62	Bridge_x_2b
FC1	1	59	63	FC2	2

MetroCluster 4 oder DR-Gruppe 4

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 4 oder DR-Gruppe 4 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Brocade Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei Brocade G630- und G630-1-Switches können Sie zusätzliche Bridges an die Ports 80–83 anschließen.
- Auf Brocade G730-Switches können Sie zusätzliche Bridges an die Ports 84–95 anschließen.

* Komponente*		Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Stack 1	Bridge_x_1a	FC1	1	74	80
FC2	2	74	80	Bridge_x_1b	FC1
1	75	81	FC2	2	75
81	Stack 2	Bridge_x_2a	FC1	1	78
82	FC2	2	78	82	Bridge_x_2b
FC1	1	79	83	FC2	2

Shelf-Konfigurationen mit FibreBridge 7500N oder 7600N und nur einem FC-Port (FC1 oder FC2)

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 1 oder DR-Gruppe 1 mit FibreBridge 7500N oder 7600N und nur einem FC-Port (FC1 oder FC2) auf Brocade Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Auf den Switches Brocade 6505, G610, G710, G620, G620-1, G630 und G630-1 werden die Ports 12–15 zusätzlich überbrückt.
- Bei Brocade 6510- und DCX 8510-8-Switches können Sie zusätzliche Bridges an die Ports 12–19

anschließen.

- Bei Brocade 6520-Switches können Sie zusätzliche Bridges an die Ports 16–21 und 24–45 anschließen.
- Bei Brocade G720- und G730-Switches können Sie zusätzliche Bridges an die Ports 16–21 anschließen.

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Stack 1	Bridge_x_1a	1	8	8	8	8	8	8	10
Bridge_x_1b	2	8	8	8	8	8	8	10	Stack 2
Bridge_x_2a	1	9	9	9	9	9	9	11	Bridge_x_2b
2	9	9	9	9	9	9	11	Stapel 3	Bridge_x_3a
1	10	10	10	10	10	10	14	Bridge_x_3b	2
10	10	10	10	10	10	14	Stapel 4	Bridge_x_4a	1
11	11	11	11	11	11	15	Bridge_x_4b	2	11

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 2 oder DR-Gruppe 2 für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port (FC1 oder FC2) auf Brocade -Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei Brocade 6520-Switches können Sie zusätzliche Bridges an die Ports 60–69 und 72–93 anschließen.
- Bei den Switches Brocade G620, G620-1, G630 und G630-1 können Sie zusätzliche Bridges an die Ports 32–35 anschließen.
- Bei Brocade G720- und G730-Switches können Sie zusätzliche Bridges an die Ports 36–39 anschließen.
- Die Portnutzung für die Brocade 6505-, G610- und G710-Switches in einer MetroCluster Konfiguration mit acht Knoten wird nicht angezeigt. Aufgrund der begrenzten Anzahl von Ports weisen Sie die Ports je nach Controllermodell und Anzahl der verwendeten ISLs und Bridge-Paare Site für Site zu.

* Komponente*	Port	Anschluss an FC-Switch…	6505-, G610-, G710-Anschluss	6510, DCX 8510-8-Anschluss	6520-Anschluss	7810-Anschluss	7840-Anschluss	G620-, G620-1-, G630-, G630-1-Anschluss	G720, G730-Anschluss
Stack 1	Bridge_x_1a	1	n/a	32	56	n/a	20	26	32
Bridge_x_1b	2	n/a	32	56	n/a	20	26	32	Stack 2
Bridge_x_2a	1	n/a	33	57	n/a	21	27	33	Bridge_x_2b
2	n/a	33	57	n/a	21	27	33	Stapel 3	Bridge_x_3a
1	n/a	34	58	n/a	22	30	34	Bridge_x_3b	2
n/a	34	58	n/a	22	30	34	Stapel 4	Bridge_x_4a	1
n/a	35	59	n/a	23	31	35	Bridge_x_4b	2	n/a

MetroCluster 3 oder DR-Gruppe 3

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 3 oder DR-Gruppe 3 für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port (FC1 oder FC2) auf Brocade -Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei Brocade G630- und G630-1-Switches können Sie zusätzliche Bridges an die Ports 60–63 anschließen.
- Bei Brocade G730-Switches können Sie zusätzliche Bridges an die Ports 64, 65, 68 und 69 anschließen.

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Stack 1	Bridge_x_1a	1	56	58
Bridge_x_1b	2	56	58	Stack 2
Bridge_x_2a	1	57	59	Bridge_x_2b
2	57	59	Stapel 3	Bridge_x_3a

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
1	58	62	Bridge_x_3b	2
58	62	Stapel 4	Bridge_x_4a	1
59	63	Bridge_x_4b	2	59

MetroCluster 4 oder DR-Gruppe 4

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 4 oder DR-Gruppe 4 für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port (FC1 oder FC2) auf Brocade -Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Bei Brocade G630- und G630-1-Switches können Sie zusätzliche Bridges an die Ports 80–83 anschließen.
- Auf Brocade G730-Switches können Sie zusätzliche Bridges an die Ports 84–95 anschließen.

* Komponente*	Port	Anschluss an FC-Switch…	G630, G630-1-Anschluss	G730-Anschluss
Stack 1	Bridge_x_1a	1	74	80
Bridge_x_1b	2	74	80	Stack 2
Bridge_x_2a	1	75	81	Bridge_x_2b
2	75	81	Stapel 3	Bridge_x_3a
1	78	82	Bridge_x_3b	2
78	82	Stapel 4	Bridge_x_4a	1
79	83	Bridge_x_4b	2	79

Brocade -Port-Nutzung für ISLs in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die Portzuweisungen, die zum Verkabeln von Brocade FC-Switches mit ISLs erforderlich sind.

- AFF A900 und FAS9500 Systeme unterstützen acht ISLs. Acht ISLs werden auf den Switches Brocade 6510, G620, G620-1, G630, G630-1, G720 und G730 unterstützt.
- Brocade 6520-Switches unterstützen acht ISLs, jedoch keine AFF A900 und FAS9500 Systeme.

ISL-Anschluss	6505-, G610-, G710-Anschluss	6520-Anschluss	7810-Anschluss	7840 (10-Gbit/s)-Anschluss	7840 (40-Gbit/s)-Anschluss	6510-, G620-, G620-1-, G630-, G630-1-, G720-, G730-Anschluss
ISL-Port 1	20	22	ge2	ge2	ge0	40
ISL-Port 2	21	23	ge3	ge3	ge1	41
ISL-Port 3	22	46	ge4	ge10	n/a	42
ISL-Port 4	23	47	ge5	ge11	n/a	43
ISL-Port 5	n/a	70	ge6	n/a	n/a	44
ISL-Port 6	n/a	71	ge7	n/a	n/a	45
ISL-Port 7	n/a	94	n/a	n/a	n/a	46
ISL-Port 8	n/a	95	n/a	n/a	n/a	47

Cisco -Port-Nutzung für Controller in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die erforderlichen Portzuweisungen zum Verkabeln der Cisco 9124V-, 9148S-, 9148V-, 9250i- und 9396S-FC-Switches mit Ihren Controllern.

In den Tabellen sind die maximal unterstützten Konfigurationen mit acht Controller-Modulen in zwei DR-Gruppen aufgeführt. Bei kleineren Konfigurationen ignorieren Sie die Zeilen für die zusätzlichen Controller-Module.

- Informationen zu Cisco 9132T finden Sie unter "Cisco 9132T-Portnutzung für Controller in einer MetroCluster FC-Konfiguration" .
- Cisco 9124V- und 9250i-Switches werden in MetroCluster -Konfigurationen mit acht Knoten nicht unterstützt.

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 1 oder DR-Gruppe 1 auf Cisco -Switches (ausgenommen 9132T).

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Controller_x_1	FC-VI-Port A	1	1	1	1	1	1

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
FC-VI-Port b	2	1	1	1	1	1	FC-VI-Port c
1	2	2	2	2	2	FC-VI-Port d	2
2	2	2	2	2	FC-VI-2-Port A	1	3
n/a	3	n/a	n/a	FC-VI-2-Port b	2	3	n/a
3	n/a	n/a	FC-VI-2-Port c	1	4	n/a	4
n/a	n/a	FC-VI-2-Port d	2	4	n/a	4	n/a
n/a	HBA-Port A	1	13	3	13	3	3
HBA-Port b	2	13	3	13	3	3	HBA-Port c
1	14	4	14	4	4	HBA-Port d	2
14	4	14	4	4	Controller_x_2	FC-VI-Port A	1
5	5	5	5	5	FC-VI-Port b	2	5
5	5	5	5	FC-VI-Port c	1	6	6
6	6	6	FC-VI-Port d	2	6	6	6
6	6	FC-VI-2-Port A	1	7	n/a	7	n/a
n/a	FC-VI-2-Port b	2	7	n/a	7	n/a	n/a
FC-VI-2-Port c	1	8	n/a	8	n/a	n/a	FC-VI-2-Port d

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
2	8	n/a	8	n/a	n/a	HBA-Port A	1
15	7	15	7	7	HBA-Port b	2	15
7	15	7	7	HBA-Port c	1	16	8
16	8	8	HBA-Port d	2	16	8	16

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Controllerkonfigurationen in MetroCluster 2 oder DR-Gruppe 2 auf Cisco -Switches (ausgenommen 9132T).

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Controller_x_3	FC-VI-Port A	1	n/a	25	25	n/a	49
FC-VI-Port b	2	n/a	25	25	n/a	49	FC-VI-Port c
1	n/a	26	26	n/a	50	FC-VI-Port d	2
n/a	26	26	n/a	50	FC-VI-2-Port A	1	n/a
n/a	27	n/a	n/a	FC-VI-2-Port b	2	n/a	n/a
27	n/a	n/a	FC-VI-2-Port c	1	n/a	n/a	28
n/a	n/a	FC-VI-2-Port d	2	n/a	n/a	28	n/a
n/a	HBA-Port A	1	n/a	27	37	n/a	51
HBA-Port b	2	n/a	27	37	n/a	51	HBA-Port c
1	n/a	28	38	n/a	52	HBA-Port d	2

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
n/a	28	38	n/a	52	Controller_x_4	FC-VI-Port A	1
n/a	29	29	n/a	53	FC-VI-Port b	2	n/a
29	29	n/a	53	FC-VI-Port c	1	n/a	30
30	n/a	54	FC-VI-Port d	2	n/a	30	30
n/a	54	FC-VI-2-Port A	1	n/a	n/a	31	n/a
n/a	FC-VI-2-Port b	2	n/a	n/a	31	n/a	n/a
FC-VI-2-Port c	1	n/a	n/a	32	n/a	n/a	FC-VI-2-Port d
2	n/a	n/a	32	n/a	n/a	HBA-Port A	1
n/a	31	39	n/a	55	HBA-Port b	2	n/a
31	39	n/a	55	HBA-Port c	1	n/a	32
40	n/a	56	HBA-Port d	1	n/a	32	40

Cisco -Port-Nutzung für FC-zu-SAS-Brücken in einer MetroCluster FC-Konfiguration

Erfahren Sie mehr über die erforderlichen Portzuweisungen für die Verkabelung der Cisco 9124V-, 9148S-, 9148V-, 9250i- und 9396S-FC-Switches mit FC-zu-SAS-Brücken. Die Portzuweisungen variieren je nachdem, ob die Brücken einen oder zwei FC-Ports verwenden.

> Informationen zu Cisco 9132T finden Sie unter "Cisco 9132t-Portnutzung für FC-zu-SAS-Brücken in einer MetroCluster FC-Konfiguration" .

Shelf-Konfigurationen mit FibreBridge 7500N oder 7600N mit beiden FC-Ports (FC1 und FC2)

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 1 oder DR-Gruppe 1 mit FibreBridge 7500N- oder 7600N-Brücken und den beiden FC-Ports (FC1 und FC2) auf Cisco Switches (außer

9132T). Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Auf Cisco 9250i-Switches können Sie zusätzliche MetroCluster 1- oder DR-Gruppe 1-Bridges an die Ports 17–40 anschließen.
- Auf Cisco 9396S-Switches können Sie zusätzliche MetroCluster 1- oder DR-Gruppe 1-Bridges an die Ports 17–32 anschließen.

* Komponente*		Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Stack 1	Bridge_x_1a	FC1	1	17	9	17	9	9
FC2	2	17	9	17	9	9	Bridge_x_1b	FC1
1	18	10	18	10	10	FC2	2	18
10	18	10	10	Stack 2	Bridge_x_2a	FC1	1	19
11	19	11	11	FC2	2	19	11	19
11	11	Bridge_x_2b	FC1	1	20	12	20	12
12	FC2	2	20	12	20	12	12	Stapel 3
Bridge_x_3a	FC1	1	21	13	21	13	13	FC2
2	21	13	21	13	13	Bridge_x_3b	FC1	1
22	14	22	14	14	FC2	2	22	14
22	14	14	Stapel 4	Bridge_x_4a	FC1	1	23	15
23	15	15	FC2	2	23	15	23	15
15	Bridge_x_4b	FC1	1	24	16	24	16	16

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 2 oder DR-Gruppe 2 mit

FibreBridge 7500N oder 7600N und beiden FC-Ports (FC1 und FC2) auf Cisco Switches (außer 9132T). Beachten Sie bei der Verwendung der Verkabelungstabellen Folgendes:

- Cisco 9124V- und 9250i-Switches werden für MetroCluster Konfigurationen mit acht Knoten nicht unterstützt.
- Auf Cisco 9396S-Switches können Sie zusätzliche MetroCluster 2-Bridges (DR-Gruppe 2) an die Ports 65–80 anschließen.

* Komponente*		Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Stack 1	Bridge_x_1a	FC1	1	n/a	33	41	n/a	57
FC2	2	n/a	33	41	n/a	57	Bridge_x_1b	FC1
1	n/a	34	42	n/a	58	FC2	2	n/a
34	42	n/a	58	Stack 2	Bridge_x_2a	FC1	1	n/a
35	43	n/a	59	FC2	2	n/a	35	43
n/a	59	Bridge_x_2b	FC1	1	n/a	36	44	n/a
60	FC2	2	n/a	36	44	n/a	60	Stapel 3
Bridge_x_3a	FC1	1	n/a	37	45	n/a	61	FC2
2	n/a	37	45	n/a	61	Bridge_x_3b	FC1	1
n/a	38	46	n/a	62	FC2	2	n/a	38
46	n/a	62	Stapel 4	Bridge_x_4a	FC1	1	n/a	39
47	n/a	63	FC2	2	n/a	39	47	n/a
63	Bridge_x_4b	FC1	1	n/a	40	48	n/a	64

Shelf-Konfigurationen mit FibreBridge 7500N oder 7600N und nur einem FC-Port (FC1 oder FC2)

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 1 oder DR-Gruppe 1 für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port (FC1 oder FC2) auf Cisco Switches (außer 9132T). Die Referenzkonfigurationsdatei (RCF) unterstützt keinen FC-Port auf FibreBridge-Bridges. Daher müssen Sie die Back-End-Fibre-Channel-Switches manuell konfigurieren.

"Konfigurieren Sie Cisco FC-Switches manuell"

Folgendes sollten Sie bei der Verwendung der Verkabelungstabellen beachten:

- Auf Cisco 9250i-Switches können Sie zusätzliche MetroCluster 1- oder DR-Gruppe 1-Bridges an die Ports 17–40 anschließen.
- Auf Cisco 9396S-Switches können Sie zusätzliche MetroCluster 1- oder DR-Gruppe 1-Bridges an die Ports 17–32 anschließen.

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Stack 1	Bridge_x_1a	1	17	9	17	9	9
Bridge_x_1b	2	17	9	17	9	9	Stack 2
Bridge_x_2a	1	18	10	18	10	10	Bridge_x_2b
2	18	10	18	10	10	Stapel 3	Bridge_x_3a
1	19	11	19	11	11	Bridge_x_3b	2
19	11	19	11	11	Stapel 4	Bridge_x_4a	1
20	12	20	12	12	Bridge_x_4b	2	20
12	20	12	12	Stapel 5	Bridge_x_5a	1	21
13	21	13	13	Bridge_x_5b	2	21	13

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
21	13	13	Stapel 6	Bridge_x_6 a	1	22	14
22	14	14	Bridge_x_6 b	2	22	14	22
14	14	Stapel 7	Bridge_x_7 a	1	23	15	23
15	15	Bridge_x_7 b	2	23	15	23	15
15	Stapel 8	Bridge_x_8 a	1	24	16	24	16
16	Bridge_x_8 b	2	24	16	24	16	16

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 2 oder DR-Gruppe 2 für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port (FC1 oder FC2) auf Cisco Switches (außer 9132T). Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- Die Cisco Switches 9124V und 9250i werden für MetroCluster -Konfigurationen mit acht Knoten nicht unterstützt.
- Auf Cisco 9396S-Switches können Sie zusätzliche MetroCluster 2- oder DR-Gruppe 2-Bridges an die Ports 65–80 anschließen.

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
Stack 1	Bridge_x_1 a	1	n/a	33	41	n/a	57
Bridge_x_1 b	2	n/a	33	41	n/a	57	Stack 2
Bridge_x_2 a	1	n/a	34	42	n/a	58	Bridge_x_2 b
2	n/a	34	42	n/a	58	Stapel 3	Bridge_x_3 a

* Komponente*	Port	Anschluss an FC-Switch…	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
1	n/a	35	43	n/a	59	Bridge_x_3 b	2
n/a	35	43	n/a	59	Stapel 4	Bridge_x_4 a	1
n/a	36	44	n/a	60	Bridge_x_4 b	2	n/a
36	44	n/a	60	Stapel 5	Bridge_x_5 a	1	n/a
37	45	n/a	61	Bridge_x_5 b	2	n/a	37
45	n/a	61	Stapel 6	Bridge_x_6 a	1	n/a	38
46	n/a	62	Bridge_x_6 b	2	n/a	38	46
n/a	62	Stapel 7	Bridge_x_7 a	1	n/a	39	47
n/a	63	Bridge_x_7 b	2	n/a	39	47	n/a
63	Stapel 8	Bridge_x_8 a	1	n/a	40	48	n/a
64	Bridge_x_8 b	2	n/a	40	48	n/a	64

Cisco -Portnutzung für ISLs in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die Portzuweisungen, die zum Verkabeln der Cisco 9124V-, 9148S-, 9148V-, 9250i- und 9396S-FC-Switches mit ISLs erforderlich sind.

Die folgende Tabelle zeigt die Verwendung des ISL-Ports. Die Verwendung des ISL-Ports ist bei allen Switches in der Konfiguration identisch.

- Informationen zu Cisco 9132T finden Sie unter "Cisco 9132T-Portnutzung für ISLs in einer MetroCluster FC-Konfiguration" .
- Für den Cisco 9250i-Switch ist eine Lizenz für 24 Ports erforderlich.

ISL-Anschluss	9124V-Anschluss	9148S-Anschluss	9148V-Anschluss	9250i-Anschluss	9396S-Anschluss
ISL-Port 1	9	20	9	12	44
ISL-Port 2	10	24	10	16	48
ISL-Port 3	11	44	11	20	92
ISL-Port 4	12	48	12	24	96
ISL-Port 5	n/a	n/a	33	n/a	n/a
ISL-Port 6	n/a	n/a	34	n/a	n/a
ISL-Port 7	n/a	n/a	35	n/a	n/a
ISL-Port 8	n/a	n/a	36	n/a	n/a

Cisco 9132T-Portnutzung für Controller in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die Portzuweisungen, die zum Verkabeln von Cisco 9132T FC-Switches mit Ihren Controllern erforderlich sind.

In der folgenden Tabelle sind die Controller-Konfigurationen aufgeführt, die FibreBridge 7500N oder 7600N verwenden, die beide FC-Ports (FC1 und FC2) verwenden. Die Tabellen zeigen die maximal unterstützten Konfigurationen mit vier und acht Controller-Modulen in zwei DR-Gruppen.

> Bei Konfigurationen mit acht Nodes müssen Sie das Zoning manuell ausführen, da keine RCFs bereitgestellt werden.

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Controller-Konfigurationen für MetroCluster 1 oder DR-Gruppe 1 auf Cisco 9132T-Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- AFF A900 und FAS9500 Systeme verfügen über acht FC-VI-Ports (a, b, c und d für FC-VI-1 und FC-VI-2).

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
Controller_x_1	FC-VI-Port A	1	LEM1-1	LEM1-1	LEM1-1	FC-VI-Port b
2	LEM1-1	LEM1-1	LEM1-1	FC-VI-Port c	1	LEM1-2
LEM1-2	LEM1-2	FC-VI-Port d	2	LEM1-2	LEM1-2	LEM1-2

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
FC-VI-2-Port A	1	LEM1-3	LEM1-3	n/a	FC-VI-2-Port b	2
LEM1-3	LEM1-3	n/a	FC-VI-2-Port c	1	LEM1-4	LEM1-4
n/a	FC-VI-2-Port d	2	LEM1-4	LEM1-4	n/a	HBA-Port A
1	LEM1-5	LEM1-5	LEM1-3	HBA-Port b	2	LEM1-5
LEM1-5	LEM1-3	HBA-Port c	1	LEM1-6	LEM1-6	LEM1-4
HBA-Port d	2	LEM1-6	LEM1-6	LEM1-4	Controller_x_2	FC-VI-Port A
1	LEM1-7	LEM1-7	LEM1-5	FC-VI-Port b	2	LEM1-7
LEM1-7	LEM1-5	FC-VI-Port c	1	LEM1-8	LEM1-8	LEM1-6
FC-VI-Port d	2	LEM1-8	LEM1-8	LEM1-6	FC-VI-2-Port A	1
LEM1-9	LEM1-9	n/a	FC-VI-2-Port b	2	LEM1-9	LEM1-9
n/a	FC-VI-2-Port c	1	LEM1-10	LEM1-10	n/a	FC-VI-2-Port d
2	LEM1-10	LEM1-10	n/a	HBA-Port A	1	LEM1-11
LEM1-11	LEM1-7	HBA-Port b	2	LEM1-11	LEM1-11	LEM1-7
HBA-Port c	1	LEM1-12	LEM1-12	LEM1-8	HBA-Port d	2

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Cisco 9132T-Controller-Konfigurationen für MetroCluster 2 oder DR-Gruppe 2 auf Cisco 9132T-Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- AFF A900 und FAS9500 Systeme verfügen über acht FC-VI-Ports (a, b, c und d für FC-VI-1 und FC-VI-2).
- MetroCluster 2 oder DR-Gruppe 2 wird auf Cisco 9132T-Switches für AFF A900 und FAS9500 Systeme nicht unterstützt.

- MetroCluster 2 oder DR-Gruppe 2 wird nur in MetroCluster -Konfigurationen mit acht Knoten unterstützt

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
Controller_x_3	FC-VI-Port A	1	n/a	n/a	LEM2-1	FC-VI-Port b
2	n/a	n/a	LEM2-1	FC-VI-Port c	1	n/a
n/a	LEM2-2	FC-VI-Port d	2	n/a	n/a	LEM2-2
FC-VI-2-Port A	1	n/a	n/a	n/a	FC-VI-2-Port b	2
n/a	n/a	n/a	FC-VI-2-Port c	1	n/a	n/a
n/a	FC-VI-2-Port d	2	n/a	n/a	n/a	HBA-Port A
1	n/a	n/a	LEM2-3	HBA-Port b	2	n/a
n/a	LEM2-3	HBA-Port c	1	n/a	n/a	LEM2-4
HBA-Port d	2	n/a	n/a	LEM2-4	Controller_x_4	FC-VI-1-Port A
1	n/a	n/a	LEM2-5	FC-VI-1-Port b	2	n/a
n/a	LEM2-5	FC-VI-1-Port c	1	n/a	n/a	LEM2-6
FC-VI-1-Port d	2	n/a	n/a	LEM2-6	FC-VI-2-Port A	1
n/a	n/a	n/a	FC-VI-2-Port b	2	n/a	n/a
n/a	FC-VI-2-Port c	1	n/a	n/a	n/a	FC-VI-2-Port d
2	n/a	n/a	n/a	HBA-Port A	1	n/a
n/a	LEM2-7	HBA-Port b	2	n/a	n/a	LEM2-7
HBA-Port c	1	n/a	n/a	LEM2-8	HBA-Port d	2

Cisco 9132T-Portnutzung für FC-zu-SAS-Brücken in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die erforderlichen Portzuweisungen zum Verkabeln von Cisco 9132T FC-Switches mit FC-zu-SAS-Brücken unter Verwendung beider FC-Ports.

> Bei Verwendung von Cisco 9132T-Switches mit 1xLEM-Modul wird nur ein (1) Bridge-Stack unterstützt.

MetroCluster 1 oder DR-Gruppe 1

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 1 oder DR-Gruppe 1 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Cisco 9132T-Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- In Konfigurationen mit vier Knoten können Sie zusätzliche Brücken an die Ports LEM2-1 bis LEM2-8 auf Cisco 9132T-Switches mit 2xLEMs verkabeln.

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
Stack 1	Bridge_x_1a	FC1	1	LEM1-13	LEM1-13	LEM1-9
FC2	2	LEM1-13	LEM1-13	LEM1-9	Bridge_x_1b	FC1
1	LEM1-14	LEM1-14	LEM1-10	FC2	2	LEM1-14
LEM1-14	LEM1-10	Stack 2	Bridge_x_2a	FC1	1	n/a
LEM1-15	LEM1-11	FC2	2	n/a	LEM1-15	LEM1-11
Bridge_x_2b	FC1	1	n/a	LEM1-16	LEM1-12	FC2

MetroCluster 2 oder DR-Gruppe 2

Die folgende Tabelle zeigt die unterstützten Shelf-Konfigurationen in MetroCluster 2 oder DR-Gruppe 2 für FibreBridge 7500N- oder 7600N-Bridges unter Verwendung beider FC-Ports (FC1 und FC2) auf Cisco 9132T-Switches. Beachten Sie bei der Verwendung dieser Konfigurationstabelle Folgendes:

- In Konfigurationen mit acht Knoten können Sie zusätzliche Brücken an die Ports LEM2-13 bis LEM2-16 auf Cisco 9132T-Switches mit 2x LEMs verkabeln.

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
Stack 1	Bridge_x_1a	FC1	1	n/a	n/a	LEM1-9
FC2	2	n/a	n/a	LEM1-9	Bridge_x_1b	FC1

* Komponente*		Port	Verbindet sich mit FC_switch…	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
1	n/a	n/a	LEM1-10	FC2	2	n/a
n/a	LEM1-10	Stack 2	Bridge_x_2a	FC1	1	n/a
n/a	LEM1-11	FC2	2	n/a	n/a	LEM1-11
Bridge_x_2b	FC1	1	n/a	n/a	LEM1-12	FC2

Cisco 9132T-Portnutzung für ISLs in einer MetroCluster FC-Konfiguration

Informieren Sie sich über die Portzuweisungen, die zum Verkabeln von Cisco 9132T FC-Switches mit ISLs erforderlich sind.

Die folgende Tabelle zeigt die Verwendung der ISL-Ports für einen Cisco 9132T-Switch.

ISL-Anschluss	9132T 1x LEM (Vier-Knoten)	9132T 2x LEM (Vier-Knoten)	9132T 2x LEM (Acht-Knoten)
ISL-Port 1	LEM1-15	LEM2-9	LEM1-13
ISL-Port 2	LEM1-16	LEM2-10	LEM1-14
ISL-Port 3	n/a	LEM2-11	LEM1-15
ISL-Port 4	n/a	LEM2-12	LEM1-16
ISL-Port 5	n/a	LEM2-13	n/a
ISL-Port 6	n/a	LEM2-14	n/a
ISL-Port 7	n/a	LEM2-15	n/a
ISL-Port 8	n/a	LEM2-16	n/a

Verkabelung des Cluster Interconnect in Konfigurationen mit acht oder vier Nodes

In MetroCluster-Konfigurationen mit acht oder vier Nodes müssen Sie die Cluster-Verbindung zwischen den lokalen Controller-Modulen an jedem Standort verkabeln.

Über diese Aufgabe

In MetroCluster-Konfigurationen mit zwei Nodes ist diese Aufgabe nicht erforderlich.

Dieser Vorgang muss an beiden MetroCluster-Standorten durchgeführt werden.

Schritt

1. Verkabeln Sie den Cluster-Interconnect von einem Controller-Modul zum anderen oder falls Cluster-Interconnect-Switches verwendet werden, von jedem Controller-Modul zu den Switches.

Verwandte Informationen

"Dokumentation zu ONTAP Hardwaresystemen"

"Netzwerk- und LIF-Management"

Verkabeln der Cluster-Peering-Verbindungen

Sie müssen die für Cluster-Peering verwendeten Controller-Modul-Ports verkabeln, damit sie eine Verbindung zum Cluster am Partnerstandort haben.

Über diese Aufgabe

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.

Schritt

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.

Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

Jede MetroCluster Website ist als Peer-to-dessen Partner-Website konfiguriert. Sie sollten die Voraussetzungen und Richtlinien für die Konfiguration der Peering-Beziehungen kennen und bei der Entscheidung, ob für diese Beziehungen freigegebene oder dedizierte Ports verwendet werden sollen.

"Cluster-Peering"

Verkabelung des HA Interconnect

Wenn Sie eine MetroCluster-Konfiguration mit acht oder vier Nodes haben und sich die Storage Controller innerhalb der HA-Paare in einem separaten Chassis befinden, müssen Sie den HA Interconnect zwischen den Controllern verkabeln.

Über diese Aufgabe

- Diese Aufgabe gilt nicht für MetroCluster-Konfigurationen mit zwei Nodes.
- Dieser Vorgang muss an beiden MetroCluster-Standorten durchgeführt werden.
- Der HA Interconnect muss nur verkabelt werden, wenn sich die Storage-Controller innerhalb des HA-Paars in einem separaten Chassis befinden.

  Einige Storage Controller-Modelle unterstützen zwei Controller in einem einzelnen Chassis, in diesem Fall wird ein interner HA Interconnect verwendet.

Schritte

1. Verkabeln Sie den HA Interconnect, wenn sich der HA-Partner des Storage Controllers in einem separaten Chassis befindet.

   "Dokumentation zu ONTAP Hardwaresystemen"

2. Wenn der Standort MetroCluster zwei HA-Paare enthält, wiederholen Sie die vorherigen Schritte auf dem zweiten HA-Paar.
3. Wiederholen Sie diesen Vorgang auf der MetroCluster-Partnerseite.

Verkabelung der Management- und Datenverbindungen

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

Über diese Aufgabe

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

Sie können die Management-Ports des Controllers und des Cluster Switches mit vorhandenen Switches im Netzwerk oder mit neuen dedizierten Netzwerk-Switches wie den NetApp CN1601 Cluster Management Switches verbinden.

Schritt

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

   "Dokumentation zu ONTAP Hardwaresystemen"

Konfigurieren Sie die FC-Switches

FC Switch-Konfiguration – Übersicht

Sie können Cisco- und Brocade-FC-Switches mithilfe von RCF-Dateien konfigurieren oder, falls erforderlich, die Switches manuell konfigurieren.

Sie suchen…	Gehen Sie wie folgt vor:
Halten Sie eine RCF bereit, die Ihren Anforderungen entspricht	• "Konfigurieren Sie Brocade FC Switches mit RCF-Dateien" • "Konfigurieren Sie Cisco FC-Switches mit RCF-Dateien"
Sie verfügen weder über eine RZB noch über eine RZB, die Ihren Anforderungen nicht entspricht	• "Konfigurieren Sie die Brocade FC-Switches manuell" • "Konfigurieren Sie Cisco FC-Switches manuell"

Konfigurieren Sie Brocade FC Switches mit RCF-Dateien

Zurücksetzen des Brocade FC-Switch auf die Werkseinstellungen

Bevor Sie eine neue Softwareversion und RCF-Dateien installieren, müssen Sie die aktuelle Switch-Konfiguration löschen und eine grundlegende Konfiguration durchführen.

Über diese Aufgabe

Sie müssen diese Schritte bei jedem der FC-Switches in der MetroCluster Fabric-Konfiguration wiederholen.

Schritte

1. Melden Sie sich als Administrator beim Switch an.
2. Deaktivieren Sie die Brocade Virtual Fabrics (VF) Funktion:

   `fosconfig options`

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   WARNING:  This is a disruptive operation that requires a reboot to take
   effect.
   Would you like to continue  [Y/N]: y
   ```

3. Trennen Sie die ISL-Kabel von den Ports am Switch.
4. Deaktivieren Sie den Schalter:

   `switchcfgpersistentdisable`

   ```
   FC_switch_A_1:admin> switchcfgpersistentdisable
   ```

5. Deaktivieren der Konfiguration:

   `cfgDisable`

   ```
   FC_switch_A_1:admin> cfgDisable
   You are about to disable zoning configuration. This action will disable
   any previous zoning configuration enabled.
   Do you want to disable zoning configuration? (yes, y, no, n): [no] y
   Updating flash ...
   Effective configuration is empty. "No  Access" default zone mode is ON.
   ```

6. Löschen Sie die Konfiguration:

   `cfgClear`

```
FC_switch_A_1:admin> cfgClear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
Run cfgSave to commit the transaction or cfgTransAbort to
cancel the transaction.
Do you really want to clear all configurations?  (yes, y, no, n): [no] y
```

7. Konfiguration speichern:

   `cfgSave`

```
FC_switch_A_1:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only?  (yes, y, no,
n): [no] y
Updating flash ...
```

8. Legen Sie die Standardkonfiguration fest:

   `configDefault`

```
FC_switch_A_1:admin> configDefault
WARNING:  This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

9. Setzen Sie für alle Ports die Portkonfiguration auf Standard:

   `portcfgdefault port-number`

   ```
   FC_switch_A_1:admin> portcfgdefault <port number>
   ```

   Diesen Schritt müssen Sie für jeden Port abschließen.

10. Wenn Sie eine Version vor FOS 9.0 ausführen, überprüfen Sie, ob der Switch die dynamische Port-on-Demand-Methode (POD) verwendet.

    > In Fabric OS 9.0 und höher ist die Lizenzmethode standardmäßig dynamisch. Die statische Lizenzmethode wird nicht unterstützt.

    Bei Brocade Fabric OS-Versionen vor 8.0 führen Sie die folgenden Befehle als admin aus, für Versionen 8.0 und höher führen Sie sie als root aus.

    a. Führen Sie den Lizenzbefehl aus:

       `licenseport --show .`

       ```
       FC_switch_A_1:admin> license --show -port
       24 ports are available in this switch
       Full POD license is installed
       Dynamic POD method is in use
       ```

    b. Aktivieren Sie den Root-Benutzer, wenn er von Brocade deaktiviert ist.

       ```
       FC_switch_A_1:admin> userconfig --change root -e yes
       FC_switch_A_1:admin> rootaccess --set consoleonly
       ```

    c. Führen Sie den Lizenzbefehl aus:

       `licenseport --show .`

       ```
       FC_switch_A_1:root> license --show -port
       24 ports are available in this switch
       Full POD license is installed
       Dynamic POD method is in use
       ```

    d. Wenn Sie Fabric OS 8.2.x und eine frühere Version verwenden, müssen Sie die Lizenzmethode in „dynamisch“ ändern:

       `licenseport --method dynamic`

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

11. Starten Sie den Switch neu:

    ```
    fastBoot
    ```

    ```
    FC_switch_A_1:admin> fastboot
    Warning: This command would cause the switch to reboot
    and result in traffic disruption.
    Are you sure you want to reboot the switch [y/n]?y
    ```

12. Vergewissern Sie sich, dass die Standardeinstellungen implementiert wurden:

    ```
    switchShow
    ```

13. Überprüfen Sie, ob die IP-Adresse korrekt eingestellt ist:

    ```
    ipAddrShow
    ```

    Sie können die IP-Adresse bei Bedarf mit dem folgenden Befehl einstellen:

    ```
    ipAddrSet
    ```

Herunterladen der RCF-Datei des Brocade FC-Switch

Sie müssen die Referenzkonfigurationsdatei (RCF) auf jeden Switch der MetroCluster Fabric-Konfiguration herunterladen.

Über diese Aufgabe

Um diese RCF-Dateien zu verwenden, muss das System ONTAP 9.1 oder höher ausführen und Sie müssen das Portlayout für ONTAP 9.1 oder höher verwenden.

Wenn Sie nur einen der FC-Ports auf den FibreBridge-Brücken verwenden möchten, konfigurieren Sie die Back-End-Fibre-Channel-Switches manuell gemäß den Anweisungen im Abschnitt "Portzuweisungen für FC-Switches" .

Schritte

1. Sehen Sie sich die RCF-Dateitabelle auf der Brocade RCF-Downloadseite an und identifizieren Sie für jeden Switch Ihrer Konfiguration die richtige RCF-Datei.

   Die RCF-Dateien müssen auf die richtigen Schalter angewendet werden.

2. Laden Sie die RCF-Dateien für die Schalter von herunter "MetroCluster RCF-Download" Seite.

   Die Dateien müssen an einem Speicherort abgelegt werden, an dem sie auf den Switch übertragen werden können. Es gibt für jeden der vier Switches eine separate Datei, aus der sich die zwei-Switch-Fabric besteht.

3. Wiederholen Sie diese Schritte bei jedem Switch in der Konfiguration.

Installieren der RCF-Datei des Brocade FC-Switch

Wenn Sie einen Brocade FC-Switch konfigurieren, können Sie die Switch-Konfigurationsdateien installieren, die die vollständigen Switch-Einstellungen für bestimmte Konfigurationen bereitstellen.

Über diese Aufgabe

- Sie müssen diese Schritte auf jedem der Brocade FC-Switches in der MetroCluster-Fabric-Konfiguration wiederholen.
- Wenn Sie eine xWDM-Konfiguration verwenden, benötigen Sie möglicherweise zusätzliche Einstellungen für die ISLs. Weitere Informationen finden Sie in der xWDM-Herstellerdokumentation.

Schritte

1. Initiieren des Download- und Konfigurationsprozesses:

   ```
   configDownload
   ```

   Beantworten Sie die Eingabeaufforderungen wie im folgenden Beispiel gezeigt.

   ```
   FC_switch_A_1:admin> configDownload
   Protocol (scp, ftp, sftp, local) [ftp]:
   Server Name or IP Address [host]: <user input>
   User Name [user]:<user input>
   Path/Filename [<home dir>/config.txt]:path to configuration file
   Section (all|chassis|switch [all]): all
   .
   .
   .
   Do you want to continue [y/n]: y
   Password: <user input>
   ```

   Nach Eingabe Ihres Kennworts lädt der Switch die Konfigurationsdatei herunter und führt sie aus.

2. Vergewissern Sie sich, dass die Konfigurationsdatei die Switch-Domäne eingestellt hat:

   ```
   switchShow
   ```

   Jedem Switch wird je nach Konfigurationsdatei des Switch eine andere Domänennummer zugewiesen.

```
FC_switch_A_1:admin> switchShow
switchName: FC_switch_A_1
switchType: 109.1
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 5
```

3. Vergewissern Sie sich, dass Ihrem Switch der richtige Domänenwert zugewiesen ist, wie in der folgenden Tabelle angegeben.

Fabric	Switch	Switch-Domäne
1	A_1	5
B_1	7	2
A_2	6	B_2

4. Ändern Sie die Portgeschwindigkeit:

   `portcfgspeed`

   ```
   FC_switch_A_1:admin> portcfgspeed port number port speed
   ```

   Standardmäßig sind alle Ports für den Betrieb mit 16 Gbit/s konfiguriert. Sie können die Portgeschwindigkeit aus den folgenden Gründen ändern:

   - Die Geschwindigkeit der Interconnect-Switch-Ports sollte geändert werden, wenn ein 8-Gbps FC-VI-Adapter verwendet wird und die Switch-Port-Geschwindigkeit auf 8 Gbit/s eingestellt werden sollte.
   - Die Geschwindigkeit der ISL-Ports muss geändert werden, wenn ISL nicht mit 16 Gbit/s ausgeführt werden kann.

5. Berechnen der ISL-Entfernung.

   Aufgrund des Verhaltens des FC-VI müssen Sie den Abstand auf das 1.5-fache des realen Abstands mit einem Minimum von 10 (LE) einstellen. Die Entfernung für die ISL wird wie folgt berechnet, gerundet auf den nächsten vollen Kilometer: 1.5 × real distance = distance.

   Wenn die Entfernung 3 km beträgt, dann 1.5 × 3 km = 4.5. Dieser Wert ist niedriger als 10; Sie müssen daher den ISL auf DEN ABSTAND LE einstellen.

   Die Entfernung beträgt 20 km, dann 1.5 × 20 km = 30. Sie müssen die ISL auf die LS-Distanzebene einstellen.

6. Legen Sie die Entfernung für jeden ISL-Port fest:

   `portcfglongdistance` *`port level vc_link_init`* `-distance` *`distance_value`*

Ein vc_Link_init-Wert von 1 verwendet standardmäßig das Füllwort "ARB". Ein Wert von 0 verwendet das Füllwort „IM LEERLAUF“. Der erforderliche Wert kann je nach verwendeter Verbindung variieren. In diesem Beispiel wird der Standardwert festgelegt und die Entfernung wird von 20 km angenommen Daher ist die Einstellung „30“ mit einem vc_Link_init Wert von „1“ und der ISL-Port ist „21“.

Beispiel: LS

```
FC_switch_A_1:admin> portcfglongdistance 21 LS 1 -distance 30
```

Beispiel: LE

```
FC_switch_A_1:admin> portcfglongdistance 21 LE 1
```

7. Dauerhaft aktivieren Sie den Switch:

   `switchcfgpersistentenable`

   Das Beispiel zeigt, wie FC Switch_A_1 dauerhaft aktiviert werden kann.

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

8. Überprüfen Sie, ob die IP-Adresse richtig eingestellt ist:

   `ipAddrshow`

   ```
   FC_switch_A_1:admin> ipAddrshow
   ```

   Sie können die IP-Adresse bei Bedarf einstellen:

   `ipAddrSet`

9. Legen Sie die Zeitzone über die Switch-Eingabeaufforderung fest:

   `tstimezone --interactive`

   Sie sollten bei Bedarf auf die Eingabeaufforderungen antworten.

   ```
   FC_switch_A_1:admin>  tstimezone --interactive
   ```

10. Starten Sie den Switch neu:

    `reboot`

    Das Beispiel zeigt, wie der FC-Switch _A_1 neu gebootet wird.

```
FC_switch_A_1:admin> reboot
```

11. Überprüfen Sie die Distanzeinstellung:

    ```
    portbuffershow
    ```

    Eine Abstandseinstellung von LE erscheint als 10 km

    ```
    FC_Switch_A_1:admin> portbuffershow
    User Port Lx   Max/Resv Buffer Needed  Link     Remaining
    Port Type Mode Buffers  Usage  Buffers Distance Buffers
    ---- ---- ---- ------- ------ ------- --------- ----------
    ...
    21    E    -      8      67     67      30 km
    22    E    -      8      67     67      30 km
    ...
    23    -    8      0       -      -      466
    ```

12. Schließen Sie die ISL-Kabel wieder an die Ports der Switches an, wo sie entfernt wurden.

    Die ISL-Kabel wurden getrennt, wenn die Werkseinstellungen auf die Standardeinstellungen zurückgesetzt wurden.

    "Zurücksetzen des Brocade FC-Switch auf die Werkseinstellungen"

13. Überprüfen Sie die Konfiguration.

    a. Stellen Sie sicher, dass die Switches eine Fabric bilden:

       ```
       switchshow
       ```

       Das folgende Beispiel zeigt die Ausgabe für eine Konfiguration, bei der ISLs auf den Ports 20 und 21 verwendet werden.

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==========================================
...
20   20  010C00   id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port,
master is Port 20)
...
```

b. Bestätigen Sie die Konfiguration der Fabrics:

```
fabricshow
```

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

c. Überprüfen Sie, ob die ISLs funktionieren:

```
islshow
```

```
FC_switch_A_1:admin> islshow
```

d. Bestätigen Sie die ordnungsgemäße Replizierung des Zoning:

```
cfgshow+
zoneshow
```

Beide Ausgaben sollten für beide Switches die gleichen Konfigurationsinformationen und Zoning-Informationen zeigen.

e. Wenn das Trunking verwendet wird, bestätigen Sie das Trunking:

```
trunkShow
```

```
FC_switch_A_1:admin> trunkshow
```

Konfigurieren Sie die Cisco FC Switches mit RCF-Dateien

Zurücksetzen des Cisco FC-Switches auf die Werkseinstellungen

Bevor Sie eine neue Softwareversion und RCFs installieren, müssen Sie die Cisco Switch-Konfiguration löschen und eine grundlegende Konfiguration durchführen.

Über diese Aufgabe

Sie müssen diese Schritte bei jedem der FC-Switches in der MetroCluster Fabric-Konfiguration wiederholen.

> Die angezeigten Ausgaben beziehen sich auf Cisco IP-Switches. Diese Schritte gelten jedoch auch für Cisco FC-Switches.

Schritte

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

   a. Löschen Sie die vorhandene Konfiguration:
   `write erase`

   b. Laden Sie die Switch-Software neu:
   `reload`

   Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung Auto Provisioning abbrechen und mit der normalen Einrichtung fortfahren?(ja/nein)[n], sollten Sie antworten **`yes`** Fortfahren.

   c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:

      - Admin-Passwort
      - Switch-Name
      - Out-of-Band-Managementkonfiguration
      - Standard-Gateway
      - SSH-Service (Remote Support Agent):

      Nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

   d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

   Im folgenden Beispiel werden die Eingabeaufforderungen und Systemantworten bei der Anmeldung am Switch angezeigt. Die Winkelklammern (`**<<<**`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password  **<<<**
  Confirm the password for "admin": password  **<<<**
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

e. Geben Sie grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Verwaltungsadresse und Gateway, und geben Sie ein **`rsa`** Für den SSH-Schlüssel, wie im Beispiel dargestellt:

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Eingabeaufforderung vervollständigt die Konfiguration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[##########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch_A_1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch_A_1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches der MetroCluster Fabric Konfiguration.

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch der MetroCluster-Fabric-Konfiguration herunterladen.

Bevor Sie beginnen

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Über diese Aufgabe

Diese Schritte müssen auf jedem der FC-Switches in der MetroCluster Fabric-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

> Die angezeigten Ausgaben beziehen sich auf Cisco IP-Switches. Diese Schritte gelten jedoch auch für Cisco FC-Switches.

Schritte

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Download-Seite"

2. Kopieren Sie die Switch-Software auf den Switch:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   In diesem Beispiel ist der `nxos.7.0.3.I4.6.bin` Datei wird vom SFTP-Server 10.10.99.99 in den lokalen Bootflash kopiert:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind:

   ```
   dir bootflash
   ```

Das folgende Beispiel zeigt, dass die Dateien auf vorhanden sind `IP_switch_A_1`:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software:

   ```
   install all system bootflash:nxos.version-number.bin kickstart
   bootflash:nxos.version-kickstart-number.bin
   ```

```
IP_switch_A_1#  install all system bootflash:nxos.7.0.3.I4.6.bin
kickstart bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"system".
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS
...
```

Der Schalter wird nach der Installation der Switch-Software automatisch neu gestartet.

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vergewissern Sie sich, dass die Switch-Software installiert ist:

   ```
   show version
   ```

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Wiederholen Sie diese Schritte auf den verbleibenden drei FC-Switches in der MetroCluster-Fabric-Konfiguration.

Herunterladen und Installieren der Cisco FC RCF-Dateien

Sie müssen die RCF-Datei auf jeden Switch der MetroCluster-Fabric-Konfiguration herunterladen.

Bevor Sie beginnen

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, Trivial File Transfer Protocol (TFTP), SFTP oder Secure Copy Protocol (SCP), um die Dateien auf die Switches zu kopieren.

Über diese Aufgabe

Diese Schritte müssen bei jedem der Cisco FC Switches in der MetroCluster Fabric Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Es gibt vier RCF-Dateien, eine für jeden der vier Switches in der MetroCluster-Fabric-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
FC_Switch_A_1	`NX3232_v1.80_Switch-A1.txt`
FC_Switch_A_2	`NX3232_v1.80_Switch-A2.txt`
FC_Switch_B_1	`NX3232_v1.80_Switch-B1.txt`
FC_Switch_B_2	`NX3232_v1.80_Switch-B2.txt`

Die angezeigten Ausgaben beziehen sich auf Cisco IP-Switches. Diese Schritte gelten jedoch auch für Cisco FC-Switches.

Schritte

1. Laden Sie die Cisco FC RCF-Dateien von herunter "MetroCluster RCF-Download-Seite".
2. Kopieren Sie die RCF-Dateien auf die Switches.

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch:

   ```
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
   bootflash: vrf management
   ```

   In diesem Beispiel ist der `NX3232_v1.80_Switch-A1.txt` Die RCF-Datei wird vom SFTP-Server unter kopiert `10.10.99.99` Zum lokalen Bootflash. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/NX3232_v1.8T-
X1_Switch-A1.txt bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Wiederholen Sie den vorherigen Unterschritt für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Überprüfen Sie auf jedem Switch, ob die RCF-Datei auf den einzelnen Switches vorhanden ist `bootflash` Verzeichnis:

   `dir bootflash:`

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
       5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Kopieren Sie die passende RCF-Datei vom lokalen Bootflash auf jeden Switch in die laufende Konfiguration:

   `copy bootflash:`*`switch-specific-RCF`*`.txt running-config`

5. Kopieren Sie die RCF-Dateien von der ausgeführten Konfiguration auf die Startkonfiguration auf jedem Switch:

```
copy running-config startup-config
```

Sie sollten eine Ausgabe wie die folgende sehen:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch_A_1# copy running-config startup-config
```

6. Schalter neu laden:

```
reload
```

```
IP_switch_A_1# reload
```

7. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Konfigurieren Sie die Brocade FC-Switches manuell

Sie müssen die einzelnen Brocade Switch-Fabrics in der MetroCluster Konfiguration konfigurieren.

Bevor Sie beginnen

- Sie müssen über eine PC- oder UNIX-Arbeitsstation mit Telnet- oder Secure Shell-Zugriff auf die FC-Switches verfügen.
- Sie müssen vier unterstützte Brocade Switches desselben Modells mit derselben Brocade Fabric Betriebssystemversion und derselben Lizenzierung verwenden.

  "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.

- Die vier unterstützten Brocade-Switches müssen mit jeweils zwei Fabrics von je zwei Switches verbunden sein, wobei jede Fabric beide Standorte umfasst.
- Jeder Storage-Controller muss vier Initiator-Ports besitzen, um mit den Switch-Fabrics verbunden zu werden. Von jedem Storage Controller müssen zwei Initiator-Ports mit jeder Fabric verbunden sein.

  > Sie können FAS8020, AFF8020, FAS8200 und AFF A300 Systeme mit zwei Initiatoren-Ports pro Controller (ein einzelner Initiator-Port zu jedem Fabric) konfigurieren, wenn alle folgenden Kriterien erfüllt sind:

  - Es sind weniger als vier FC-Initiator-Ports zum Verbinden des Festplatten-Storage verfügbar, und keine zusätzlichen Ports können als FC-Initiatoren konfiguriert werden.
  - Alle Steckplätze werden verwendet und es kann keine FC-Initiatorgruppe hinzugefügt werden.

Über diese Aufgabe

- Sie sollten Inter-Switch Link (ISL) Trunking aktivieren, wenn es von den Links unterstützt wird.

  "Überlegungen bei der Verwendung von TDM/WDM-Geräten mit Fabric-Attached MetroCluster-Konfigurationen"

- Wenn Sie eine xWDM-Konfiguration verwenden, benötigen Sie möglicherweise zusätzliche Einstellungen für die ISLs. Weitere Informationen finden Sie in der xWDM-Herstellerdokumentation.
- Alle ISLs müssen in einem Fabric dieselbe Länge und dieselbe Geschwindigkeit aufweisen.

  Verschiedene Längen können in den verschiedenen Stoffen verwendet werden. Die gleiche Geschwindigkeit muss in allen Stoffen verwendet werden.

- Metro-E und TDM (SONET/SDH) werden nicht unterstützt, und keine systemeigene Framing- oder Signalgebung, die nicht FC-Systeme sind, wird nicht unterstützt.

  Metro-E bedeutet, dass Ethernet-Framing oder -Signalisierung entweder nativ über eine Metro-Entfernung oder durch Zeitdivision-Multiplexing (TDM), Multiprotocol Label Switching (MPLS) oder Wavelength-Division Multiplexing (WDM) erfolgt.

- TDMS, FCR (natives FC-Routing) oder FCIP-Erweiterungen werden von der MetroCluster FC-Switch-Fabric nicht unterstützt.
- Die folgenden Brocade FC Switches unterstützen WAN-ISL-Verschlüsselung und -Komprimierung für MetroCluster FC Back-End Fabrics:
  - Brocade G720
  - Brocade G630
  - Brocade G620
  - Brocade 6520
- Die Funktion Brocade Virtual Fabric (VF) wird nicht unterstützt.
- FC-Zoning auf Basis des Domain-Ports wird unterstützt, aber das Zoning auf Basis des weltweiten Namens (WWN) wird nicht unterstützt.

Überprüfen Sie die Lizenzanforderungen von Brocade

Sie benötigen bestimmte Lizenzen für die Switches in einer MetroCluster-Konfiguration. Sie müssen diese Lizenzen auf allen vier Switches installieren.

Über diese Aufgabe

Die MetroCluster-Konfiguration erfüllt die folgenden Anforderungen an die Brocade-Lizenz:

- Trunking-Lizenz für Systeme mit mehr als einer ISL, wie empfohlen.
- Erweiterte Fabric-Lizenz (für ISL-Entfernungen über 6 km)
- Enterprise-Lizenz für Standorte mit mehr als einem ISL und einer ISL-Entfernung von mehr als 6 km

  Die Enterprise-Lizenz umfasst Brocade Network Advisor und alle Lizenzen, mit Ausnahme zusätzlicher Port-Lizenzen.

Schritt

1. Vergewissern Sie sich, dass die Lizenzen installiert sind:

Für Fabric OS 8.2.x und früher

Führen Sie den Befehl aus `licenseshow`.

Für Fabric OS 9.0 und höher

Führen Sie den Befehl aus `license --show`.

Wenn Sie diese Lizenzen nicht besitzen, wenden Sie sich an Ihren Vertriebsmitarbeiter, bevor Sie fortfahren.

Setzen Sie die Brocade FC-Switch-Werte auf die Werkseinstellungen

Sie müssen den Schalter auf die werkseitigen Standardeinstellungen setzen, um eine erfolgreiche Konfiguration zu gewährleisten. Außerdem müssen Sie jedem Switch einen eindeutigen Namen zuweisen.

Über diese Aufgabe

In den Beispielen dieses Verfahrens besteht das Gewebe aus BrocadeSwitchA und BrocadeSwitchB.

Schritte

1. Verbinden Sie die Konsole und melden Sie sich bei beiden Switches in einer Fabric an.
2. Deaktivieren Sie den Switch dauerhaft:

   `switchcfgpersistentdisable`

   Dadurch wird sichergestellt, dass der Schalter nach einem Neustart oder einem Fastboot deaktiviert bleibt. Wenn dieser Befehl nicht verfügbar ist, verwenden Sie den `switchdisable` Befehl.

   Im folgenden Beispiel wird der Befehl auf BrocadeSwitchA angezeigt:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   Im folgenden Beispiel wird der Befehl auf BrocadeSwitchB angezeigt:

   ```
   BrocadeSwitchB:admin> switchcfgpersistentdisable
   ```

3. Den Switch-Namen festlegen:

   `switchname switch_name`

   Die Schalter sollten jeweils einen eindeutigen Namen haben. Nach Festlegen des Namens ändert sich die Eingabeaufforderung entsprechend.

   Im folgenden Beispiel wird der Befehl auf BrocadeSwitchA angezeigt:

   ```
   BrocadeSwitchA:admin> switchname "FC_switch_A_1"
   FC_switch_A_1:admin>
   ```

Im folgenden Beispiel wird der Befehl auf BrocadeSwitchB angezeigt:

```
BrocadeSwitchB:admin> switchname "FC_Switch_B_1"
FC_switch_B_1:admin>
```

4. Legen Sie für alle Ports die Standardwerte fest:

   `portcfgdefault`

   Dies muss für alle Ports auf dem Switch durchgeführt werden.

   Im folgenden Beispiel werden die Befehle an FC_Switch_A_1 angezeigt:

```
FC_switch_A_1:admin> portcfgdefault 0
FC_switch_A_1:admin> portcfgdefault 1
...
FC_switch_A_1:admin> portcfgdefault 39
```

   Im folgenden Beispiel werden die Befehle an FC_Switch_B_1 angezeigt:

```
FC_switch_B_1:admin> portcfgdefault 0
FC_switch_B_1:admin> portcfgdefault 1
...
FC_switch_B_1:admin> portcfgdefault 39
```

5. Löschen Sie die Zoning-Informationen:

   `cfgdisable`

   `cfgclear`

   `cfgsave`

   Im folgenden Beispiel werden die Befehle an FC_Switch_A_1 angezeigt:

```
FC_switch_A_1:admin> cfgdisable
FC_switch_A_1:admin> cfgclear
FC_switch_A_1:admin> cfgsave
```

   Im folgenden Beispiel werden die Befehle an FC_Switch_B_1 angezeigt:

```
FC_switch_B_1:admin> cfgdisable
FC_switch_B_1:admin> cfgclear
FC_switch_B_1:admin> cfgsave
```

6. Legen Sie die allgemeinen Switch-Einstellungen auf Standard fest:

   `configdefault`

   Im folgenden Beispiel wird der Befehl an FC_Switch_A_1 angezeigt:

   ```
   FC_switch_A_1:admin> configdefault
   ```

   Im folgenden Beispiel wird der Befehl an FC_Switch_B_1 angezeigt:

   ```
   FC_switch_B_1:admin> configdefault
   ```

7. Legen Sie für alle Ports den nicht-Trunking-Modus fest:

   `switchcfgtrunk 0`

   Im folgenden Beispiel wird der Befehl an FC_Switch_A_1 angezeigt:

   ```
   FC_switch_A_1:admin> switchcfgtrunk 0
   ```

   Im folgenden Beispiel wird der Befehl an FC_Switch_B_1 angezeigt:

   ```
   FC_switch_B_1:admin> switchcfgtrunk 0
   ```

8. Deaktivieren Sie bei Brocade 6510 Switches die Funktion Brocade Virtual Fabrics (VF):

   `fosconfig options`

   Im folgenden Beispiel wird der Befehl an FC_Switch_A_1 angezeigt:

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   ```

   Im folgenden Beispiel wird der Befehl an FC_Switch_B_1 angezeigt:

   ```
   FC_switch_B_1:admin> fosconfig --disable vf
   ```

9. Löschen Sie die Administrator-Domänenkonfiguration (AD):

Im folgenden Beispiel werden die Befehle an FC_Switch_A_1 angezeigt:

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

Im folgenden Beispiel werden die Befehle an FC_Switch_B_1 angezeigt:

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

10. Starten Sie den Switch neu:

    ```
    reboot
    ```

    Im folgenden Beispiel wird der Befehl an FC_Switch_A_1 angezeigt:

    ```
    FC_switch_A_1:admin> reboot
    ```

    Im folgenden Beispiel wird der Befehl an FC_Switch_B_1 angezeigt:

    ```
    FC_switch_B_1:admin> reboot
    ```

Konfigurieren der grundlegenden Switch-Einstellungen

Für Brocade Switches müssen Sie die globalen Grundeinstellungen, einschließlich der Domänen-ID, konfigurieren.

Über diese Aufgabe

Diese Aufgabe enthält Schritte, die auf jedem Switch an beiden MetroCluster-Standorten ausgeführt werden müssen.

In diesem Verfahren legen Sie die eindeutige Domänen-ID für jeden Switch fest, wie im folgenden Beispiel dargestellt. Im Beispiel bilden die Domänen-IDs 5 und 7 Fabric_1 und die Domänen-IDs 6 und 8 Form Fabric_2.

- FC_Switch_A_1 ist der Domänen-ID 5 zugewiesen
- FC_Switch_A_2 ist der Domänen-ID 6 zugewiesen
- FC_Switch_B_1 ist der Domänen-ID 7 zugewiesen
- FC_Switch_B_2 ist der Domänen-ID 8 zugewiesen

Schritte

1. Konfigurationsmodus aufrufen:

```
configure
```

2. Gehen Sie die Eingabeaufforderungen durch:
   a. Legen Sie die Domänen-ID für den Switch fest.
   b. Drücken Sie als Antwort auf die Eingabeaufforderungen **Enter**, bis Sie auf "RDP-Polling-Zyklus" gelangen, und setzen Sie diesen Wert dann auf `0` So deaktivieren Sie die Abfrage.
   c. Drücken Sie **Enter**, bis Sie zur Switch-Eingabeaufforderung zurückkehren.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = 5
.
.

RSCN Transmission Mode [yes, y, no, no: [no] y

End-device RSCN Transmission Mode
 (0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric
RSCN): (0..2) [1]
Domain RSCN To End-device for switch IP address or name change
 (0 = disabled, 1 = enabled): (0..1) [0] 1

.
.
RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
```

3. Wenn Sie zwei oder mehr ISLs pro Fabric verwenden, können Sie entweder in-Order Delivery (IOD) von Frames oder Out-of-Order (OOD) Lieferung von Frames konfigurieren.

   Die Standard-IOD-Einstellungen werden empfohlen. Sie sollten OOD nur bei Bedarf konfigurieren.

   "Überlegungen bei der Verwendung von TDM/WDM-Geräten mit Fabric-Attached MetroCluster-Konfigurationen"

   a. Zur Konfiguration von IOD der Frames müssen die folgenden Schritte auf jeder Switch-Fabric durchgeführt werden:
      i. IOD aktivieren:

         ```
         iodset
         ```

      ii. Setzen Sie die Advanced Performance Tuning-Richtlinie (APT) auf 1:

         ```
         aptpolicy 1
         ```

      iii. Deaktivieren der DLS (Dynamic Load Sharing):

```
dlsreset
```

iv. Überprüfen Sie die IOD-Einstellungen mithilfe des `iodshow`, `aptpolicy`, und `dlsshow` Befehle.

Geben Sie beispielsweise die folgenden Befehle an FC_Switch_A_1 aus:

```
FC_switch_A_1:admin> iodshow
    IOD is set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 1 0(ap)

    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
         0: AP Shared Link Policy
         1: AP Dedicated Link Policy
    command aptpolicy completed

    FC_switch_A_1:admin> dlsshow
    DLS is not set
```

i. Wiederholen Sie diese Schritte auf der zweiten Switch Fabric.

b. Die folgenden Schritte müssen auf jeder Switch-Fabric ausgeführt werden, um OOD von Frames zu konfigurieren:

i. OOD aktivieren:

```
iodreset
```

ii. Setzen Sie die Advanced Performance Tuning-Richtlinie (APT) auf 3:

```
aptpolicy 3
```

iii. Deaktivieren der DLS (Dynamic Load Sharing):

```
dlsreset
```

iv. Überprüfen Sie die OOD-Einstellungen:

```
iodshow

aptpolicy

dlsshow
```

Geben Sie beispielsweise die folgenden Befehle an FC_Switch_A_1 aus:

```
FC_switch_A_1:admin> iodshow
    IOD is not set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 3 0(ap)
    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
    command aptpolicy completed


    FC_switch_A_1:admin> dlsshow
    DLS is set by default with current routing policy
```

i. Wiederholen Sie diese Schritte auf der zweiten Switch Fabric.

> Bei der Konfiguration von ONTAP auf den Controller-Modulen muss OOD explizit auf jedem Controller-Modul in der MetroCluster-Konfiguration konfiguriert sein.

"Konfigurieren Sie die In-Order-Zustellung oder Out-of-Order-Zustellung von Frames auf der ONTAP -Software"

4. Wenn Sie eine Version vor FOS 9.0 ausführen, überprüfen Sie, ob der Switch die dynamische Port on Demand (POD)-Lizenzierungsmethode verwendet.

> In Fabric OS 9.0 und höher ist die Lizenzmethode standardmäßig dynamisch. Die statische Lizenzmethode wird nicht unterstützt.

a. Führen Sie den Lizenzbefehl aus:

```
licenseport --show
```

```
FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

> Brocade FabricPool Versionen vor 8.0 führen die folgenden Befehle als Administrator und Version 8.0 aus und führen sie später als „root“ aus.

b. Aktivieren Sie den Root-Benutzer.

Wenn der Root-Benutzer bereits von Brocade deaktiviert ist, aktivieren Sie den Root-Benutzer wie im folgenden Beispiel dargestellt:

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

c. Führen Sie den Lizenzbefehl aus:

```
license --show -port
```

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Wenn Sie Fabric OS 8.2.x und eine frühere Version verwenden, müssen Sie die Lizenzmethode in „dynamisch“ ändern:

```
licenseport --method dynamic
```

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

5. Aktivieren Sie Trap für T11-FC-ZONE-SERVER-MIB für die erfolgreiche Integritätsüberwachung der Switches in ONTAP:

   a. Aktivieren Sie die T11-FC-ZONE-SERVER-MIB:

   ```
   snmpconfig --set mibCapability -mib_name T11-FC-ZONE-SERVER-MIB -bitmask
   0x3f
   ```

   b. Aktivieren Sie den T11-FC-ZONE-SERVER-MIB-Trap:

   ```
   snmpconfig --enable mibcapability -mib_name SW-MIB -trap_name
   swZoneConfigChangeTrap
   ```

   c. Wiederholen Sie die vorherigen Schritte auf der zweiten Switch Fabric.

6. **Optional**: Wenn Sie die Community-Zeichenkette auf einen anderen Wert als „öffentlich“ setzen, müssen Sie die ONTAP Health Monitore mit der von Ihnen angegebenen Community-Zeichenfolge konfigurieren:

   a. Vorhandene Community-Zeichenfolge ändern:

   ```
   snmpconfig --set snmpv1
   ```

   b. Drücken Sie **Enter**, bis der Text „Community (ro): [Public]“ angezeigt wird.

   c. Geben Sie die gewünschte Community-Zeichenfolge ein.

   Am FC_Switch_A_1:

```
FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm     <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]    in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_A_1:admin>
```

Am FC_Switch_B_1:

```
FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]     in this example it is set to
"mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_B_1:admin>
```

7. Starten Sie den Switch neu:

   ```
   reboot
   ```

   Am FC_Switch_A_1:

```
FC_switch_A_1:admin> reboot
```

Am FC_Switch_B_1:

```
FC_switch_B_1:admin> reboot
```

8. Dauerhaft aktivieren Sie den Switch:

   `switchcfgpersistentenable`

   Am FC_Switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

   Am FC_Switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgpersistentenable
   ```

Konfigurieren Sie die grundlegenden Switch-Einstellungen auf einem Brocade DCX 8510-8-Switch

Für Brocade Switches müssen Sie die globalen Grundeinstellungen, einschließlich der Domänen-ID, konfigurieren.

Über diese Aufgabe

Sie müssen die einzelnen Schritte auf jedem Switch an beiden MetroCluster Standorten durchführen. In diesem Verfahren legen Sie die Domänen-ID für jeden Switch fest, wie in den folgenden Beispielen dargestellt:

- FC_Switch_A_1 ist der Domänen-ID 5 zugewiesen
- FC_Switch_A_2 ist der Domänen-ID 6 zugewiesen
- FC_Switch_B_1 ist der Domänen-ID 7 zugewiesen
- FC_Switch_B_2 ist der Domänen-ID 8 zugewiesen

Im vorherigen Beispiel bilden die Domänen-IDs 5 und 7 Fabric_1 sowie die Domänen-IDs 6 und 8 Form Fabric_2.

> Mit diesem Verfahren können Sie die Switches auch konfigurieren, wenn Sie nur einen DCX 8510-8-Switch pro Standort verwenden.

Mit diesem Verfahren sollten Sie auf jedem Brocade DCX 8510-8 Switch zwei logische Switches erstellen. Die beiden logischen Switches, die auf beiden Brocade DCX8510-8 Switches erstellt wurden, bilden wie in den folgenden Beispielen dargestellt zwei logische Fabrics:

- LOGISCHE STRUKTUR 1: Switch 1/Blade1 und Switch 2 Blade 1
- LOGISCHES GEWEBE 2: Switch1/Blade2 und Switch 2 Blade 2

Schritte

1. Wechseln Sie in den Befehlsmodus:

   `configure`

2. Gehen Sie die Eingabeaufforderungen durch:
   a. Legen Sie die Domänen-ID für den Switch fest.
   b. Wählen Sie weiter **Enter**, bis Sie auf "RDP-Polling Cycle" gelangen, und setzen Sie dann den Wert auf `0` So deaktivieren Sie die Abfrage.
   c. Wählen Sie **Enter**, bis Sie zur Switch-Eingabeaufforderung zurückkehren.

   ```
   FC_switch_A_1:admin> configure
   Fabric parameters = y
   Domain_id = `5


   RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
   `
   ```

3. Wiederholen Sie diese Schritte bei allen Schaltern in Fabric_1 und Fabric_2.
4. Konfigurieren Sie die virtuellen Fabrics.
   a. Aktivieren Sie virtuelle Fabrics auf dem Switch:

      `fosconfig --enablevf`

   b. Konfigurieren Sie das System so, dass es auf allen logischen Switches dieselbe Basiskonfiguration verwendet:

      `configurechassis`

      Das folgende Beispiel zeigt die Ausgabe für das `configurechassis` Befehl:

   ```
   System (yes, y, no, n): [no] n
   cfgload attributes (yes, y, no, n): [no] n
   Custom attributes (yes, y, no, n): [no] y
   Config Index (0 to ignore): (0..1000) [3]:
   ```

5. Logischen Switch erstellen und konfigurieren:

   `scfg --create fabricID`

6. Fügen Sie alle Ports von einem Blade zur virtuellen Fabric hinzu:

   `lscfg --config fabricID -slot slot -port lowest-port - highest-port`

Die Blades bilden eine logische Struktur (z.B. Switch 1 Blade 1 und Switch 3 Blade 1) müssen dieselbe Fabric-ID haben.

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

Verwandte Informationen

"Anforderungen für die Verwendung eines Brocade DCX 8510-8 Switches"

Konfigurieren Sie E-Ports auf Brocade FC-Switches mithilfe von FC-Ports

Für Brocade Switches, auf denen die Inter-Switch-Links (ISL) über FC-Ports konfiguriert sind, müssen Sie die Switch-Ports an jedem Switch-Fabric mit ISL konfigurieren. Diese ISL-Ports werden auch als E-Ports bezeichnet.

Bevor Sie beginnen

- Alle ISLs in einer FC Switch Fabric müssen mit derselben Geschwindigkeit und Entfernung konfiguriert sein.
- Die Kombination aus Switch-Port und Small Form-Factor Pluggable (SFP) muss die Geschwindigkeit unterstützen.
- Die unterstützte ISL-Entfernung hängt vom FC-Switch-Modell ab.

  "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.

- Der ISL-Link muss über eine dedizierte Lambda verfügen, und der Link muss von Brocade für die Entfernung, den Switch-Typ und das Fabric-Betriebssystem (FOS) unterstützt werden.

Über diese Aufgabe

Sie dürfen die L0-Einstellung nicht verwenden, wenn Sie die ausgeben `portCfgLongDistance` Befehl. Stattdessen sollten Sie die EINSTELLUNG LE oder LS verwenden, um die Entfernung auf den Brocade-Switches mit einer Mindestentfernungsstufe VON LE zu konfigurieren.

Sie dürfen die LD-Einstellung nicht verwenden, wenn Sie die ausgeben `portCfgLongDistance` Befehl beim Arbeiten mit xWDM/TDM-Geräten. Verwenden Sie stattdessen die EINSTELLUNG LE oder LS, um die Entfernung der Brocade-Switches zu konfigurieren.

Diese Aufgabe müssen Sie für jede FC-Switch-Fabric durchführen.

In den folgenden Tabellen werden die ISL-Ports für verschiedene Switches und verschiedene ISLs in einer Konfiguration mit ONTAP 9.1 oder 9.2 angezeigt. Die in diesem Abschnitt gezeigten Beispiele gelten für einen

Brocade 6505-Switch. Sie sollten die Beispiele ändern, um Ports zu verwenden, die für den Switch-Typ gelten.

Sie müssen die erforderliche Anzahl von ISLs für Ihre Konfiguration verwenden.

Switch-Modell	ISL-Port	Switch-Port
Brocade 6520	ISL-Port 1	23
	ISL-Port 2	47
	ISL-Port 3	71
	ISL-Port 4	95
Brocade 6505	ISL-Port 1	20
	ISL-Port 2	21
	ISL-Port 3	22
	ISL-Port 4	23
Brocade 6510 und Brocade DCX 8510-8	ISL-Port 1	40
	ISL-Port 2	41
	ISL-Port 3	42
	ISL-Port 4	43
	ISL-Port 5	44
	ISL-Port 6	45
	ISL-Port 7	46
	ISL-Port 8	47
Brocade 7810	ISL-Port 1	ge2 (10 Gbit/s)
	ISL-Port 2	ge3 (10 Gbit/s)
	ISL-Port 3	ge4 (10 Gbit/s)
	ISL-Port 4	Ge5 (10 Gbit/s)
	ISL-Port 5	ge6 (10 Gbit/s)
	ISL-Port 6	Ge7 (10 Gbit/s)
Brocade 7840 **Hinweis:** der Brocade 7840 Switch unterstützt entweder zwei VE-Ports mit 40 Gbit/s oder bis zu vier VE-Ports mit 10 Gbit/s pro Switch zur Erstellung von FCIP-ISLs.	ISL-Port 1	ge0 (40 Gbit/s) oder ge2 (10 Gbit/s)
	ISL-Port 2	ge1 (40 Gbit/s) oder ge3 (10 Gbit/s)
	ISL-Port 3	ge10 (10 Gbit/s)
	ISL-Port 4	Ge11 (10 Gbit/s)

Brocade G610, G710	ISL-Port 1	20
	ISL-Port 2	21
	ISL-Port 3	22
	ISL-Port 4	23
BROCADE G620, G620-1, G630, G630-1, G720	ISL-Port 1	40
	ISL-Port 2	41
	ISL-Port 3	42
	ISL-Port 4	43
	ISL-Port 5	44
	ISL-Port 6	45
	ISL-Port 7	46

Schritte

1. Konfigurieren der Portgeschwindigkeit:

   `portcfgspeed port-numberspeed`

   Sie müssen die höchste gemeinsame Geschwindigkeit verwenden, die von den Komponenten im Pfad unterstützt wird.

   Im folgenden Beispiel sind zwei ISLs für jede Fabric verfügbar:

   ```
   FC_switch_A_1:admin> portcfgspeed 20 16
   FC_switch_A_1:admin> portcfgspeed 21 16

   FC_switch_B_1:admin> portcfgspeed 20 16
   FC_switch_B_1:admin> portcfgspeed 21 16
   ```

2. Konfigurieren Sie den Trunking-Modus für jede ISL:

   `portcfgtrunkport port-number`

   - Wenn Sie die ISLs für Trunking (IOD) konfigurieren, stellen Sie die Port-numberport-Nummer von portcfgTrunk auf 1 ein, wie im folgenden Beispiel dargestellt:

```
FC_switch_A_1:admin> portcfgtrunkport 20 1
FC_switch_A_1:admin> portcfgtrunkport 21 1
FC_switch_B_1:admin> portcfgtrunkport 20 1
FC_switch_B_1:admin> portcfgtrunkport 21 1
```

- Wenn Sie die ISL for Trunking (OOD) nicht konfigurieren möchten, setzen Sie die Portcfgtrunkport-Nummer auf 0, wie im folgenden Beispiel dargestellt:

```
FC_switch_A_1:admin> portcfgtrunkport 20 0
FC_switch_A_1:admin> portcfgtrunkport 21 0
FC_switch_B_1:admin> portcfgtrunkport 20 0
FC_switch_B_1:admin> portcfgtrunkport 21 0
```

3. QoS-Datenverkehr für jeden ISL-Port aktivieren:

   `portcfgqos --enable port-number`

   Im folgenden Beispiel gibt es zwei ISLs pro Switch Fabric:

```
FC_switch_A_1:admin> portcfgqos --enable 20
FC_switch_A_1:admin> portcfgqos --enable 21

FC_switch_B_1:admin> portcfgqos --enable 20
FC_switch_B_1:admin> portcfgqos --enable 21
```

4. Überprüfen Sie die Einstellungen:

   `portCfgShow command`

   Das folgende Beispiel zeigt die Ausgabe für eine Konfiguration, die zwei mit Port 20 und Port 21 verkabelte ISLs verwendet. Die Einstellung für den Trunk-Port sollte FÜR IOD und OOD AUS aktiviert sein:

```
Ports of Slot 0   12  13   14 15    16  17  18  19   20  21 22  23    24
25  26  27
----------------+---+---+---+---+-----+---+---+---+----+---+---+---+
-----+---+---+---
Speed             AN  AN  AN  AN    AN  AN  8G  AN   AN  AN  16G  16G
AN  AN  AN  AN
Fill Word         0   0   0   0     0   0   3   0    0   0   3   3     3
0   0   0
AL_PA Offset 13   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Trunk Port        ..  ..  ..  ..    ..  ..  ..  ..   ON  ON  ..  ..
..  ..  ..  ..
```

```
Long Distance     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
VC Link Init      ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked L_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked G_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Disabled E_Port   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Locked E_Port     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
ISL R_RDY Mode    ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
RSCN Suppressed   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Persistent Disable..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
LOS TOV enable    ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
NPIV capability   ON  ON  ON  ON    ON  ON  ON  ON   ON  ON  ON  ON
ON  ON  ON  ON
NPIV PP Limit    126 126 126 126   126 126 126 126  126 126 126 126
126 126 126 126
QOS E_Port        AE  AE  AE  AE    AE  AE  AE  AE   AE  AE  AE  AE
AE  AE  AE  AE
Mirror Port       ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Rate Limit        ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Credit Recovery   ON  ON  ON  ON    ON  ON  ON  ON   ON  ON  ON  ON
ON  ON  ON  ON
Fport Buffers     ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Port Auto Disable ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
CSCTL mode        ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..

Fault Delay       0  0  0  0    0  0  0  0   0  0  0  0    0  0  0  0
```

5. Berechnen der ISL-Entfernung.

   Aufgrund des Verhaltens von FC-VI muss die Entfernung auf das 1.5-fache der realen Entfernung mit einer Mindestentfernung von 10 km (über DIE LE-Entfernungsebene) eingestellt werden.

   Der Abstand für die ISL wird wie folgt berechnet, gerundet auf den nächsten vollen Kilometer:

1.5 × Real_distance = Entfernung

Wenn die Entfernung 3 km beträgt, dann 1.5 × 3 km = 4.5 km Dies ist weniger als 10 km, daher muss die ISL auf DIE LE-Distanzebene eingestellt werden.

Wenn die Entfernung 20 km beträgt, dann 1.5 × 20 km = 30 km Die ISL muss auf 30 km eingestellt sein und die LS-Abstandsebene verwenden.

6. Legen Sie die Entfernung an jedem ISL-Port fest:

   `portcfglongdistance portdistance-level vc_link_init distance`

   A `vc_link_init` Der Wert von `1` Verwendet das ARB-Füllwort (Standard). Der Wert von `0` Nutzt DEN LEERLAUF. Der erforderliche Wert hängt von der verwendeten Verbindung ab. Für jeden ISL-Port müssen die Befehle wiederholt werden.

   Bei einer ISL-Entfernung von 3 km, wie im Beispiel im vorherigen Schritt angegeben, beträgt die Einstellung 4.5 km mit der Standardeinstellung `vc_link_init` Der Wert von `1`. Da die Einstellung von 4.5 km weniger als 10 km beträgt, muss der Hafen auf DIE LE-Distanzebene eingestellt werden:

   ```
   FC_switch_A_1:admin> portcfglongdistance 20 LE 1

   FC_switch_B_1:admin> portcfglongdistance 20 LE 1
   ```

   Bei einer ISL-Entfernung von 20 km, wie im Beispiel im vorherigen Schritt angegeben, beträgt die Einstellung 30 km mit dem Standardwert vc_Link_init `1`:

   ```
   FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30

   FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30
   ```

7. Überprüfen Sie die Distanzeinstellung:

   `portbuffershow`

   Eine Entfernung von LE erscheint als 10 km

   Das folgende Beispiel zeigt die Ausgabe für eine Konfiguration, die ISLs an Port 20 und Port 21 verwendet:

```
FC_switch_A_1:admin> portbuffershow

User  Port     Lx      Max/Resv    Buffer Needed    Link      Remaining
Port  Type    Mode     Buffers     Usage  Buffers   Distance  Buffers
----  ----    ----     -------     ------ -------   --------- ---------
...
 20     E      -          8         67      67       30km
 21     E      -          8         67      67       30km
...
 23            -          8          0      -        -        466
```

8. Vergewissern Sie sich, dass beide Switches eine Struktur bilden:

   ```
   switchshow
   ```

   Das folgende Beispiel zeigt die Ausgabe für eine Konfiguration, die ISLs an Port 20 und Port 21 verwendet:

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==========================================
...
20   20  010C00   id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port, master
is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       7
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State Proto
==============================================
...
20   20  030C00   id    16G  Online  FC  LE E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)(Trunk master)
21   21  030D00   id    16G  Online  FC  LE E-Port  (Trunk port, master
is Port 20)
...
```

9. Bestätigen Sie die Konfiguration der Fabrics:

```
fabricshow
```

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

```
FC_switch_B_1:admin> fabricshow
   Switch ID   Worldwide Name     Enet IP Addr FC IP Addr   Name
-------------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"

3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1
```

10. Bestätigen Sie das Trunking der ISLs:

    `trunkshow`

    - Wenn Sie die ISLs für Trunking (IOD) konfigurieren, sollte die Ausgabe ähnlich wie die folgenden angezeigt werden:

      ```
      FC_switch_A_1:admin> trunkshow
       1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
          21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
       FC_switch_B_1:admin> trunkshow
       1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
          21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16
      ```

    - Wenn Sie die ISLs für Trunking (OOD) nicht konfigurieren, sollte die Ausgabe ähnlich wie die folgenden angezeigt werden:

      ```
      FC_switch_A_1:admin> trunkshow
       1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
       2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER
      FC_switch_B_1:admin> trunkshow
       1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
       2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER
      ```

11. Wiederholen Schritt 1 Bis Schritt 10 Für das zweite FC Switch Fabric.

Verwandte Informationen

"Portzuweisungen für FC-Switches"

Konfigurieren von 10 Gbps VE-Ports an Brocade FC 7840-Switches

Wenn Sie die 10-Gbit/s-VE-Ports (die FCIP verwenden) für ISLs verwenden, müssen Sie an jedem Port IP-Schnittstellen erstellen und FCIP-Tunnel und -Leitungen in jedem Tunnel konfigurieren.

Über diese Aufgabe

Dieses Verfahren muss an jeder Switch-Fabric in der MetroCluster Konfiguration durchgeführt werden.

Die Beispiele in diesem Verfahren gehen davon aus, dass die beiden Brocade 7840-Switches die folgenden IP-Adressen haben:

- FC_Switch_A_1 ist lokal.
- FC_Switch_B_1 ist Remote.

Schritte

1. IP-Schnittstellenadressen für die 10-Gbit/s-Ports auf beiden Switches in der Fabric erstellen:

   ```
   portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_IP_address
   netmask netmask_number vlan 2 mtu auto
   ```

   Mit dem folgenden Befehl werden ipif-Adressen an den Ports ge2.dp0 und ge3.dp0 von FC_Switch_A_1 erstellt:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   Mit dem folgenden Befehl werden ipif-Adressen an den Ports ge2.dp0 und ge3.dp0 von FC_Switch_B_1 erstellt:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

2. Überprüfen Sie, ob die ipif-Adressen auf beiden Switches erfolgreich erstellt wurden:

   ```
   portshow ipif all
   ```

   Mit dem folgenden Befehl werden die ipif-Adressen auf Switch FC_Switch_A_1 angezeigt:

```
FC_switch_A_1:root> portshow ipif all

 Port         IP Address                    / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.71                   / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.71                   / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

Mit dem folgenden Befehl werden die ipif-Adressen auf Switch FC_Switch_B_1 angezeigt:

```
FC_switch_B_1:root> portshow ipif all

 Port         IP Address                    / Pfx  MTU   VLAN  Flags
-------------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.72                   / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.72                   / 20   AUTO  2     U R M I
-------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. Erstellen Sie den ersten der beiden FCIP-Tunnel unter Verwendung der Ports auf dp0:

   `portcfg fciptunnel`

   Mit diesem Befehl wird ein Tunnel mit einer einzigen Schaltung erstellt.

   Mit dem folgenden Befehl wird der Tunnel auf Switch FC_Switch_A_1 erstellt:

```
portcfg fciptunnel 24 create -S 10.10.20.71  -D 10.10.20.72 -b 10000000
-B 10000000
```

   Mit dem folgenden Befehl wird der Tunnel auf Switch FC_Switch_B_1 erstellt:

```
portcfg fciptunnel 24 create -S 10.10.20.72  -D 10.10.20.71 -b 10000000
-B 10000000
```

4. Überprüfen Sie, ob die FCIP-Tunnel erfolgreich erstellt wurden:

   ```
   portshow fciptunnel all
   ```

   Das folgende Beispiel zeigt, dass die Tunnel erstellt wurden und die Stromkreise aktiv sind:

   ```
   FC_switch_B_1:root>

    Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
   CommRt Met/G
   ------------------------------------------------------------------------
   --------
    24    -         Up      ---------     2d8m    0.05    0.41   3      -
   -
   ------------------------------------------------------------------------
   --------
    Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
   r=ReservedBW
                    a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                    I=IP-Ext
   ```

5. Erstellen Sie einen zusätzlichen Stromkreis für dp0.

   Mit dem folgenden Befehl wird ein Schaltkreis auf Switch FC_Switch_A_1 für dp0 erzeugt:

   ```
   portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72  --min
   -comm-rate 5000000 --max-comm-rate 5000000
   ```

   Mit dem folgenden Befehl wird ein Schaltkreis auf Schalter FC_Switch_B_1 für dp0 erzeugt:

   ```
   portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71  --min
   -comm-rate 5000000 --max-comm-rate 5000000
   ```

6. Vergewissern Sie sich, dass alle Stromkreise erfolgreich erstellt wurden:

   ```
   portshow fcipcircuit all
   ```

   Mit dem folgenden Befehl werden die Schaltkreise und deren Status angezeigt:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
-------------------------------------------------------------------------
--------
 24    0 ge2     Up      ---va---4    2d12m    0.02    0.03   3
10000/10000 0/-
 24    1 ge3     Up      ---va---4    2d12m    0.02    0.04   3
10000/10000 0/-
-------------------------------------------------------------------------
--------
 Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                  ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
```

Konfigurieren Sie 40-Gbit/s-VE-Ports auf Brocade 7810- und 7840-FC-Switches

Wenn Sie die zwei 40-GbE-VE-Ports (die FCIP verwenden) für ISLs verwenden, müssen Sie an jedem Port IP-Schnittstellen erstellen und FCIP-Tunnel und -Leitungen in jedem Tunnel konfigurieren.

Über diese Aufgabe

Dieses Verfahren muss an jeder Switch-Fabric in der MetroCluster Konfiguration durchgeführt werden.

Die Beispiele in diesem Verfahren verwenden zwei Schalter:

- FC_Switch_A_1 ist lokal.
- FC_Switch_B_1 ist Remote.

Schritte

1. IP-Schnittstellenadressen für die 40-Gbit/s-Ports auf beiden Switches in der Fabric erstellen:

   ```
   portcfg ipif FC_switch_namefirst_port_name create FC_switch_IP_address netmask
   netmask_number vlan 2 mtu auto
   ```

   Mit dem folgenden Befehl werden ipif-Adressen an den Ports ge0.dp0 und ge1.dp0 von FC_Switch_A_1 erstellt:

   ```
   portcfg ipif  ge0.dp0 create  10.10.82.10 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge1.dp0 create  10.10.82.11 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   Mit dem folgenden Befehl werden ipif-Adressen an den Ports ge0.dp0 und ge1.dp0 von FC_Switch_B_1 erstellt:

```
portcfg ipif  ge0.dp0 create  10.10.83.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif  ge1.dp0 create  10.10.83.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. Überprüfen Sie, ob die ipif-Adressen auf beiden Switches erfolgreich erstellt wurden:

   ```
   portshow ipif all
   ```

   Im folgenden Beispiel werden die IP-Schnittstellen an FC_Switch_A_1 angezeigt:

   ```
   Port         IP Address                     / Pfx  MTU   VLAN  Flags
   ---------------------------------------------------------------------------
   ---
   -----
    ge0.dp0      10.10.82.10                    / 16   AUTO  2     U R M
    ge1.dp0      10.10.82.11                    / 16   AUTO  2     U R M
   ---------------------------------------------------------------------------
   --------
   Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
   I=InUse
          N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
   ```

   Im folgenden Beispiel werden die IP-Schnittstellen an FC_Switch_B_1 angezeigt:

   ```
   Port         IP Address                     / Pfx  MTU   VLAN  Flags
   ---------------------------------------------------------------------------
   --------
    ge0.dp0      10.10.83.10                    / 16   AUTO  2     U R M
    ge1.dp0      10.10.83.11                    / 16   AUTO  2     U R M
   ---------------------------------------------------------------------------
   --------
   Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
   I=InUse
          N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
   ```

3. Erstellen Sie den FCIP-Tunnel an beiden Switches:

   ```
   portcfig fciptunnel
   ```

   Mit dem folgenden Befehl wird der Tunnel auf FC_Switch_A_1 erstellt:

```
portcfg fciptunnel 24 create -S 10.10.82.10  -D 10.10.83.10 -b 10000000
-B 10000000
```

Mit dem folgenden Befehl wird der Tunnel auf FC_Switch_B_1 erstellt:

```
portcfg fciptunnel 24 create -S 10.10.83.10  -D 10.10.82.10 -b 10000000
-B 10000000
```

4. Überprüfen Sie, ob der FCIP-Tunnel erfolgreich erstellt wurde:

   ```
   portshow fciptunnel all
   ```

   Das folgende Beispiel zeigt, dass der Tunnel erstellt wurde und die Stromkreise aktiv sind:

   ```
   FC_switch_A_1:root>

    Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
   CommRt Met/G
   ---------------------------------------------------------------------
   --------
    24    -         Up      ---------     2d8m    0.05    0.41   3      -
   -
    ---------------------------------------------------------------------
   ---------
    Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
   r=ReservedBW
                    a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                    I=IP-Ext
   ```

5. Erstellen Sie einen zusätzlichen Stromkreis an jedem Schalter:

   ```
   portcfg fcipcircuit 24 create 1 -S source-IP-address -D destination-IP-address
   --min-comm-rate 10000000 --max-comm-rate 10000000
   ```

   Mit dem folgenden Befehl wird ein Schaltkreis auf Switch FC_Switch_A_1 für dp0 erzeugt:

   ```
   portcfg fcipcircuit 24  create 1 -S 10.10.82.11 -D 10.10.83.11  --min
   -comm-rate 10000000 --max-comm-rate 10000000
   ```

   Mit dem folgenden Befehl wird ein Schaltkreis am Schalter FC_Switch_B_1 für dp1 erzeugt:

```
portcfg fcipcircuit 24 create 1  -S 10.10.83.11 -D 10.10.82.11  --min
-comm-rate 10000000 --max-comm-rate 10000000
```

6. Vergewissern Sie sich, dass alle Stromkreise erfolgreich erstellt wurden:

   ```
   portshow fcipcircuit all
   ```

   Im folgenden Beispiel werden die Schaltkreise aufgeführt und der OpStatus angezeigt:

   ```
   FC_switch_A_1:root> portshow fcipcircuit all

    Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
   CommRt Met/G
   ---------------------------------------------------------------------
   --------
    24    0 ge0     Up      ---va---4    2d12m    0.02    0.03   3
   10000/10000 0/-
    24    1 ge1     Up      ---va---4    2d12m    0.02    0.04   3
   10000/10000 0/-
    ---------------------------------------------------------------------
   ---------
    Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
   6=IPv6
                    ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
   ```

Konfigurieren Sie die Nicht-E-Ports auf dem Brocade -Switch

Sie müssen die nicht-E-Ports auf dem FC-Switch konfigurieren. In einer MetroCluster-Konfiguration sind dies die Ports, die den Switch mit den HBA-Initiatoren, FC-VI-Interconnects und FC-to-SAS-Bridges verbinden. Diese Schritte müssen für jeden Port durchgeführt werden.

Über diese Aufgabe

Im folgenden Beispiel verbinden die Ports eine FC-to-SAS-Bridge:

- Port 6 auf FC_FC_Switch_A_1 an Site_A
- Port 6 auf FC_FC_Switch_B_1 an Standort_B

Schritte

1. Konfigurieren Sie die Portgeschwindigkeit für jeden nicht-E-Port:

   ```
   portcfgspeed portspeed
   ```

   Sie sollten die höchste allgemeine Geschwindigkeit verwenden, die von allen Komponenten im Datenpfad unterstützt wird: Dem SFP, dem Switch-Port, auf dem der SFP installiert ist, und dem angeschlossenen Gerät (HBA, Bridge usw.).

   Für die Komponenten werden u. U. die folgenden unterstützten Geschwindigkeiten unterstützt:

- Das SFP-Modul kann 4, 8 oder 16 GB betragen.
- Der Switch-Port kann 4, 8 oder 16 GB betragen.
- Die maximale Geschwindigkeit des angeschlossenen HBA beträgt 16 GB. Die höchste übliche Geschwindigkeit in diesem Fall ist 16 GB, daher sollte der Port für eine Geschwindigkeit von 16 GB konfiguriert werden.

```
FC_switch_A_1:admin> portcfgspeed 6 16

FC_switch_B_1:admin> portcfgspeed 6 16
```

2. Überprüfen Sie die Einstellungen:

   `portcfgshow`

   ```
   FC_switch_A_1:admin> portcfgshow

   FC_switch_B_1:admin> portcfgshow
   ```

   In der Beispielausgabe hat Port 6 die folgenden Einstellungen; die Geschwindigkeit ist auf 16G festgelegt:

```
Ports of Slot 0                      0   1   2   3   4   5   6   7   8
-------------------------------------+---+---+---+--+---+---+---+---+--
Speed                                16G 16G 16G 16G 16G 16G 16G 16G 16G
AL_PA Offset 13                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Trunk Port                           ..  ..  ..  ..  ..  ..  ..  ..  ..
Long Distance                        ..  ..  ..  ..  ..  ..  ..  ..  ..
VC Link Init                         ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked L_Port                        -   -   -   -   -  -   -   -   -
Locked G_Port                        ..  ..  ..  ..  ..  ..  ..  ..  ..
Disabled E_Port                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked E_Port                        ..  ..  ..  ..  ..  ..  ..  ..  ..
ISL R_RDY Mode                       ..  ..  ..  ..  ..  ..  ..  .. ..
RSCN Suppressed                      ..  ..  ..  ..  ..  ..  ..  .. ..
Persistent Disable                   ..  ..  ..  ..  ..  ..  ..  .. ..
LOS TOV enable                       ..  ..  ..  ..  ..  ..  ..  .. ..
NPIV capability                      ON  ON  ON  ON  ON  ON  ON  ON  ON
NPIV PP Limit                        126 126 126 126 126 126 126 126 126
QOS Port                             AE  AE  AE  AE  AE  AE  AE  AE  ON
EX Port                              ..  ..  ..  ..  ..  ..  ..  ..  ..
Mirror Port                          ..  ..  ..  ..  ..  ..  ..  ..  ..
Rate Limit                           ..  ..  ..  ..  ..  ..  ..  ..  ..
Credit Recovery                      ON  ON  ON  ON  ON  ON  ON  ON  ON
Fport Buffers                        ..  ..  ..  ..  ..  ..  ..  ..  ..
Eport Credits                        ..  ..  ..  ..  ..  ..  ..  ..  ..
Port Auto Disable                    ..  ..  ..  ..  ..  ..  ..  ..  ..
CSCTL mode                           ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port mode                          ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port over DWDM                     ..  ..  ..  ..  ..  ..  ..  ..  ..
FEC                                  ON  ON  ON  ON  ON  ON  ON  ON  ON
Fault Delay                          0   0   0   0   0   0   0   0   0
Non-DFE                              ..  ..  ..  ..  ..  ..  ..  ..  ..
```

Konfigurieren der Komprimierung auf ISL-Ports auf einem Brocade G620-Switch

Wenn Sie Brocade G620 Switches verwenden und die Komprimierung für die ISLs aktivieren, müssen Sie diese an jedem E-Port der Switches konfigurieren.

Über diese Aufgabe

Diese Aufgabe muss an den ISL-Ports beider Switches mit ISL ausgeführt werden.

Schritte

1. Deaktivieren Sie den Port, auf dem die Komprimierung konfiguriert werden soll:

   ```
   portdisable port-id
   ```

2. Aktivieren Sie die Komprimierung am Port:

```
portCfgCompress --enable port-id
```

3. Aktivieren Sie den Port, um die Konfiguration mit Komprimierung zu aktivieren:

```
portenable port-id
```

4. Bestätigen Sie, dass die Einstellung geändert wurde:

```
portcfgshow port-id
```

Im folgenden Beispiel wird die Komprimierung für Port 0 aktiviert.

```
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

Mit dem Befehl islShow können Sie überprüfen, ob der E_Port mit konfigurierter und aktiver Verschlüsselung oder Komprimierung online geschaltet wurde.

```
FC_switch_A_1:admin> islshow
  1: 0-> 0 10:00:c4:f5:7c:8b:29:86   5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

Mit dem Befehl portEncCompShow können Sie feststellen, welche Ports aktiv sind. In diesem Beispiel sehen Sie, dass Verschlüsselung und Komprimierung für Port 0 konfiguriert und aktiv sind.

```
FC_switch_A_1:admin> portenccompshow
User      Encryption                  Compression           Config
Port   Configured    Active   Configured   Active  Speed
----   ----------    -------  ----------   ------  -----
  0    Yes            Yes        Yes             Yes        16G
```

Konfigurieren Sie Zoning auf Brocade FC-Switches

Sie müssen die Switch-Ports separaten Zonen zuweisen, sodass der Controller- und Storage-Datenverkehr voneinander getrennt ist.

Zonen für FC-VI-Ports einrichten

Sie müssen für jede DR-Gruppe in der MetroCluster zwei Zonen für die FC-VI-Verbindungen konfigurieren, die den Controller-zu-Controller-Datenverkehr ermöglichen. Diese Zonen enthalten die FC-Switch-Ports, die mit den FC-VI-Ports des Controller-Moduls verbunden sind. Diese Zonen sind Quality of Service (QoS)-Zonen.

Ein QoS-Zonenname beginnt mit dem Präfix QOSHid_, gefolgt von einem benutzerdefinierten String, um ihn von einer regulären Zone zu unterscheiden. Diese QoS-Zonen sind unabhängig vom verwendeten Modell der FibreBridge Bridge identisch.

Jede Zone enthält alle FC-VI-Ports, einen für jedes FC-VI-Kabel von jedem Controller. Diese Zonen werden für eine hohe Priorität konfiguriert.

In den folgenden Tabellen werden die FC-VI-Zonen für zwei DR-Gruppen angezeigt.

DR-Gruppe 1 : QOSH1 FC-VI-Zone für FC-VI-Port A / c

FC Switch	Standort	Switch-Domäne	6505 / 6510 Anschlüsse	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	0	0	0	Controller_A_1-Port FC-VI A
FC_Switch_A_1	A	5	1	1	1	Controller_A_1-Port FC-VI c
FC_Switch_A_1	A	5	4	4	4	Controller_A_2-Port FC-VI A
FC_Switch_A_1	A	5	5	5	5	Controller_A_2-Port FC-VI c
FC_Switch_B_1	B	7	0	0	0	Controller_B_1-Port FC-VI A
FC_Switch_B_1	B	7	1	1	1	Controller_B_1-Port FC-VI c
FC_Switch_B_1	B	7	4	4	4	Controller_B_2-Port FC-VI A
FC_Switch_B_1	B	7	5	5	5	Controller_B_2-Port FC-VI c

Zone in Fabric_1	Mitgliedsports
QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5

DR-Gruppe 1 : QOSH1 FC-VI-Zone für FC-VI-Port b / d

FC Switch	Standort	Switch-Domäne	6505 / 6510 Anschlüsse	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	0	0	0	Controller_A_1-Port FC-VI b
			1	1	1	Controller_A_1-Port FC-VI D
			4	4	4	Controller_A_2-Port FC-VI b
			5	5	5	Controller_A_2-Port FC-VI D
FC_Switch_B_2	B	8	0	0	0	Controller_B_1-Port FC-VI b
			1	1	1	Controller_B_1-Port FC-VI D
			4	4	4	Controller_B_2-Port FC-VI b
			5	5	5	Controller_B_2-Port FC-VI D

Zone in Fabric_1	Mitgliedsports
QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5

DR-Gruppe 2 : QOSH2 FC-VI-Zone für FC-VI-Port A / c

FC Switch	Standort	Switch-Domäne	Switch-Port			Verbindung wird hergestellt mit…
			6510	6520	G620	
FC_Switch_A_1	A	5	24	48	18	Controller_A_3-Port FC-VI A
			25	49	19	Controller_A_3-Port FC-VI c
			28	52	22	Controller_A_4-Port FC-VI A
			29	53	23	Controller_A_4-Port FC-VI c

FC Switch	Standort	Switch-Domäne	Switch-Port			Verbindung wird hergestellt mit…
FC_Switch_B_1	B	7	24	48	18	Controller_B_3-Port FC-VI A
			25	49	19	Controller_B_3-Port FC-VI c
			28	52	22	Controller_B_4-Port FC-VI A
			29	53	23	Controller_B_4-Port FC-VI c

Zone in Fabric_1	Mitgliedsports
QOSH2_MC2_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
QOSH2_MC2_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

DR-Gruppe 2 : QOSH2 FC-VI-Zone für FC-VI-Port b / d

FC Switch	Standort	Switch-Domäne	6510 Anschlüsse	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	24	48	18	Controller_A_3-Port FC-VI b
FC_Switch_A_2	A	6	25	49	19	Controller_A_3-Port FC-VI D
FC_Switch_A_2	A	6	28	52	22	Controller_A_4-Port FC-VI b
FC_Switch_A_2	A	6	29	53	23	Controller_A_4-Port FC-VI D
FC_Switch_B_2	B	8	24	48	18	Controller_B_3-Port FC-VI b
FC_Switch_B_2	B	8	25	49	19	Controller_B_3-Port FC-VI D
FC_Switch_B_2	B	8	28	52	22	Controller_B_4-Port FC-VI b
FC_Switch_B_2	B	8	29	53	23	Controller_B_4-Port FC-VI D

Zone in Fabric_2	Mitgliedsports
QOSH2_MC2_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
QOSH2_MC2_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

Die folgende Tabelle enthält eine Zusammenfassung der FC-VI-Zonen:

Fabric	Zonenname	Mitgliedsports
FC_Switch_A_1 und FC_Switch_B_1	QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
	QOSH2_MC1_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28; 7,29
	QOSH2_MC1_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52; 7,53
FC_Switch_A_2 und FC_Switch_B_2	QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
	QOSH2_MC1_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28; 8,29
	QOSH2_MC1_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52; 8,53

Zone FibreBridge 7500N- oder 7600N-Brücken mit einem FC-Port

Wenn Sie FibreBridge 7500N- oder 7600N-Bridges verwenden, die nur einen der beiden FC-Ports verwenden, müssen Sie Storage-Zonen für die Bridge-Ports erstellen. Sie sollten die Zonen und die zugehörigen Ports verstehen, bevor Sie die Zonen konfigurieren.

Die Beispiele zeigen nur das Zoning für DR-Gruppe 1. Wenn die Konfiguration eine zweite DR-Gruppe umfasst, konfigurieren Sie das Zoning für die zweite DR-Gruppe auf dieselbe Weise unter Verwendung der entsprechenden Ports der Controller und Bridges.

Erforderliche Zonen

Sie müssen eine Zone für jede der FC-to-SAS-Bridge-FC-Ports konfigurieren, die den Datenverkehr zwischen Initiatoren auf jedem Controller-Modul und diese FC-to-SAS-Bridge zulässt.

Jede Speicherzone enthält neun Ports:

- Acht HBA-Initiator-Ports (zwei Verbindungen pro Controller)
- Ein Port mit einer FC-to-SAS-Bridge-FC-Port

Die Storage-Zonen verwenden das Standard-Zoning.

Die Beispiele zeigen zwei Brückenpaare, die an jedem Standort zwei Stapelgruppen miteinander verbinden. Da jede Bridge einen FC Port verwendet, gibt es insgesamt vier Storage-Zonen pro Fabric (insgesamt acht).

Brückenbenennung

Die Brücken verwenden das folgende Beispiel: Bridge_site_Stack Sammelversetzung in Paar

Dieser Teil des Namens…	Identifiziert…	Mögliche Werte…
Standort	Standort, auf dem sich das Brückenpaar physisch befindet.	A oder B
Stapelgruppe	Nummer der Stapelgruppe, mit der das Brückenpaar verbunden ist. FibreBridge 7600N oder 7500N-Brücken unterstützen bis zu vier Stapel in der Stapelgruppe. Die Stack-Gruppe kann maximal 10 Storage Shelves enthalten.	1, 2, usw.
Position in Paar	Brücke innerhalb des Brückenpaares.Ein Paar Brücken verbinden sich mit einer bestimmten Stapelgruppe.	A oder b

Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

- Bridge_A_1a
- Bridge_A_1b
- Bridge_B_1a
- Bridge_B_1b

DR-Gruppe 1 - Stack 1 bei Site_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	7	Controller_A_2-Port 0c
FC_Switch_A_1	A	5	8	Bridge_A_1a FC1

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_B_1	B	7	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	6	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	7	Controller_B_2-Port 0c

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	6	2	Port 0b_A_1
FC_Switch_A_1	A	6	3	Controller_A_1-Port 0d
FC_Switch_A_1	A	6	6	Port 0b_Controller_A_2
FC_Switch_A_1	A	6	7	Controller_A_2-Port 0d
FC_Switch_A_1	A	6	8	Bridge_A_1b FC1
FC_Switch_B_1	B	8	2	Controller_B_1-Port 0b
FC_Switch_B_1	B	8	3	Controller_B_1-Port 0d
FC_Switch_B_1	B	8	6	Port 0b_B_2
FC_Switch_B_1	B	8	7	Controller_B_2-Port 0d

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8

DR-Gruppe 1 - Stack 2 bei Site_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	7	Controller_A_2-Port 0c
FC_Switch_A_1	A	5	9	Bridge_A_2a FC1
FC_Switch_B_1	B	7	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	6	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	7	Controller_B_2-Port 0c

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	6	2	Port 0b_A_1
FC_Switch_A_1	A	6	3	Controller_A_1-Port 0d
FC_Switch_A_1	A	6	6	Port 0b_Controller_A_2
FC_Switch_A_1	A	6	7	Controller_A_2-Port 0d
FC_Switch_A_1	A	6	9	Bridge_A_2b FC1

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_B_1	B	8	2	Controller_B_1-Port 0b
FC_Switch_B_1	B	8	3	Controller_B_1-Port 0d
FC_Switch_B_1	B	8	6	Port 0b_B_2
FC_Switch_B_1	B	8	7	Controller_B_2-Port 0d

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9

DR-Gruppe 1 – Stack 1 an Standort_B

MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505-, 6510-, 6520-, G620-, G610- oder G710-Switch	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	7	Controller_A_2-Port 0c
FC_Switch_B_1	B	7	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	6	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	7	Controller_B_2-Port 0c
FC_Switch_B_1	B	7	8	Bridge_B_1a FC1

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505-, 6510-, 6520-, G620-, G610- oder G710-Switch	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	6	2	Port 0b_A_1
FC_Switch_A_1	A	6	3	Controller_A_1-Port 0d
FC_Switch_A_1	A	6	6	Port 0b_Controller_A_2
FC_Switch_A_1	A	6	7	Controller_A_2-Port 0d
FC_Switch_B_1	B	8	2	Controller_B_1-Port 0b
FC_Switch_B_1	B	8	3	Controller_B_1-Port 0d
FC_Switch_B_1	B	8	6	Port 0b_B_2
FC_Switch_B_1	B	8	7	Controller_B_2-Port 0d
FC_Switch_B_1	B	8	8	Bridge_B_1b FC1

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8

DR-Gruppe 1 - Stack 2 an Standort_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	7	Controller_A_2-Port 0c
FC_Switch_B_1	B	7	2	Controller_B_1-Port 0a

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_B_1	B	7	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	6	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	7	Controller_B_2-Port 0c
FC_Switch_B_1	B	7	9	Bridge_b_2a FC1

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1:

FC Switch	Standort	Switch-Domäne	Brocade 6505, 6510, 6520, G620, G610 oder G710 Switch-Port	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	6	2	Port 0b_A_1
FC_Switch_A_1	A	6	3	Controller_A_1-Port 0d
FC_Switch_A_1	A	6	6	Port 0b_Controller_A_2
FC_Switch_A_1	A	6	7	Controller_A_2-Port 0d
FC_Switch_B_1	B	8	2	Controller_B_1-Port 0b
FC_Switch_B_1	B	8	3	Controller_B_1-Port 0d
FC_Switch_B_1	B	8	6	Port 0b_B_2
FC_Switch_B_1	B	8	7	Controller_B_2-Port 0d
FC_Switch_B_1	B	8	9	Bridge_B_1b FC1

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Zusammenfassung der Speicherzonen

Fabric	Zonenname	Mitgliedsports

FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Zone FibreBridge 7500N-Brücken verwenden beide FC-Ports

Wenn Sie FibreBridge 7500N-Brücken mit beiden FC-Ports verwenden, müssen Sie Speicherzonen für die Bridge-Ports erstellen. Sie sollten die Zonen und die zugehörigen Ports verstehen, bevor Sie die Zonen konfigurieren.

Erforderliche Zonen

Sie müssen eine Zone für jede der FC-to-SAS-Bridge-FC-Ports konfigurieren, die den Datenverkehr zwischen Initiatoren auf jedem Controller-Modul und diese FC-to-SAS-Bridge zulässt.

Jede Speicherzone enthält fünf Ports:

- Vier HBA-Initiator-Ports (eine Verbindung für jeden Controller)
- Ein Port mit einer FC-to-SAS-Bridge-FC-Port

Die Storage-Zonen verwenden das Standard-Zoning.

Die Beispiele zeigen zwei Brückenpaare, die an jedem Standort zwei Stapelgruppen miteinander verbinden. Da jede Bridge einen FC Port verwendet, gibt es insgesamt acht Storage-Zonen pro Fabric (insgesamt sechzehn).

Brückenbenennung

Die Brücken verwenden das folgende Beispiel: Bridge_site_Stack Sammelversetzung in Paar

Dieser Teil des Namens…	Identifiziert…	Mögliche Werte…
Standort	Standort, auf dem sich das Brückenpaar physisch befindet.	A oder B

Stapelgruppe	Nummer der Stapelgruppe, mit der das Brückenpaar verbunden ist. FibreBridge 7600N oder 7500N-Brücken unterstützen bis zu vier Stapel in der Stapelgruppe. Die Stack-Gruppe kann maximal 10 Storage Shelves enthalten.	1, 2, usw.
Position in Paar	Brücke innerhalb des Brückenpaares. Ein Paar Brücken verbinden sich mit einer bestimmten Stapelgruppe.	A oder b

Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

- Bridge_A_1a
- Bridge_A_1b
- Bridge_B_1a
- Bridge_B_1b

DR-Gruppe 1 - Stack 1 bei Site_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 /G710 / G620-Anschluss	6520 Anschlüsse	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	6	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	8	8	Bridge_A_1a FC1
FC_Switch_B_1	B	7	2	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	6	6	Controller_B_2-Port 0a

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	3	3	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	7	7	7	Controller_A_2-Port 0c
FC_Switch_A_1	A	5	9	9	9	Bridge_A_1b FC1
FC_Switch_B_1	B	7	3	3	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	7	7	7	Controller_B_2-Port 0c

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710	6520	G620	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	2	2	2	Port 0b_A_1
FC_Switch_A_2	A	6	6	6	6	Port 0b_Controller_A_2
FC_Switch_A_2	A	6	8	8	8	Bridge_A_1a FC2
FC_Switch_B_2	B	8	2	2	2	Controller_B_1-Port 0b
FC_Switch_B_2	B	8	6	6	6	Port 0b_B_2

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710	6520	G620	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	3	3	3	Controller_A_1-Port 0d
FC_Switch_A_2	A	6	7	7	7	Controller_A_2-Port 0d
FC_Switch_A_2	A	6	9	9	9	Bridge_A_1b FC2
FC_Switch_B_2	B	8	3	3	3	Controller_B_1-Port 0d
FC_Switch_B_2	B	8	7	7	7	Controller_B_2-Port 0d

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9

DR-Gruppe 1 - Stack 2 bei Site_A

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	2	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	6	6	6	Controller_A_2-Port 0a
FC_Switch_A_1	A	5	10	10	10	Bridge_A_2a FC1

FC_Switch_B_1	B	7	2	2	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	6	6	6	Controller_B_2-Port 0a

Zone in Fabric_1 h	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	3	3	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	7	7	7	Controller_A_2-Port 0c
FC_Switch_A_1	A	5	11	11	11	Bridge_A_2b FC1
FC_Switch_B_1	B	7	3	3	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	7	7	7	Controller_B_2-Port 0c

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11

DRGROUP 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	2	0	0	Port 0b_A_1

FC_Switch_A_2	A	6	6	4	4	Port 0b_Controller_A_2
FC_Switch_A_2	A	6	10	10	10	Bridge_A_2a FC2
FC_Switch_B_2	B	8	2	2	2	Controller_B_1-Port 0b
FC_Switch_B_2	B	8	6	6	6	Port 0b_B_2

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	3	3	3	Controller_A_1-Port 0d
FC_Switch_A_2	A	6	7	7	7	Controller_A_2-Port 0d
FC_Switch_A_2	A	6	11	11	11	Bridge_A_2b FC2
FC_Switch_B_2	B	8	3	3	3	Controller_B_1-Port 0d
FC_Switch_B_2	B	8	7	7	7	Controller_B_2-Port 0d

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11

DR-Gruppe 1 – Stack 1 an Standort_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	2	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	6	6	6	Controller_A_2-Port 0a
FC_Switch_B_1	B	7	2	2	8	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	6	6	2	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	8	8	6	Bridge_B_1a FC1

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	3	3	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	7	7	7	Controller_A_2-Port 0c
FC_Switch_B_1	B	7	3	3	9	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	7	7	3	Controller_B_2-Port 0c
FC_Switch_B_1	B	7	9	9	7	Bridge_B_1b FC1

Zone in Fabric_2	Mitgliedsports

MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	2	2	2	Port 0b_A_1
FC_Switch_A_2	A	6	6	6	6	Port 0b_Controller_A_2
FC_Switch_B_2	B	8	2	2	2	Controller_B_1-Port 0b
FC_Switch_B_2	B	8	6	6	6	Port 0b_B_2
FC_Switch_B_2	B	8	8	8	8	Bridge_B_1a FC2

Zone in Fabric_1	**Mitgliedsports**
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	3	3	3	Controller_A_1-Port 0d
FC_Switch_A_2	A	6	7	7	7	Controller_A_2-Port 0d
FC_Switch_B_2	B	8	3	3	3	Controller_B_1-Port 0d
FC_Switch_B_2	B	8	7	7	7	Controller_B_2-Port 0d

FC_Switch_B_2	B	8	9	9	9	Bridge_A_1b FC2

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

DR-Gruppe 1 - Stack 2 an Standort_B

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	2	2	2	Controller_A_1-Port 0a
FC_Switch_A_1	A	5	6	6	6	Controller_A_2-Port 0a
FC_Switch_B_1	B	7	2	2	2	Controller_B_1-Port 0a
FC_Switch_B_1	B	7	6	6	6	Controller_B_2-Port 0a
FC_Switch_B_1	B	7	10	10	10	Bridge_B_2a FC1

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_1	A	5	3	3	3	Controller_A_1-Port 0c
FC_Switch_A_1	A	5	7	7	7	Controller_A_2-Port 0c

FC_Switch_B_1	B	7	3	3	3	Controller_B_1-Port 0c
FC_Switch_B_1	B	7	7	7	7	Controller_B_2-Port 0c
FC_Switch_B_1	B	7	11	11	11	Bridge_B_2b FC1

Zone in Fabric_2 h	Mitgliedsports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

DRGROUP 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…
FC_Switch_A_2	A	6	2	2	2	Port 0b_A_1
FC_Switch_A_2	A	6	6	6	6	Port 0b_Controller_A_2
FC_Switch_B_2	B	8	2	2	2	Controller_B_1-Port 0b
FC_Switch_B_2	B	8	6	6	6	Port 0b_B_2
FC_Switch_B_2	B	8	10	10	10	Bridge_B_2a FC2

Zone in Fabric_1	Mitgliedsports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10

DRGROUP 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2:

FC Switch	Standort	Switch-Domäne	6505 / 6510 / G610 / G710-Anschluss	6520 Anschlüsse	G620-Anschluss	Verbindung wird hergestellt mit…

FC_Switch_A_2	A	6	3	3	3	Controller_A_1-Port 0d
FC_Switch_A_2	A	6	7	7	7	Controller_A_2-Port 0d
FC_Switch_B_2	B	8	3	3	3	Controller_B_1-Port 0d
FC_Switch_B_2	B	8	7	7	7	Controller_B_2-Port 0d
FC_Switch_B_2	B	8	11	11	11	Bridge_B_2b FC2

Zone in Fabric_2	Mitgliedsports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Zusammenfassung der Speicherzonen

Fabric	Zonenname	Mitgliedsports
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10
FC_Switch_A_1 und FC_Switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10
FC_Switch_A_2 und FC_Switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Zonieren Sie die Brocade FC-Switches

Sie müssen die Switch-Ports separaten Zonen zuweisen, sodass der Controller- und Storage-Traffic über Zonen für die FC-VI-Ports und Zonen für die Storage-Ports getrennt wird.

Über diese Aufgabe

Bei den folgenden Schritten wird das Standard-Zoning für die MetroCluster-Konfiguration verwendet.

"Zoning für FC-VI-Ports"

"Zoning für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port"

"Zoning für FibreBridge 7500N-Bridges unter Verwendung beider FC-Ports"

Schritte

1. Erstellung der FC-VI-Zonen auf jedem Switch:

   ```
   zonecreate "QOSH1_FCVI_1", member;member …
   ```

   In diesem Beispiel wird eine QOS FCVI-Zone mit den Ports 5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5 erstellt:

   ```
   Switch_A_1:admin> zonecreate "QOSH1_FCVI_1",
   "5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
   ```

2. Konfigurieren Sie die Storage-Zonen auf jedem Switch.

   Sie können das Zoning für die Fabric von einem Switch in der Fabric konfigurieren. Im folgenden Beispiel wird das Zoning auf Switch_A_1 konfiguriert.

   a. Erstellen der Storage-Zone für jede Switch-Domäne in der Switch-Fabric:

      ```
      zonecreate name, member;member …
      ```

      In diesem Beispiel wird eine Speicherzone für eine FibreBridge 7500N mit beiden FC-Ports erstellt. Die Zonen enthalten Anschlüsse 5,2;5,6;7,2;7,6;5,16:

      ```
      Switch_A_1:admin> zonecreate
      "MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
      ```

   b. Konfiguration in der ersten Switch-Fabric erstellen:

      ```
      cfgcreate config_name, zone;zone…
      ```

      In diesem Beispiel wird eine Konfiguration mit dem Namen CFG_1 und den beiden Zonen QOSH1_MC1_FAB_1_FCVI und MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1 erstellt

      ```
      Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;
      MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
      ```

   c. Fügen Sie bei Bedarf Zonen zur Konfiguration hinzu:

      ```
      cfgadd config_namezone;zone…
      ```

   d. Aktivieren der Konfiguration:

      ```
      cfgenable config_name
      ```

      ```
      Switch_A_1:admin> cfgenable "CFG_1"
      ```

   e. Konfiguration speichern:

      ```
      cfgsave
      ```

      ```
      Switch_A_1:admin> cfgsave
      ```

   f. Validierung der Zoning-Konfiguration:

      ```
      zone --validate
      ```

```
Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
-----------------------------------
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone
```

ISL-Verschlüsselung auf Brocade 6510- oder G620-Switches einrichten

Bei Brocade 6510- oder G620-Switches kann optional die Brocade Verschlüsselungsfunktion auf den ISL-Verbindungen genutzt werden. Wenn Sie die Verschlüsselungsfunktion verwenden möchten, müssen Sie bei jedem Switch der MetroCluster-Konfiguration weitere Konfigurationsschritte durchführen.

Bevor Sie beginnen

- Sie benötigen Brocade 6510 oder G620 Switches.

> Unterstützung der ISL-Verschlüsselung bei Brocade G620 Switches wird nur ab ONTAP 9.4 unterstützt.

- Sie müssen zwei Schalter aus derselben Fabric ausgewählt haben.
- Sie müssen die Brocade Dokumentation für Ihren Switch und Fabric Operating System Version überprüfen, um die Bandbreiten- und Port-Grenzwerte zu bestätigen.

Über diese Aufgabe

Die Schritte müssen an beiden Switches in derselben Fabric ausgeführt werden.

Virtuelles Fabric deaktivieren

Um die ISL-Verschlüsselung einzustellen, muss die virtuelle Fabric auf allen vier in einer MetroCluster-Konfiguration verwendeten Switches deaktiviert werden.

Schritte

1. Deaktivieren Sie die virtuelle Fabric, indem Sie an der Switch-Konsole den folgenden Befehl eingeben:

   ```
   fosconfig --disable vf
   ```

2. Starten Sie den Switch neu.

Legen Sie die Nutzlast fest

Nach der Deaktivierung der virtuellen Fabric müssen Sie die Nutzlastgröße oder die Datenfeldgröße auf beiden Switches in der Fabric festlegen.

Über diese Aufgabe

Die Größe des Datenfelds darf 2048 nicht überschreiten.

Schritte

1. Deaktivieren Sie den Schalter:

   ```
   switchdisable
   ```

2. Konfigurieren und Festlegen der Nutzlast:

   ```
   configure
   ```

3. Stellen Sie die folgenden Schalterparameter ein:
   a. Legen Sie den Fabric-Parameter wie folgt fest: `y`
   b. Legen Sie die anderen Parameter fest, z. B. Domain, WWN-basierte persistente PID usw.
   c. Festlegen der Datenfeldgröße: `2048`

Legen Sie die Authentifizierungsrichtlinie fest

Sie müssen die Authentifizierungsrichtlinie und die zugehörigen Parameter festlegen.

Über diese Aufgabe

Die Befehle müssen an der Switch-Konsole ausgeführt werden.

Schritte

1. Legen Sie den Authentifizierungsschlüssel fest:

   a. Starten Sie den Setup-Prozess:

      ```
      secAuthSecret --set
      ```

   Mit diesem Befehl werden eine Reihe von Eingabeaufforderungen initiiert, auf die Sie in den folgenden

Schritten reagieren:

a. Geben Sie den weltweiten Namen (WWN) des anderen Switch in der Fabric für den Parameter „Enter Peer WWN, Domain, Switch Name“ ein.
b. Geben Sie den Peer Secret für den Parameter „Enter Peer Secret“ ein.
c. Geben Sie das lokale Geheimnis für den Parameter „Ortsgeheimnis eingeben“ an.
d. Eingabe `Y` Für den Parameter „are you done“.

   Das folgende Beispiel ist das Festlegen des Authentifizierungsgeheimnisses:

```
brcd> secAuthSecret --set

This command is used to set up secret keys for the DH-CHAP
authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is
performed
whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using
an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):
10:00:00:05:33:76:2e:99
Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] yes
Saving data to key store... Done.
```

2. Setzen Sie die Authentifizierungsgruppe auf 4:

```
authUtil --set -g 4
```

3. Legen Sie den Authentifizierungstyp auf „dhchap“ fest:

   ```
   authUtil --set -a dhchap
   ```

   Das System zeigt die folgende Ausgabe an:

   ```
   Authentication is set to dhchap.
   ```

4. Legen Sie die Authentifizierungsrichtlinie auf ein:

   ```
   authUtil --policy -sw on
   ```

   Das System zeigt die folgende Ausgabe an:

   ```
   Warning: Activating the authentication policy requires either DH-CHAP
   secrets or PKI certificates depending on the protocol selected.
   Otherwise, ISLs will be segmented during next E-port bring-up.
   ARE YOU SURE  (yes, y, no, n): [no] yes
   Auth Policy is set to ON
   ```

Aktivierung der ISL-Verschlüsselung bei Brocade Switches

Nachdem Sie die Authentifizierungsrichtlinie und das Authentifizierungsgeheimnis festgelegt haben, müssen Sie die ISL-Verschlüsselung auf den Ports aktivieren, damit sie wirksam wird.

Über diese Aufgabe

- Diese Schritte sollten jeweils an der Switch-Fabric durchgeführt werden.
- Die Befehle müssen an der Switch-Konsole ausgeführt werden.

Schritte

1. Verschlüsselung auf allen ISL-Ports aktivieren:

   ```
   portCfgEncrypt --enable port_number
   ```

   Im folgenden Beispiel wird die Verschlüsselung auf den Ports 8 und 12 aktiviert:

   ```
   portCfgEncrypt --enable 8
   ```

   ```
   portCfgEncrypt --enable 12
   ```

2. Schalter aktivieren:

   ```
   switchenable
   ```

3. Stellen Sie sicher, dass die ISL verfügbar ist und funktioniert:

   ```
   islshow
   ```

4. Vergewissern Sie sich, dass die Verschlüsselung aktiviert ist:

   ```
   portenccompshow
   ```

   Das folgende Beispiel zeigt, dass die Verschlüsselung auf den Ports 8 und 12 aktiviert ist:

   ```
   User Encryption
   Port  configured     Active
   ----   ----------    ------
    8      yes          yes
    9      No           No
    10     No           No
    11     No           No
    12     yes          yes
   ```

Nächste Schritte

Führen Sie in einer MetroCluster-Konfiguration alle Schritte auf den Switches in der anderen Fabric aus.

Konfigurieren Sie Cisco FC-Switches manuell

Jeder Cisco Switch in der MetroCluster-Konfiguration muss entsprechend für ISL- und Storage-Verbindungen konfiguriert sein.

Bevor Sie beginnen

Für die Cisco FC Switches gelten die folgenden Anforderungen:

- Sie müssen vier unterstützte Cisco Switches desselben Modells mit derselben NX-OS-Version und derselben Lizenzierung verwenden.
- Die MetroCluster Konfiguration erfordert vier Switches.

  Die vier Switches müssen mit zwei Fabrics von jeweils zwei Switches verbunden sein, wobei jede Fabric beide Standorte umfasst.

- Der Switch muss die Konnektivität zum ATTO FibreBridge-Modell unterstützen.
- Sie können die Verschlüsselung oder Komprimierung nicht in der Cisco FC Storage Fabric verwenden. Es wird in der MetroCluster-Konfiguration nicht unterstützt.

Im "NetApp Interoperabilitäts-Matrix-Tool (IMT)", Sie können im Feld Storage-Lösung die MetroCluster-Lösung auswählen. 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.

Über diese Aufgabe

Für die Inter-Switch Link-Verbindungen (ISL) gelten folgende Anforderungen:

- Alle ISLs müssen in einem Fabric dieselbe Länge und dieselbe Geschwindigkeit aufweisen.

  In den verschiedenen Fabrics können verschiedene Längen von ISLs verwendet werden. Die gleiche Geschwindigkeit muss in allen Stoffen verwendet werden.

Folgende Anforderungen gelten für die Storage-Verbindungen:

- Jeder Storage-Controller muss vier Initiator-Ports besitzen, um mit den Switch-Fabrics verbunden zu werden.

  Von jedem Storage Controller müssen zwei Initiator-Ports mit jeder Fabric verbunden sein.

> Sie können FAS8020, AFF8020, FAS8200 und AFF A300 Systeme mit zwei Initiatoren-Ports pro Controller (ein einzelner Initiator-Port zu jedem Fabric) konfigurieren, wenn alle folgenden Kriterien erfüllt sind:
>
> - Es sind weniger als vier FC-Initiator-Ports zum Verbinden des Festplatten-Storage verfügbar, und keine zusätzlichen Ports können als FC-Initiatoren konfiguriert werden.
> - Alle Steckplätze werden verwendet und es kann keine FC-Initiatorgruppe hinzugefügt werden.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Lizenzanforderungen für Cisco Switch

Bestimmte funktionsbasierte Lizenzen sind möglicherweise für die Cisco Switches in einer Fabric-Attached MetroCluster Konfiguration erforderlich. Mit diesen Lizenzen können Funktionen wie QoS oder Gutschriften im Fernmodus auf den Switches verwendet werden. Sie müssen die erforderlichen funktionsbasierten Lizenzen auf allen vier Switches einer MetroCluster-Konfiguration installieren.

Die folgenden funktionsbasierten Lizenzen sind möglicherweise in einer MetroCluster Konfiguration erforderlich:

- ENTERPRISE_PKG

  Diese Lizenz ermöglicht die Verwendung der QoS-Funktion auf Cisco Switches.

- PORT_ACTIVATION_PKG

  Sie können diese Lizenz für Cisco 9148-Switches verwenden. Mit dieser Lizenz können Sie Ports an den Switches aktivieren oder deaktivieren, solange jeweils nur 16 Ports aktiv sind. Standardmäßig sind 16 Ports in Cisco MDS 9148 Switches aktiviert.

- FM_SERVER_PKG

  Mit dieser Lizenz können Sie Fabrics gleichzeitig verwalten und Switches über einen Webbrowser verwalten.

  Die FM_SERVER_PKG-Lizenz ermöglicht außerdem Leistungsmanagementfunktionen wie Leistungsschwellenwerte und Schwellenwertüberwachung. Weitere Informationen zu dieser Lizenz finden Sie im Cisco Fabric Manager Server Package.

Sie können mithilfe des Befehls show license Usage überprüfen, ob die Lizenzen installiert wurden. Wenn Sie diese Lizenzen nicht besitzen, wenden Sie sich an Ihren Vertriebsmitarbeiter, bevor Sie mit der Installation fortfahren.

Die Cisco MDS 9250i Switches verfügen über zwei feste 1/10 GbE IP-Storage-Service-Ports. Für diese Ports sind keine zusätzlichen Lizenzen erforderlich. Das Cisco SAN Extension over IP Application-Paket ist eine Standardlizenz für diese Switches, die Funktionen wie FCIP und Komprimierung unterstützt.

Setzen des Cisco FC-Switches auf die Werkseinstellungen

Um eine erfolgreiche Konfiguration zu gewährleisten, müssen Sie den Switch auf die Werkseinstellungen zurücksetzen. Dadurch wird sichergestellt, dass der Switch von einer sauberen Konfiguration gestartet wird.

Über diese Aufgabe

Diese Aufgabe muss an allen Switches der MetroCluster-Konfiguration ausgeführt werden.

Schritte

1. Verbinden Sie die Konsole, und melden Sie sich bei beiden Switches in derselben Fabric an.
2. Setzen Sie den Schalter auf die Standardeinstellungen zurück:

   ```
   write erase
   ```

   Sie können „`y`“ antworten, wenn Sie dazu aufgefordert werden, den Befehl zu bestätigen. Dadurch werden alle Lizenzen und Konfigurationsinformationen auf dem Switch gelöscht.

3. Starten Sie den Switch neu:

   ```
   reload
   ```

   Sie können „`y`“ antworten, wenn Sie dazu aufgefordert werden, den Befehl zu bestätigen.

4. Wiederholen Sie den `write erase` Und `reload` Befehle auf dem anderen Switch.

   Nach Ausstellung des `reload` Befehl, der Switch wird neu gebootet und anschließend werden mit Setup-Fragen aufgefordert. Dann fahren Sie mit dem nächsten Abschnitt fort.

Beispiel

Das folgende Beispiel zeigt den Prozess für eine Fabric, die aus FC_Switch_A_1 und FC_Switch_B_1 besteht.

```
FC_Switch_A_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_A_1# reload
    This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_B_1# reload
    This command will reboot the system. (y/n)?  [n] y
```

Konfigurieren Sie die Grundeinstellungen des Cisco FC-Switches und den Community String

Sie müssen die Grundeinstellungen mit dem angeben `setup` Befehl oder nach Ausgabe des `reload` Befehl.

Schritte

1. Wenn der Switch die Setup-Fragen nicht anzeigt, konfigurieren Sie die grundlegenden Switch-Einstellungen:

   ```
   setup
   ```

2. Akzeptieren Sie die Standardantworten auf die Setup-Fragen, bis Sie zur SNMP-Community-Zeichenfolge aufgefordert werden.
3. Setzen Sie die Community-Zeichenfolge auf „`public`“ (alle Kleinbuchstaben), um den Zugriff von den ONTAP Health-Monitoren zu ermöglichen.

   Sie können die Community-Zeichenfolge auf einen anderen Wert als „`public`“ setzen. Sie müssen jedoch die ONTAP-Integritätsmonitore mithilfe der von Ihnen angegebenen Community-Zeichenfolge konfigurieren.

   Im folgenden Beispiel werden die Befehle an FC_Switch_A_1 angezeigt:

   ```
   FC_switch_A_1# setup
       Configure read-only SNMP community string (yes/no) [n]: y
       SNMP community string : public
       Note:  Please set the SNMP community string to "Public" or another
   value of your choosing.
       Configure default switchport interface state (shut/noshut) [shut]:
   noshut
       Configure default switchport port mode F (yes/no) [n]: n
       Configure default zone policy (permit/deny) [deny]: deny
       Enable full zoneset distribution? (yes/no) [n]: yes
   ```

   Im folgenden Beispiel werden die Befehle an FC_Switch_B_1 angezeigt:

   ```
   FC_switch_B_1# setup
       Configure read-only SNMP community string (yes/no) [n]: y
       SNMP community string : public
       Note:  Please set the SNMP community string to "Public" or another
   value of your choosing.
       Configure default switchport interface state (shut/noshut) [shut]:
   noshut
       Configure default switchport port mode F (yes/no) [n]: n
       Configure default zone policy (permit/deny) [deny]: deny
       Enable full zoneset distribution? (yes/no) [n]: yes
   ```

Erwerben von Lizenzen für Ports

Sie müssen keine Cisco Switch-Lizenzen auf einer kontinuierlichen Reihe von Ports verwenden. Stattdessen können Sie Lizenzen für bestimmte Ports erwerben, die verwendet werden, und Lizenzen von nicht verwendeten Ports entfernen.

Bevor Sie beginnen

Sie sollten die Anzahl der lizenzierten Ports in der Switch-Konfiguration überprüfen und bei Bedarf Lizenzen von einem Port in einen anderen verschieben.

Schritte

1. Anzeigen der Lizenzverwendung für eine Switch-Fabric:

   ```
   show port-resources module 1
   ```

   Ermitteln Sie, welche Ports Lizenzen benötigen. Wenn einige dieser Ports nicht lizenziert sind, ermitteln Sie, ob Sie über zusätzliche lizenzierte Ports verfügen, und ziehen Sie in Betracht, die Lizenzen von ihnen zu entfernen.

2. Konfigurationsmodus aufrufen:

   ```
   config t
   ```

3. Entfernen Sie die Lizenz vom ausgewählten Port:
   a. Wählen Sie den Port aus, der nicht lizenziert werden soll:

      ```
      interface interface-name
      ```

      b. Entfernen Sie die Lizenz vom Port:

      ```
      no port-license acquire
      ```

      c. Beenden Sie die Schnittstelle für die Portkonfiguration:

      ```
      exit
      ```

4. Erwerben Sie die Lizenz für den ausgewählten Port:
   a. Wählen Sie den Port aus, der nicht lizenziert werden soll:

      ```
      interface interface-name
      ```

      b. Stellen Sie den Port für den Erwerb einer Lizenz zur Verfügung:

      ```
      port-license
      ```

      c. Erwerben Sie die Lizenz auf dem Port:

      ```
      port-license acquire
      ```

      d. Beenden Sie die Schnittstelle für die Portkonfiguration:

      ```
      exit
      ```

5. Wiederholen Sie diesen Vorgang für alle weiteren Ports.
6. Konfigurationsmodus beenden:

```
exit
```

Entfernen und Erwerb einer Lizenz auf einem Port

Dieses Beispiel zeigt, dass eine Lizenz von Port fc1/2 entfernt wird, Port fc1/1 für den Erwerb einer Lizenz zugelassen ist und die Lizenz an Port fc1/1 erworben wird:

```
Switch_A_1# conf t
    Switch_A_1(config)# interface fc1/2
    Switch_A_1(config)# shut
    Switch_A_1(config-if)# no port-license acquire
    Switch_A_1(config-if)# exit
    Switch_A_1(config)# interface fc1/1
    Switch_A_1(config-if)# port-license
    Switch_A_1(config-if)# port-license acquire
    Switch_A_1(config-if)# no shut
    Switch_A_1(config-if)# end
    Switch_A_1# copy running-config startup-config

    Switch_B_1# conf t
    Switch_B_1(config)# interface fc1/2
    Switch_B_1(config)# shut
    Switch_B_1(config-if)# no port-license acquire
    Switch_B_1(config-if)# exit
    Switch_B_1(config)# interface fc1/1
    Switch_B_1(config-if)# port-license
    Switch_B_1(config-if)# port-license acquire
    Switch_B_1(config-if)# no shut
    Switch_B_1(config-if)# end
    Switch_B_1# copy running-config startup-config
```

Im folgenden Beispiel wird die Verwendung der Portlizenz überprüft:

```
Switch_A_1# show port-resources module 1
    Switch_B_1# show port-resources module 1
```

Ermöglicht Ports in einem Cisco MDS 9148 oder 9148S Switch

Bei Cisco MDS 9148 oder 9148S Switches müssen die in einer MetroCluster-Konfiguration erforderlichen Ports manuell aktiviert werden.

Über diese Aufgabe

- Sie können 16 Ports in einem Cisco MDS 9148 oder 9148S Switch manuell aktivieren.
- Mithilfe der Cisco Switches können Sie die POD-Lizenz auf zufälligen Ports anwenden, anstatt sie nacheinander anzuwenden.
- Für Cisco Switches ist erforderlich, dass Sie einen Port pro Portgruppe verwenden, es sei denn, Sie benötigen mehr als 12 Ports.

Schritte

1. Zeigen Sie die Portgruppen an, die in einem Cisco-Switch verfügbar sind:

   ```
   show port-resources module blade_number
   ```

2. Lizenz und erwerben Sie den erforderlichen Port in einer Portgruppe:

   ```
   config t

   interface port_number

   shut

   port-license acquire

   no shut
   ```

   Beispiel: Die folgende Befehlssequenz lizenziert und erwirbt Port fc 1/45:

   ```
   switch# config t
   switch(config)#
   switch(config)# interface fc 1/45
   switch(config-if)#
   switch(config-if)# shut
   switch(config-if)# port-license acquire
   switch(config-if)# no shut
   switch(config-if)# end
   ```

3. Konfiguration speichern:

   ```
   copy running-config startup-config
   ```

Konfiguration der F-Ports an einem Cisco FC-Switch

Sie müssen die F-Ports auf dem FC-Switch konfigurieren.

Über diese Aufgabe

In einer MetroCluster-Konfiguration sind die F-Ports die Ports, die den Switch mit den HBA-Initiatoren, FC-VI-Interconnects und FC-to-SAS-Bridges verbinden.

Jeder Port muss individuell konfiguriert werden.

In den folgenden Abschnitten werden die F-Ports (Switch-to-Node) für Ihre Konfiguration identifiziert:

- "Portzuweisungen für FC-Switches"

Diese Aufgabe muss an jedem Switch in der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   config t
   ```

2. Wechseln Sie in den Schnittstellenkonfigurationsmodus für den Port:

   `interface` *`port-ID`*

3. Fahren Sie den Port herunter:

   ```
   shutdown
   ```

4. Legen Sie die Ports auf F-Modus fest:

   ```
   switchport mode F
   ```

5. Legen Sie die Ports auf feste Geschwindigkeit fest:

   `switchport speed` *`speed-value`*

   `speed-value` Ist auch so `8000` Oder `16000`

6. Stellen Sie den Rate-Modus des Switch-Ports auf Dedicated ein:

   ```
   switchport rate-mode dedicated
   ```

7. Starten Sie den Port neu:

   ```
   no shutdown
   ```

8. Konfigurationsmodus beenden:

   ```
   end
   ```

Beispiel

Im folgenden Beispiel werden die Befehle an den beiden Switches angezeigt:

```
Switch_A_1# config  t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config  t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

Zuweisen von Buffer-to-Buffer Credits zu F-Ports in derselben Portgruppe wie die ISL

Sie müssen den F-Ports die Buffer-to-Buffer Credits zuweisen, wenn sie sich in derselben Portgruppe wie ISL befinden. Wenn die Ports nicht über die erforderlichen Buffer-to-Buffer Credits verfügen, könnte ISL funktionsunfähig sein.

Über diese Aufgabe

Dieser Task ist nicht erforderlich, wenn sich die F-Ports nicht in derselben Portgruppe wie der ISL-Port befinden.

Wenn sich die F-Ports in einer Portgruppe befinden, die ISL enthält, muss diese Aufgabe auf jedem FC-Switch in der MetroCluster-Konfiguration ausgeführt werden.

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   config t
   ```

2. Legen Sie den Schnittstellenkonfigurationsmodus für den Port fest:

   `interface` *`port-ID`*

3. Deaktivieren des Ports:

   ```
   shut
   ```

4. Wenn sich der Port nicht bereits im F-Modus befindet, setzen Sie den Port auf F-Modus:

   ```
   switchport mode F
   ```

5. Setzen Sie den Buffer-to-Buffer-Kredit der nicht-E-Ports auf 1:

   ```
   switchport fcrxbbcredit 1
   ```

6. Port erneut aktivieren:

   ```
   no shut
   ```

7. Konfigurationsmodus beenden:

   ```
   exit
   ```

8. Kopieren Sie die aktualisierte Konfiguration in die Startkonfiguration:

   ```
   copy running-config startup-config
   ```

9. Überprüfen Sie die Puffer-zu-Puffer-Gutschrift, die einem Port zugewiesen wurde:

   ```
   show port-resources module 1
   ```

10. Konfigurationsmodus beenden:

    ```
    exit
    ```

11. Wiederholen Sie diese Schritte auf dem anderen Schalter in der Struktur.
12. Überprüfen Sie die Einstellungen:

    ```
    show port-resource module 1
    ```

Beispiel

In diesem Beispiel ist Port fc1/40 ISL. Die Ports fc1/37, fc1/38 und fc1/39 befinden sich in derselben Portgruppe und müssen konfiguriert sein.

Mit den folgenden Befehlen wird der Portbereich angezeigt, der für fc1/37 bis fc1/39 konfiguriert ist:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

Mit den folgenden Befehlen und der Systemausgabe werden die Einstellungen ordnungsgemäß angewendet:

```
FC_switch_A_1# show port-resource module 1
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                      Buffers     (Gbps)

--------------------------------------------------------------------
fc1/37                                     32        8.0  dedicated
fc1/38                                      1        8.0  dedicated
fc1/39                                      1        8.0  dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                        Buffers     (Gbps)

--------------------------------------------------------------------
fc1/37                                     32        8.0  dedicated
fc1/38                                      1        8.0  dedicated
fc1/39                                      1        8.0 dedicated
...
```

Erstellen und Konfigurieren von VSANs auf Cisco FC-Switches

Sie müssen ein VSAN für die FC-VI-Ports und ein VSAN für die Storage-Ports an jedem FC-Switch in der MetroCluster Konfiguration erstellen.

Über diese Aufgabe

Die VSANs sollten eine eindeutige Nummer und einen eindeutigen Namen haben. Sie müssen zusätzliche Konfigurationen vornehmen, wenn Sie zwei ISLs in der Reihenfolge der Frames verwenden.

Die Beispiele für diese Aufgabe verwenden die folgenden Namenskonventionen:

Switch-Fabric	VSAN-Name	ID-Nummer
1	FCVI_1_10	10
STOR_1_20	20	2

FCVI_2_30	30	STOR_2_20

Diese Aufgabe muss an jeder FC-Switch-Fabric durchgeführt werden.

Schritte

1. Konfiguration des FC-VI VSAN:
   a. Konfigurationsmodus aufrufen, falls dies noch nicht geschehen ist:

      ```
      config t
      ```

   b. Bearbeiten der VSAN-Datenbank:

      ```
      vsan database
      ```

   c. VSAN-ID festlegen:

      ```
      vsan vsan-ID
      ```

   d. VSAN-Name festlegen:

      ```
      vsan vsan-ID name vsan_name
      ```

2. Hinzufügen von Ports zum FC-VI VSAN:
   a. Fügen Sie die Schnittstellen für jeden Port im VSAN hinzu:

      ```
      vsan vsan-ID interface interface_name
      ```

      Bei dem FC-VI VSAN werden die Ports hinzugefügt, die die lokalen FC-VI-Ports verbinden.

   b. Konfigurationsmodus beenden:

      ```
      end
      ```

   c. Kopieren Sie die Running-config auf die Startup-config:

      ```
      copy running-config startup-config
      ```

      Im folgenden Beispiel sind die Ports fc1/1 und fc1/13:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

3. Überprüfen Sie die Portmitgliedschaft des VSAN:

   `show vsan member`

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

4. VSAN so konfigurieren, dass Frames in der Bestellung oder bei Lieferung nicht bestellter Frames geliefert werden:

   > Die Standard-IOD-Einstellungen werden empfohlen. Sie sollten OOD nur bei Bedarf konfigurieren.

   "Überlegungen bei der Verwendung von TDM/WDM-Geräten mit Fabric-Attached MetroCluster-Konfigurationen"

   - Zur Konfiguration der in der Reihenfolge der Bereitstellung von Frames müssen folgende Schritte durchgeführt werden:

     i. Konfigurationsmodus aufrufen:

     `conf t`

     ii. Ermöglichung der in-Order-Garantie für den Austausch des VSAN:

     `in-order-guarantee vsan vsan-ID`

     > Für FC-VI VSANs (FCVI_1_10 und FCVI_2_30) müssen Sie die in-Order-Garantie für Frames und Umtausche nur auf VSAN 10 aktivieren.

     iii. Lastausgleich für das VSAN aktivieren:

     `vsan vsan-ID loadbalancing src-dst-id`

iv. Konfigurationsmodus beenden:

```
end
```

v. Kopieren Sie die Running-config auf die Startup-config:

```
copy running-config startup-config
```

Die Befehle zur Konfiguration der in-order-Bereitstellung von Frames auf FC_Switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Die Befehle zur Konfiguration der in-order-Bereitstellung von Frames auf FC_Switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

- Die folgenden Schritte müssen ausgeführt werden, um die Lieferung von Frames außerhalb der Reihenfolge zu konfigurieren:

i. Konfigurationsmodus aufrufen:

```
conf t
```

ii. Deaktivieren der „in-order“-Garantie für den Austausch des VSAN:

```
no in-order-guarantee vsan vsan-ID
```

iii. Lastausgleich für das VSAN aktivieren:

```
vsan vsan-ID loadbalancing src-dst-id
```

iv. Konfigurationsmodus beenden:

```
end
```

v. Kopieren Sie die Running-config auf die Startup-config:

```
copy running-config startup-config
```

Die Befehle zur Konfiguration der nicht bestellenden Bereitstellung von Frames auf FC_Switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Die Befehle zur Konfiguration der nicht bestellenden Bereitstellung von Frames auf FC_Switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

+

> Bei der Konfiguration von ONTAP auf den Controller-Modulen muss OOD explizit auf jedem Controller-Modul in der MetroCluster-Konfiguration konfiguriert sein.

"Konfigurieren von in-Order-Lieferung oder Lieferung von Frames auf ONTAP Software außerhalb der Reihenfolge"

5. QoS-Richtlinien für FC-VI VSAN festlegen:

   a. Konfigurationsmodus aufrufen:

      ```
      conf t
      ```

   b. Aktivieren Sie die QoS und erstellen Sie eine Klassenzuordnung, indem Sie die folgenden Befehle nacheinander eingeben:

      ```
      qos enable
      ```

      ```
      qos class-map class_name match-any
      ```

   c. Fügen Sie die in einem vorherigen Schritt erstellte Klassenzuordnung der Richtlinienzuordnung hinzu:

      ```
      class class_name
      ```

   d. Legen Sie die Priorität fest:

      ```
      priority high
      ```

e. Fügen Sie das VSAN der zuvor in diesem Verfahren erstellten Richtlinienzuordnung hinzu:

```
qos service policy policy_name vsan vsan-id
```

f. Kopieren Sie die aktualisierte Konfiguration in die Startkonfiguration:

```
copy running-config startup-config
```

Die Befehle zum Festlegen der QoS-Richtlinien auf FC_Switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

Die Befehle zum Festlegen der QoS-Richtlinien auf FC_Switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. Konfiguration des Storage VSAN:

a. VSAN-ID festlegen:

```
vsan vsan-ID
```

b. VSAN-Name festlegen:

```
vsan vsan-ID name vsan_name
```

Die Befehle zur Konfiguration des Speicher-VSAN auf FC_Switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

Die Befehle zur Konfiguration des Speicher-VSAN auf FC_Switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

7. Ports zum Storage VSAN hinzufügen

   Bei dem Storage VSAN müssen alle Ports, die HBA- oder FC-to-SAS-Bridges verbinden, hinzugefügt werden. In diesem Beispiel fc1/5, fc1/9, fc1/17, fc1/21. fc1/25, fc1/29, fc1/33 und fc1/37 werden hinzugefügt.

   Die Befehle zum Hinzufügen von Ports zum Speicher VSAN zu FC_Switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

   Die Befehle zum Hinzufügen von Ports zum Speicher VSAN zu FC_Switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

E-Ports werden konfiguriert

Die Switch-Ports mit ISL müssen konfiguriert werden (dies sind die E-Ports).

Über diese Aufgabe

Die von Ihnen verwendete Vorgehensweise hängt davon ab, welchen Schalter Sie verwenden:

- Konfiguration der E-Ports am Cisco FC-Switch
- Konfiguration von FCIP-Ports für ein einzelnes ISL auf Cisco 9250i FC-Switches
- Konfiguration von FCIP-Ports für Dual ISL auf Cisco 9250i FC-Switches

Konfiguration der E-Ports am Cisco FC-Switch

Sie müssen die FC-Switch-Ports konfigurieren, die den Inter-Switch-Link (ISL) verbinden.

Über diese Aufgabe

Dies sind die E-Ports, und die Konfiguration muss für jeden Port erfolgen. Dazu müssen Sie die korrekte Anzahl von Buffer-to-Buffer Credits (BPCs) berechnen.

Alle ISLs in der Fabric müssen mit den gleichen Einstellungen für Geschwindigkeit und Entfernung konfiguriert sein.

Diese Aufgabe muss an jedem ISL-Port ausgeführt werden.

Schritte

1. Anhand der folgenden Tabelle können Sie die angepassten benötigten BBCs pro Kilometer für mögliche Portgeschwindigkeiten bestimmen.

   Um die korrekte Anzahl der BBCs zu ermitteln, multiplizieren Sie die benötigten angepassten BBCs (ermittelt aus der folgenden Tabelle) mit dem Abstand in Kilometern zwischen den Schaltern. Zur Berücksichtigung des FC-VI-Framing-Verhaltens ist ein Anpassungsfaktor von 1.5 erforderlich.

Geschwindigkeit in GB/s	BBCS pro Kilometer erforderlich	Angepasste BBCs erforderlich (BBU pro km x 1.5)

1	0.5	0.75
2	1	1.5
4	2	3
8	4	6
16	8	12

Um beispielsweise die erforderliche Anzahl an Credits für eine Entfernung von 30 km auf einem 4-Gbit/s-Link zu berechnen, gehen Sie wie folgt vor:

- `Speed in Gbps` Ist 4
- `Adjusted BBCs required` Ist 3
- `Distance in kilometers between switches` Ist 30 km
- 3 x 30 = 90

a. Konfigurationsmodus aufrufen:

```
config t
```

b. Geben Sie den Port an, den Sie konfigurieren:

```
interface port-name
```

c. Fahren Sie den Port herunter:

```
shutdown
```

d. Stellen Sie den Rate-Modus des Ports auf „Dedicated“ ein:

```
switchport rate-mode dedicated
```

e. Stellen Sie die Geschwindigkeit für den Port ein:

```
switchport speed speed-value
```

f. Legen Sie die Buffer-to-Buffer Credits für den Port fest:

```
switchport fcrxbbcredit number_of_buffers
```

g. Stellen Sie den Port auf E-Modus:

```
switchport mode E
```

h. Aktivieren Sie den Trunk-Modus für den Port:

```
switchport trunk mode on
```

i. Fügen Sie das ISL Virtual Storage Area Networks (VSANs) zum Trunk hinzu:

```
switchport trunk allowed vsan 10

switchport trunk allowed vsan add 20
```

j. Fügen Sie den Port zu Port Kanal 1 hinzu:

```
channel-group 1
```

k. Wiederholen Sie die vorherigen Schritte für den passenden ISL-Port am Partner-Switch in der Fabric.

Das folgende Beispiel zeigt den Port fc1/41, der für eine Entfernung von 30 km und 8 Gbit/s konfiguriert ist:

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

l. Geben Sie bei beiden Switches den folgenden Befehl ein, um die Ports neu zu starten:

```
no shutdown
```

m. Wiederholen Sie die vorherigen Schritte für die anderen ISL-Ports in der Fabric.

n. Fügen Sie das native VSAN an die Port-Channel-Schnittstelle bei beiden Switches im selben Fabric hinzu:

```
interface port-channel number
```

```
switchport trunk allowed vsan add native_san_id
```

o. Überprüfen Sie die Konfiguration des Port-Kanals:

```
show interface port-channel number
```

Der Port-Kanal sollte die folgenden Attribute aufweisen:

- Der Port-Channel lautet „Trunking“.
- Der Admin-Port-Modus ist E, der Trunk-Modus ist eingeschaltet.
- Die Geschwindigkeit gibt den kumulativen Wert aller ISL-Verbindungsgeschwindigkeiten an.

  Zwei ISL-Ports mit 4 Gbit/s sollten beispielsweise eine Geschwindigkeit von 8 Gbit/s aufweisen.

- `Trunk vsans (admin allowed and active)` Zeigt alle zulässigen VSANs an.
- `Trunk vsans (up)` Zeigt alle zulässigen VSANs an.
- Die Mitgliedsliste zeigt alle ISL-Ports an, die dem Port-Channel hinzugefügt wurden.
- Die Port-Nummer von VSAN sollte mit dem VSAN übereinstimmen, das die ISLs enthält (in der Regel natives vsan 1).

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
    Hardware is Fibre Channel
    Port WWN is 24:01:54:7f:ee:e2:8d:a0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,10,20)
    Trunk vsans (up)                       (1,10,20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
    5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
      535724861 frames input,1069616011292 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      572290295 frames output,1144869385204 bytes
        0 discards,0 errors
      5 input OLS,11  LRR,2 NOS,0 loop inits
      14 output OLS,5 LRR, 0 NOS, 0 loop inits
    Member[1] : fc1/36
    Member[2] : fc1/40
    Interface last changed at Thu Oct 16 11:48:00 2014
```

a. Konfiguration der beenden-Schnittstelle auf beiden Switches:

```
end
```

b. Kopieren Sie die aktualisierte Konfiguration in die Startkonfiguration auf beiden Fabrics:

```
copy running-config startup-config
```

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

a. Wiederholen Sie die vorherigen Schritte auf der zweiten Switch Fabric.

Verwandte Informationen

Sie müssen beim Verkabeln der FC-Switches sicherstellen, dass Sie die angegebenen Portzuweisungen verwenden. Siehe "Portzuweisungen für FC-Switches"

Konfiguration von FCIP-Ports für ein einzelnes ISL auf Cisco 9250i FC-Switches

Sie müssen die FCIP-Switch-Ports konfigurieren, die ISL (E-Ports) verbinden, indem Sie FCIP-Profile und Schnittstellen erstellen und sie dann der IPStorage1/1-GbE-Schnittstelle zuweisen.

Über diese Aufgabe

Diese Aufgabe richtet sich nur an Konfigurationen, die ein einzelnes ISL pro Switch-Fabric verwenden und auf denen die IPStorage1/1-Schnittstelle auf jedem Switch verwendet wird.

Diese Aufgabe muss an jedem FC-Switch ausgeführt werden.

An jedem Switch werden zwei FCIP-Profile erstellt:

- Fabric 1
  - FC_Switch_A_1 ist mit FCIP-Profilen 11 und 111 konfiguriert.
  - FC_Switch_B_1 ist mit FCIP-Profilen 12 und 121 konfiguriert.
- Fabric 2
  - FC_Switch_A_2 ist mit FCIP-Profilen 13 und 131 konfiguriert.
  - FC_Switch_B_2 ist mit FCIP-Profilen 14 und 141 konfiguriert.

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   config t
   ```

2. FCIP aktivieren:

   ```
   feature fcip
   ```

3. Konfigurieren Sie die IPStorage1/1 GbE-Schnittstelle:

   a. Konfigurationsmodus aufrufen:

      ```
      conf t
      ```

   b. Geben Sie die IPStorage1/1-Schnittstelle an:

      ```
      interface IPStorage1/1
      ```

   c. Geben Sie die IP-Adresse und die Subnetzmaske an:

      ```
      interface ip-address subnet-mask
      ```

   d. Geben Sie die MTU-Größe von 2500 an:

      ```
      switchport mtu 2500
      ```

e. Aktivieren Sie den Port:

```
no shutdown
```

f. Konfigurationsmodus beenden:

```
exit
```

Das folgende Beispiel zeigt die Konfiguration eines IPStorage1/1-Ports:

```
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```

4. Konfigurieren Sie das FCIP-Profil für den FC-VI-Datenverkehr:

a. Konfigurieren Sie ein FCIP-Profil, und wechseln Sie in den Konfigurationsmodus für FCIP-Profile:

```
fcip profile FCIP-profile-name
```

Der Profilname hängt davon ab, welcher Switch konfiguriert wird.

b. Weisen Sie die IP-Adresse der IPStorage1/1-Schnittstelle dem FCIP-Profil zu:

```
ip address ip-address
```

c. Weisen Sie das FCIP-Profil dem TCP-Port 3227 zu:

```
port 3227
```

d. Legen Sie die TCP-Einstellungen fest:

```
tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable``no tcp cwm
```

Im folgenden Beispiel wird die Konfiguration des FCIP-Profils angezeigt:

```
conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

5. Konfigurieren Sie das FCIP-Profil für den Speicherdatenverkehr:

   a. Konfigurieren Sie ein FCIP-Profil mit dem Namen 111, und wechseln Sie in den Konfigurationsmodus für das FCIP-Profil:

      ```
      fcip profile 111
      ```

   b. Weisen Sie die IP-Adresse der IPStorage1/1-Schnittstelle dem FCIP-Profil zu:

      ```
      ip address ip-address
      ```

   c. Weisen Sie das FCIP-Profil dem TCP-Port 3229 zu:

      ```
      port 3229
      ```

   d. Legen Sie die TCP-Einstellungen fest:

      ```
      tcp keepalive-timeout 1

      tcp max-retransmissions 3

      max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
      3

      tcp min-retransmit-time 200

      tcp keepalive-timeout 1

      tcp pmtu-enable reset-timeout 3600

      tcp sack-enable``no tcp cwm
      ```

Im folgenden Beispiel wird die Konfiguration des FCIP-Profils angezeigt:

```
conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

6. Erstellen Sie das erste von zwei FCIP-Schnittstellen:

   `interface fcip 1`

   Diese Schnittstelle wird für den FC-IV-Datenverkehr verwendet.

   a. Wählen Sie das zuvor erstellte Profil 11 aus:

      `use-profile 11`

   b. Legen Sie die IP-Adresse und den Port des IPStorage1/1-Ports auf dem Partner-Switch fest:

      `peer-info ipaddr` *`partner-switch-port-ip`* `port 3227`

   c. TCP-Verbindung 2 auswählen:

      `tcp-connection 2`

   d. Komprimierung deaktivieren:

      `no ip-compression`

   e. Aktivieren der Schnittstelle:

      `no shutdown`

   f. Konfigurieren Sie die TCP-Steuerverbindung zu 48 und die Datenverbindung zu 26, um alle Pakete auf diesem differenzierten Service Code Point (DSCP)-Wert zu markieren:

      `qos control 48 data 26`

   g. Beenden Sie den Konfigurationsmodus der Schnittstelle:

      `exit`

   Im folgenden Beispiel wird die Konfiguration der FCIP-Schnittstelle angezeigt:

```
interface fcip  1
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.334   port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. Erstellen Sie das zweite von zwei FCIP-Schnittstellen:

   `interface fcip 2`

   Diese Schnittstelle wird für Storage-Traffic verwendet.

   a. Wählen Sie das zuvor erstellte Profil 111 aus:

      `use-profile 111`

   b. Legen Sie die IP-Adresse und den Port des IPStorage1/1-Ports auf dem Partner-Switch fest:

      `peer-info ipaddr` *`partner-switch-port-ip`* `port 3229`

   c. TCP-Verbindung 2 auswählen:

      `tcp-connection 5`

   d. Komprimierung deaktivieren:

      `no ip-compression`

   e. Aktivieren der Schnittstelle:

      `no shutdown`

   f. Konfigurieren Sie die TCP-Steuerverbindung zu 48 und die Datenverbindung zu 26, um alle Pakete auf diesem differenzierten Service Code Point (DSCP)-Wert zu markieren:

      `qos control 48 data 26`

   g. Beenden Sie den Konfigurationsmodus der Schnittstelle:

      `exit`

   Im folgenden Beispiel wird die Konfiguration der FCIP-Schnittstelle angezeigt:

```
interface fcip  2
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.33e  port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. Konfigurieren Sie die Einstellungen für den Switchport auf der fcip 1-Schnittstelle:
   a. Konfigurationsmodus aufrufen:

      ```
      config t
      ```

   b. Geben Sie den Port an, den Sie konfigurieren:

      ```
      interface fcip 1
      ```

   c. Fahren Sie den Port herunter:

      ```
      shutdown
      ```

   d. Stellen Sie den Port auf E-Modus:

      ```
      switchport mode E
      ```

   e. Aktivieren Sie den Trunk-Modus für den Port:

      ```
      switchport trunk mode on
      ```

   f. Legen Sie den Trunk für das vsan auf 10 fest:

      ```
      switchport trunk allowed vsan 10
      ```

   g. Stellen Sie die Geschwindigkeit für den Port ein:

      `switchport speed` *`speed-value`*

9. Konfigurieren Sie die Einstellungen für den Switchport auf der fcip 2-Schnittstelle:
   a. Konfigurationsmodus aufrufen:

      ```
      config t
      ```

   b. Geben Sie den Port an, den Sie konfigurieren:

      ```
      interface fcip 2
      ```

   c. Fahren Sie den Port herunter:

```
shutdown
```

d. Stellen Sie den Port auf E-Modus:

```
switchport mode E
```

e. Aktivieren Sie den Trunk-Modus für den Port:

```
switchport trunk mode on
```

f. Legen Sie den Trunk für das vsan auf 20 fest:

```
switchport trunk allowed vsan 20
```

g. Stellen Sie die Geschwindigkeit für den Port ein:

```
switchport speed speed-value
```

10. Wiederholen Sie die vorherigen Schritte auf dem zweiten Schalter.

    Die einzigen Unterschiede sind die entsprechenden IP-Adressen und eindeutige FCIP-Profilnamen.

    - Bei der Konfiguration der ersten Switch Fabric wird FC_Switch_B_1 mit FCIP-Profilen 12 und 121 konfiguriert.
    - Bei der Konfiguration der ersten Switch Fabric wird FC_Switch_A_2 mit FCIP-Profilen 13 und 131 konfiguriert und FC_Switch_B_2 mit FCIP-Profilen 14 und 141 konfiguriert.

11. Starten Sie die Ports auf beiden Switches neu:

    ```
    no shutdown
    ```

12. Beenden Sie die Schnittstellenkonfiguration bei beiden Switches:

    ```
    end
    ```

13. Kopieren Sie die aktualisierte Konfiguration auf die Startkonfiguration auf beiden Switches:

    ```
    copy running-config startup-config
    ```

    ```
    FC_switch_A_1(config-if)# end
    FC_switch_A_1# copy running-config startup-config

    FC_switch_B_1(config-if)# end
    FC_switch_B_1# copy running-config startup-config
    ```

14. Wiederholen Sie die vorherigen Schritte auf der zweiten Switch Fabric.

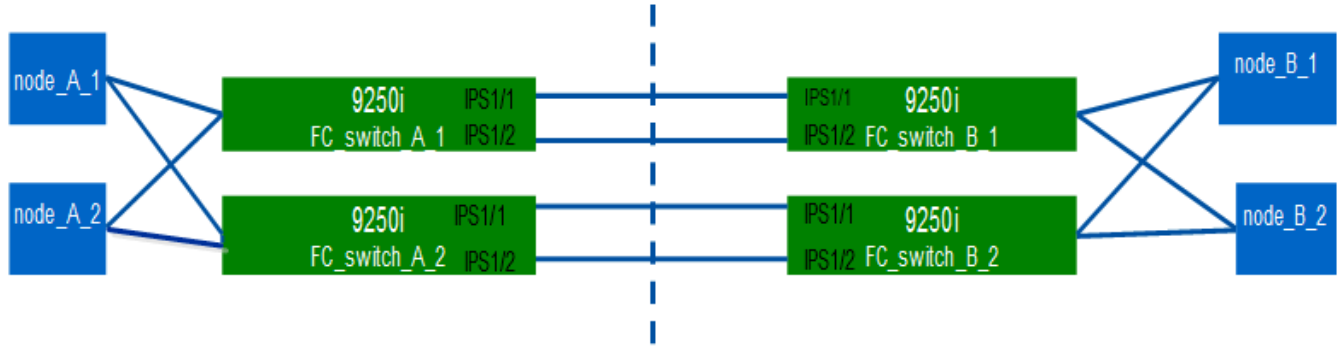
Konfiguration von FCIP-Ports für Dual ISL auf Cisco 9250i FC-Switches

Sie müssen die FCIP-Switch-Ports konfigurieren, die die ISL (E-Ports) verbinden, indem Sie FCIP-Profile und Schnittstellen erstellen und sie dann den IPStorage1/1- und IPStorage1/2-GbE-Schnittstellen zuweisen.

Über diese Aufgabe

Diese Aufgabe gilt nur für Konfigurationen, die ein duales ISL pro Switch-Fabric verwenden und auf jedem Switch die Schnittstellen IPStorage1/1 und IPStorage1/2 GbE verwenden.

Diese Aufgabe muss an jedem FC-Switch ausgeführt werden.



Die Aufgabe und Beispiele verwenden die folgenden Profilkonfigurationstabellen:

- [fabric1_table]
- [fabric2_table]

Tabelle zur Konfiguration des Fabric 1-Profils

Switch-Fabric	IPStorage-Schnittstelle	IP-Adresse	Porttyp	FCIP-Schnittstelle	FCIP-Profil	Port	Peer-IP/Port	VSAN-ID
FC_Switch_A_1	IPStorage 1/1	A.a.a.a.a	FC-VI	fcip 1	15	3220	c.c.c/3230	10
Storage	fcip 2	20	3221	c.c.c/3231	20	IPStorage 1/2	B.b.b.b	FC-VI
fcip 3	25	3222	1. d.d.d.d/3232	10	Storage	fcip 4	30	3223
1. d.d.d.d/3233	20	FC_Switch_B_1	IPStorage 1/1	C.c.c.c	FC-VI	fcip 1	15	3230
1. a. a. A. A. A. A. A./3220	10	Storage	fcip 2	20	3231	1. a. a. A. A. A. A. A./3221	20	IPStorage 1/2

D.d.	FC-VI	fcip 3	25	3232	1. b.b.b.b.b/3222	10	Storage	fcip 4

Tabelle zur Konfiguration des Fabric 2-Profils

Switch-Fabric	IPStorage-Schnittstelle	IP-Adresse	Porttyp	FCIP-Schnittstelle	FCIP-Profil	Port	Peer-IP/Port	VSAN-ID
FC_Switch_A_2	IPStorage 1/1	1. B.	FC-VI	fcip 1	15	3220	g.g.g./3230	10
Storage	fcip 2	20	3221	g.g.g./3231	20	IPStorage 1/2	Fw	FC-VI
fcip 3	25	3222	h.H.H.H.h./h/3232	10	Storage	fcip 4	30	3223
h.H.H.H.h./h/3233	20	FC_Switch_B_2	IPStorage 1/1	G.g.g	FC-VI	fcip 1	15	3230
1. B. e/3220	10	Storage	fcip 2	20	3231	1. B. e/3221	20	IPStorage 1/2
h.h.h.h	FC-VI	fcip 3	25	3232	1. qm: F/3222	10	Storage	fcip 4

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   config t
   ```

2. FCIP aktivieren:

   ```
   feature fcip
   ```

3. Konfigurieren Sie auf jedem Switch die beiden IPStorage-Schnittstellen („`IPStorage1/1`" und „`IPStorage1/2`“):

   a. Konfigurationsmodus eingeben:

      ```
      conf t
      ```

   b. Geben Sie die zu erstellenden IPStorage-Schnittstelle an:

      ```
      interface ipstorage
      ```

      Der *`ipstorage`* Der Parameterwert lautet „`IPStorage1/1`“ oder „`IPStorage1/2`“.

c. Geben Sie die IP-Adresse und die Subnetzmaske der zuvor angegebenen IPStorage-Schnittstelle an:

```
interface ip-address subnet-mask
```

> Auf jedem Switch müssen die IPStorage-Schnittstellen „`IPStorage1/1`“ und „`IPStorage1/2`“ unterschiedliche IP-Adressen haben.

a. Geben Sie die MTU-Größe als 2500 an:

```
switchport mtu 2500
```

b. Aktivieren Sie den Port:

```
no shutdown
```

c. Konfigurationsmodus beenden:

```
exit
```

d. Wiederholen substep „`a`“ Bis substep „`f`“ So konfigurieren Sie die IPStorage1/2 GbE-Schnittstelle mit einer anderen IP-Adresse.

4. Konfigurieren Sie die FCIP-Profile für FC-VI und Storage Traffic mit den Profilnamen, die in der Tabelle der Profilkonfiguration angegeben sind:

a. Konfigurationsmodus aufrufen:

```
conf t
```

b. Konfigurieren Sie die FCIP-Profile mit den folgenden Profilnamen:

```
fcip profile FCIP-profile-name
```

In der folgenden Liste werden die Werte für das aufgeführt *`FCIP-profile-name`* Parameter:

- 15 für FC-VI auf IPStorage1/1
- 20 für Storage auf IPStorage1/1
- 25 für FC-VI auf IPStorage1/2
- 30 für Speicherung auf IPStorage1/2

c. Weisen Sie die FCIP-Profilports gemäß der Profilkonfigurationstabelle zu:

```
port port_number
```

d. Legen Sie die TCP-Einstellungen fest:

```
tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3
```

```
    tcp min-retransmit-time 200

    tcp keepalive-timeout 1

    tcp pmtu-enable reset-timeout 3600

    tcp sack-enable

no tcp cwm
```

5. FCIP-Schnittstellen erstellen:

   ```
   interface fcip FCIP_interface
   ```

   Der *FCIP_interface* Parameterwert ist „1“, „2“, „3“ oder „4“, wie in der Profilkonfigurationstabelle dargestellt.

   a. Schnittstellen zu den zuvor erstellten Profilen zuordnen:

      ```
      use-profile profile
      ```

   b. Legen Sie die Peer-IP-Adresse und die Port-Nummer des Peer-Profils fest:

      ```
      peer-info peer IPstorage ipaddr port peer_profile_port_number
      ```

   c. Wählen Sie die TCP-Verbindungen aus:

      ```
      tcp-connection connection-#
      ```

   Der *connection-#* Der Parameterwert ist „2“ für FC-VI-Profile und „5“ für Storage-Profile.

   a. Komprimierung deaktivieren:

      ```
      no ip-compression
      ```

   b. Aktivieren der Schnittstelle:

      ```
      no shutdown
      ```

   c. Konfigurieren Sie die TCP-Steuerverbindung zu „48“ und die Datenverbindung zu „26“, um alle Pakete zu markieren, die einen differenzierten Service Code Point (DSCP)-Wert haben:

      ```
      qos control 48 data 26
      ```

   d. Konfigurationsmodus beenden:

      ```
      exit
      ```

6. Konfigurieren Sie die Einstellungen für den Switchport auf jeder FCIP-Schnittstelle:

   a. Konfigurationsmodus aufrufen:

      ```
      config t
      ```

b. Geben Sie den Port an, den Sie konfigurieren:

```
interface fcip 1
```

c. Fahren Sie den Port herunter:

```
shutdown
```

d. Stellen Sie den Port auf E-Modus:

```
switchport mode E
```

e. Aktivieren Sie den Trunk-Modus für den Port:

```
switchport trunk mode on
```

f. Geben Sie den Trunk an, der auf einem bestimmten VSAN zulässig ist:

```
switchport trunk allowed vsan vsan_id
```

Der Parameterwert *vsan_id* lautet „`VSAN 10`“ für FC-VI-Profile und „`VSAN 20`“ für Storage-Profile.

a. Stellen Sie die Geschwindigkeit für den Port ein:

```
switchport speed speed-value
```

b. Konfigurationsmodus beenden:

```
exit
```

7. Kopieren Sie die aktualisierte Konfiguration auf die Startkonfiguration auf beiden Switches:

```
copy running-config startup-config
```

Die folgenden Beispiele zeigen die Konfiguration von FCIP-Ports für eine Dual-ISL in Fabric 1-Switches FC_Switch_A_1 und FC_Switch_B_1.

Für FC_Switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  a.a.a.a
```

```
#  Mask:  y.y.y.y
  ip address <a.a.a.a   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit
conf t
fcip profile 15
  ip address <a.a.a.a>
  port 3220
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <a.a.a.a>
  port 3221
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  b.b.b.b
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <b.b.b.b>
  port 3222
```

```
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <b.b.b.b>
  port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3230
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3231
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
```

```
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3232
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3233
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
```

```
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Für FC_Switch_B_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  c.c.c.c
#  Mask:  y.y.y.y
  ip address <c.c.c.c   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 15
  ip address <c.c.c.c>
  port 3230
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
```

```
fcip profile 20
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  d.d.d.d
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
```

```
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3220
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3221
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3222
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3223
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
```

```
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Konfigurieren des Zoning auf einem Cisco FC Switch

Sie müssen die Switch-Ports separaten Zonen zuweisen, um den Storage- (HBA) und Controller-Datenverkehr (FC-VI) zu isolieren.

Über diese Aufgabe

Diese Schritte müssen auf beiden FC Switch Fabrics ausgeführt werden.

Verwenden Sie die folgenden Schritte das im Abschnitt Zoning für eine FibreBridge 7500N in einer

MetroCluster-Konfiguration mit vier Knoten beschriebene Zoning. Siehe "Zoning für FC-VI-Ports".

Schritte

1. Löschen Sie gegebenenfalls die vorhandenen Zonen und den Zonensatz.

   a. Bestimmen Sie, welche Zonen und welche Zonensätze aktiv sind:

   `show zoneset active`

   ```
   FC_switch_A_1# show zoneset active

   FC_switch_B_1# show zoneset active
   ```

   b. Deaktivieren Sie die im vorherigen Schritt identifizierten aktiven Zonensätze:

   `no zoneset activate name zoneset_name vsan vsan_id`

   Im folgenden Beispiel werden zwei Zonensätze angezeigt, die deaktiviert werden:

   - ZoneSet_A on FC_Switch_A_1 in VSAN 10
   - ZoneSet_B on FC_Switch_B_1 in VSAN 20

   ```
   FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10

   FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
   ```

   c. Nachdem alle Zonensätze deaktiviert wurden, löschen Sie die Zonendatenbank:

   `clear zone database zone-name`

   ```
   FC_switch_A_1# clear zone database 10
   FC_switch_A_1# copy running-config startup-config

   FC_switch_B_1# clear zone database 20
   FC_switch_B_1# copy running-config startup-config
   ```

2. Beziehen Sie den Switch Worldwide Name (WWN) ein:

   `show wwn switch`

3. Konfigurieren Sie die grundlegenden Zoneneinstellungen:

   a. Legen Sie die standardmäßige Zoning-Richtlinie auf „`permit`“ fest:

   `no system default zone default-zone permit`

   b. Aktivieren Sie die vollständige Zonenverteilung:

```
system default zone distribute full
```

c. Legen Sie die Standard-Zoning-Richtlinie für jedes VSAN fest:

```
no zone default-zone permit vsanid
```

d. Legen Sie die standardmäßige Vollzonenverteilung für jedes VSAN fest:

```
zoneset distribute full vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

4. Erstellen Sie Storage-Zonen und fügen Sie diesen die Storage-Ports hinzu.

> Führen Sie diese Schritte nur bei einem Switch in jedem Fabric durch.

Das Zoning hängt von der FC-to-SAS-Brücke ab, die Sie verwenden. Weitere Informationen finden Sie im Abschnitt zu Ihrer Modellbrücke. Die Beispiele zeigen Brocade Switch Ports, passen Sie Ihre Ports also entsprechend an.

- "Zoning für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port"
- "Zoning für FibreBridge 7500N-Bridges unter Verwendung beider FC-Ports"

Jede Storage-Zone enthält die HBA-Initiator-Ports von allen Controllern und einen einzelnen Port, der eine FC-to-SAS-Bridge verbindet.

a. Erstellung der Speicherzonen:

```
zone name STOR-zone-name vsan vsanid
```

b. Fügen Sie der Zone Speicherports hinzu:

```
member portswitch WWN
```

c. Aktivieren Sie den Zonensatz:

```
zoneset activate name STOR-zone-name-setname vsan vsan-id
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. Erstellen Sie einen Storage Zone-Satz, und fügen Sie dem neuen Satz die Speicherzonen hinzu.

> Führen Sie diese Schritte nur bei einem Switch in der Fabric aus.

a. Speicherzonensatz erstellen:

```
zoneset name STOR-zone-set-name vsan vsan-id
```

b. Speicherzonen zum Zonensatz hinzufügen:

```
member STOR-zone-name
```

c. Aktivieren Sie den Zonensatz:

```
zoneset activate name STOR-zone-set-name vsan vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Erstellen Sie FCVI-Zonen, und fügen Sie diesen die FCVI-Ports hinzu.

   Jede FCVI-Zone enthält die FCVI-Ports aus allen Controllern einer DR-Gruppe.

   > Führen Sie diese Schritte nur bei einem Switch in der Fabric aus.

   Das Zoning hängt von der FC-to-SAS-Brücke ab, die Sie verwenden. Weitere Informationen finden Sie im Abschnitt zu Ihrer Modellbrücke. Die Beispiele zeigen Brocade Switch Ports, passen Sie Ihre Ports also entsprechend an.

   - "Zoning für FibreBridge 7500N- oder 7600N-Bridges mit einem FC-Port"
   - "Zoning für FibreBridge 7500N-Bridges unter Verwendung beider FC-Ports"

   Jede Storage-Zone enthält die HBA-Initiator-Ports von allen Controllern und einen einzelnen Port, der eine FC-to-SAS-Bridge verbindet.

   a. Erstellen der FCVI-Zonen:

      `zone name` *`FCVI-zone-name`* `vsan` *`vsanid`*

   b. Fügen Sie der Zone FCVI-Ports hinzu:

      `member` *`FCVI-zone-name`*

   c. Aktivieren Sie den Zonensatz:

      `zoneset activate name` *`FCVI-zone-name-set-name`* `vsan` *`vsanid`*

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

7. Erstellen Sie einen FCVI-Zonensatz, und fügen Sie ihm die FCVI-Zonen hinzu:

   Führen Sie diese Schritte nur bei einem Switch in der Fabric aus.

   a. Erstellen Sie den FCVI-Zonensatz:

      `zoneset name FCVI_zone_set_name vsan vsan-id`

   b. Fügen Sie dem Zonensatz FCVI-Zonen hinzu:

      `member FCVI_zonename`

   c. Aktivieren Sie den Zonensatz:

      `zoneset activate name FCVI_zone_set_name vsan vsan-id`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
    ...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

8. Überprüfen Sie das Zoning:

   `show zone`

9. Wiederholen Sie die vorherigen Schritte auf der zweiten FC Switch Fabric.

Sicherstellen, dass die FC-Switch-Konfiguration gespeichert ist

Sie müssen sicherstellen, dass die FC-Switch-Konfiguration auf allen Switches in der Startkonfiguration gespeichert ist.

Schritt

Geben Sie den folgenden Befehl an beiden FC Switch Fabrics ein:

`copy running-config startup-config`

```
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# copy running-config startup-config
```

Installation von FC-to-SAS-Bridges und SAS-Platten-Shelves

Wenn Sie der Konfiguration neuen Speicher hinzufügen, installieren und verkabeln Sie ATTO FibreBridge Bridges und SAS-Platten-Shelves.

Über diese Aufgabe

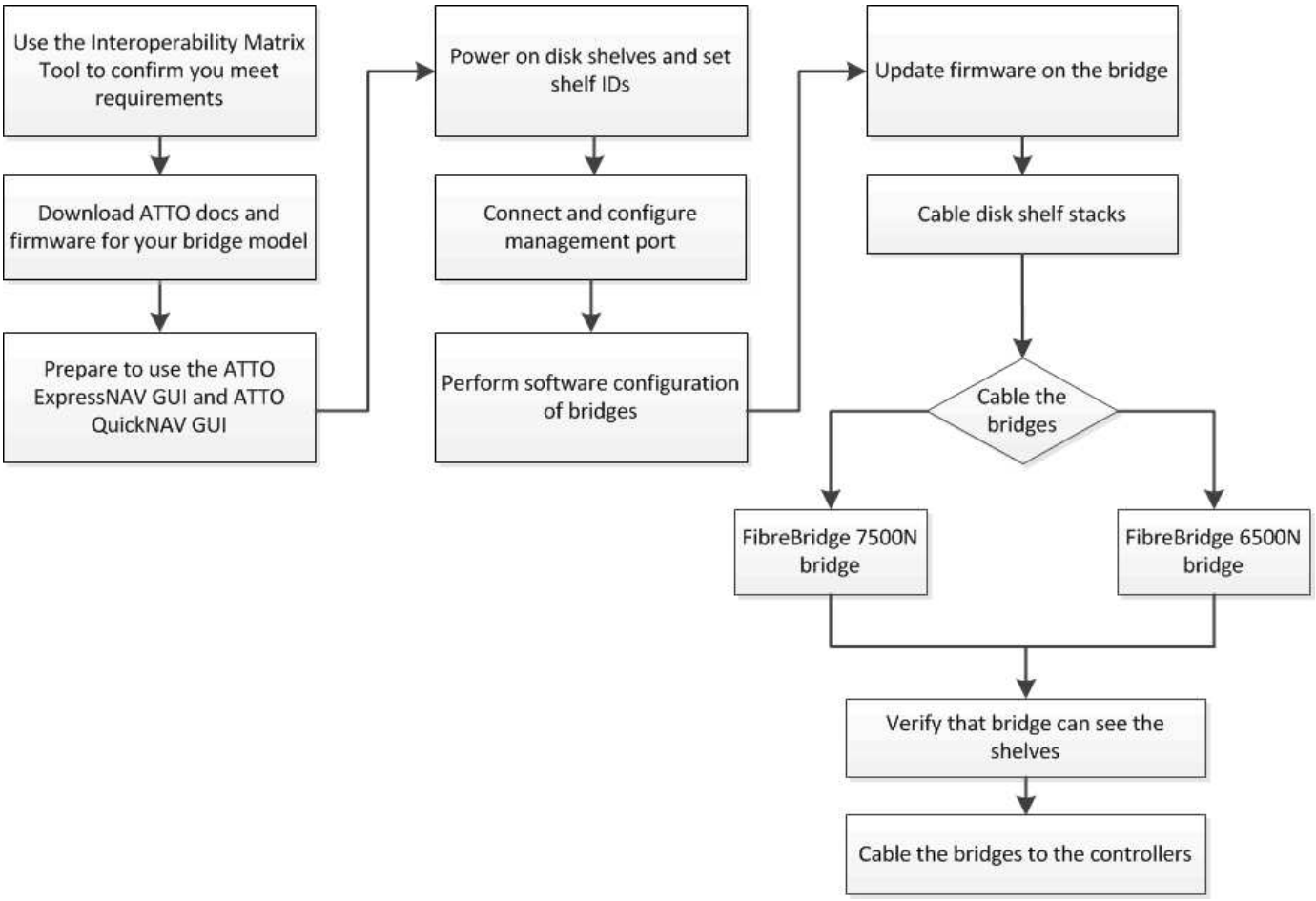
Bei den werkseitig eingegangenen Systemen sind die FC-zu-SAS-Bridges vorkonfiguriert und erfordern keine zusätzliche Konfiguration.

Dieses Verfahren wird mit der Annahme geschrieben, dass Sie die empfohlenen Bridge Management-Schnittstellen verwenden: Die ATTO ExpressNAV GUI und ATTO Quicknav Dienstprogramm.

Sie verwenden die ATTO ExpressNAV GUI, um eine Bridge zu konfigurieren und zu verwalten und die Bridge-Firmware zu aktualisieren. Sie verwenden das ATTO Quicknav Dienstprogramm, um den Bridge Ethernet Management 1 Port zu konfigurieren.

Stattdessen können Sie bei Bedarf andere Managementoberflächen verwenden, z. B. einen seriellen Port oder Telnet, um eine Bridge zu konfigurieren und zu verwalten, den Ethernet Management 1-Port zu konfigurieren und FTP, um die Bridge-Firmware zu aktualisieren.

Bei diesem Verfahren wird folgender Workflow verwendet:



In-Band-Management der FC-to-SAS-Bridges

Ab ONTAP 9.5 mit FibreBridge 7500N oder 7600N Bridges wird *in-Band-Management* der Brücken als Alternative zum IP-Management der Brücken unterstützt. Ab ONTAP 9.8 ist das Out-of-Band-Management veraltet.

> 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.

Bei Verwendung der in-Band-Verwaltung können die Brücken über die FC-Verbindung zur Bridge von der ONTAP-CLI verwaltet und überwacht werden. Der physische Zugriff auf die Bridge über die Bridge-Ethernet-Ports ist nicht erforderlich, wodurch die Sicherheitslücke der Bridge verringert wird.

Die Verfügbarkeit der in-Band-Verwaltung der Brücken hängt von der Version von ONTAP ab:

- Ab ONTAP 9.8 werden Brücken standardmäßig über in-Band-Verbindungen verwaltet und die Out-of-Band-Verwaltung der Brücken über SNMP ist veraltet.
- ONTAP 9.5 bis 9.7: Entweder in-Band-Management oder Out-of-Band-SNMP-Management wird unterstützt.
- Vor ONTAP 9.5 wird nur bandexterne SNMP-Verwaltung unterstützt.

Bridge-CLI-Befehle können über die ONTAP-Schnittstelle ausgegeben werden `storage bridge run-cli -name` *`bridge_name`* `-command` *`bridge_command_name`* Befehl über die ONTAP-Schnittstelle.

Die Verwendung der bandinternen Verwaltung mit deaktiviertem IP-Zugriff wird empfohlen, um die Sicherheit zu verbessern, indem die physische Konnektivität zur Bridge eingeschränkt wird.

FiberBridge 7600N und 7500N Brückengrenzen und Befestigungsregeln

Überprüfen Sie die Grenzwerte und Überlegungen beim Anbringen von FibreBridge 7600N- und 7500N-Brücken.

Grenzwerte für FibreBridge 7600N und 7500N-Brücken

- Die maximale Anzahl der kombinierten HDD- und SSD-Laufwerke beträgt 240.
- Die maximale Anzahl von SSD-Laufwerken beträgt 96.
- Es sind maximal 48 SSDs pro SAS-Port zulässig.
- Die maximale Anzahl von Shelfs pro SAS-Port ist 10.

Befestigungsregeln für FibreBridge 7600N und 7500N

- Verwenden Sie keine SSD- und HDD-Laufwerke zusammen am selben SAS-Port.
- Verteilen Sie die Shelfs gleichmäßig über die SAS-Ports.
- Sie sollten DS460 Shelfs nicht auf demselben SAS Port wie andere Shelf-Typen (z. B. DS212 oder DS224 Shelfs) einsetzen.

Beispielkonfiguration

Im Folgenden ist eine Beispielkonfiguration zum Anschluss von vier DS224-Shelfs mit SSD-Laufwerken und sechs DS224-Shelfs mit HDD-Laufwerken dargestellt:

SAS-Port	Shelfs und Laufwerke
SAS Port-A	2 DS224-Shelfs mit SSD-Laufwerken
SAS-Port-B	2 DS224-Shelfs mit SSD-Laufwerken
SAS-Port-C	3x DS224-Shelfs mit HDD-Laufwerken
SAS-Port-D	3x DS224-Shelfs mit HDD-Laufwerken

Bereiten Sie die Installation vor

Wenn Sie die Installation der Brücken als Teil Ihres neuen MetroCluster-Systems vorbereiten, müssen Sie sicherstellen, dass Ihr System bestimmte Anforderungen erfüllt, einschließlich der Erfüllung von Setup- und Konfigurationsanforderungen für die Brücken. Weitere Anforderungen sind das Herunterladen der erforderlichen Dokumente, das Dienstprogramm ATTO Quicknav und die Bridge-Firmware.

Bevor Sie beginnen

- Das System muss bereits in einem Rack installiert sein, wenn es nicht in einem Systemschrank ausgeliefert wurde.
- Ihre Konfiguration muss unterstützte Hardware-Modelle und Software-Versionen verwenden.

  Im "NetApp Interoperabilitäts-Matrix-Tool (IMT)", Sie können im Feld Storage-Lösung die MetroCluster-Lösung auswählen. 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.

- Jeder FC-Switch muss über einen FC-Port verfügen, damit eine Bridge mit ihm verbunden werden kann.
- Sie müssen sich vertraut machen mit dem Umgang mit SAS-Kabeln und den Überlegungen und Best Practices für die Installation und Verkabelung von Platten-Shelves.

  Das Handbuch „ *Installation and Service Guide*“ für Ihr Festplatten-Shelf-Modell beschreibt die Überlegungen und Best Practices.

- Der Computer, mit dem Sie die Brücken einrichten, muss einen ATTO-unterstützten Webbrowser betreiben, um die ATTO ExpressNAV GUI nutzen zu können.

  Die *ATTO Product Release Notes* verfügen über eine aktuelle Liste der unterstützten Webbrowser. Sie können auf dieses Dokument über die ATTO-Website zugreifen, wie in den folgenden Schritten beschrieben.

Schritte

1. Laden Sie das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell herunter:
   a. Greifen Sie über den Link Ihres FibreBridge-Modells auf die ATTO-Website zu, und laden Sie das Handbuch und das Quicknav-Dienstprogramm herunter.

   > Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihre Modellbrücke enthält weitere Informationen zu Management-Schnittstellen.
   >
   > Sie können auf diesen und andere Inhalte auf der ATTO-Website zugreifen, indem Sie den Link auf der ATTO FibreBridge-Beschreibungsseite verwenden.

2. Sammeln Sie die Hardware und Informationen, die benötigt werden, um die empfohlenen Bridge Management-Schnittstellen, die ATTO ExpressNAV GUI und das ATTO Quicknav Dienstprogramm zu verwenden:
   a. Legen Sie einen nicht standardmäßigen Benutzernamen und ein Kennwort fest (für den Zugriff auf die Brücken).

      Sie sollten den Standardbenutzernamen und das Standardpasswort ändern.

   b. Bei der Konfiguration für die IP-Verwaltung der Brücken benötigen Sie das abgeschirmte Ethernet-Kabel mit den Brücken (das vom Bridge Ethernet Management 1-Port mit Ihrem Netzwerk verbunden wird).
   c. Wenn Sie für das IP-Management der Brücken konfigurieren, benötigen Sie eine IP-Adresse, eine Subnetzmaske und Gateway-Informationen für den Ethernet-Management-Port 1 auf jeder Bridge.
   d. Deaktivieren Sie VPN-Clients auf dem Computer, den Sie für die Einrichtung verwenden.

      Aktive VPN-Clients führen zum Fehlschlagen des Quicknav-Scans für Brücken.

Installieren Sie die FC-to-SAS-Bridge und die SAS-Shelfs

Nachdem Sie sichergestellt haben, dass das System alle Anforderungen in „`Vorbereitung auf die Installation`“ erfüllt, können Sie Ihr neues System installieren.

Über diese Aufgabe

- Die Festplatten- und Shelf-Konfiguration an beiden Standorten sollte identisch sein.

  Wenn ein nicht gespiegeltes Aggregat verwendet wird, kann die Festplatten- und Shelf-Konfiguration an

jedem Standort unterschiedlich sein.

> Alle Festplatten in der Disaster Recovery-Gruppe müssen denselben Verbindungstyp verwenden und für alle Nodes innerhalb der Disaster Recovery-Gruppe sichtbar sein. Dabei spielt es keine Rolle, welche Festplatten für ein gespiegeltes oder nicht gespiegeltes Aggregat verwendet werden.

- Die Anforderungen an die Systemkonnektivität für maximale Entfernungen von Platten-Shelfs, FC-Switches und Backup-Bandgeräten mit 50-Mikron- und Multimode-Glasfaserkabeln gelten auch für FibreBridge-Brücken.

  "NetApp Hardware Universe"

- Eine Kombination aus IOM12-Modulen und IOM3-Modulen wird im selben Storage-Stack nicht unterstützt. Wenn auf dem System eine unterstützte Version von ONTAP ausgeführt wird, wird im selben Storage Stack eine Kombination aus IOM12-Modulen und IOM6-Modulen unterstützt.

> In-Band ACP wird ohne zusätzliche Verkabelung in den folgenden Shelves und FibreBridge 7500N oder 7600N Bridge unterstützt:
>
> - IOM12 (DS460C) hinter einer 7500N bzw. 7600N Brücke mit ONTAP 9.2 und höher
> - IOM12 (DS212C und DS224C) hinter einer 7500N oder 7600N Brücke mit ONTAP 9.1 und höher

> SAS-Shelves in MetroCluster-Konfigurationen unterstützen keine ACP-Verkabelung.

Aktivieren Sie ggf. den IP-Port-Zugriff auf die FibreBridge 7600N-Brücke

Wenn Sie eine ONTAP-Version vor 9.5 verwenden oder anderweitig planen, Out-of-Band-Zugriff auf die FibreBridge 7600N-Brücke über Telnet oder andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) zu nutzen, können Sie die Zugriffsservices über den Konsolen-Port aktivieren.

Über diese Aufgabe

Im Gegensatz zu den ATTO FibreBridge 7500N Bridges wird die FibreBridge 7600N mit deaktivierten IP-Port-Protokollen und -Diensten ausgeliefert.

Ab ONTAP 9.5 wird *in-Band-Management* der Brücken unterstützt. Das bedeutet, dass die Brücken über die FC-Verbindung zur Bridge von der ONTAP-CLI konfiguriert und überwacht werden können. Physischer Zugang zur Bridge über die Bridge-Ethernet-Ports ist nicht erforderlich und die Bridge-Benutzeroberflächen sind nicht erforderlich.

Ab ONTAP 9.8 wird *in-Band-Management* der Bridges standardmäßig unterstützt und out-of-Band SNMP-Management ist veraltet.

Diese Aufgabe ist erforderlich, wenn Sie zur Verwaltung der Brücken * nicht* verwenden. In diesem Fall müssen Sie die Bridge über den Ethernet-Management-Port konfigurieren.

Schritte

1. Greifen Sie auf die Konsolenschnittstelle der Bridge zu, indem Sie ein serielles Kabel an den seriellen Port der FibreBridge 7600N-Brücke anschließen.
2. Aktivieren Sie die Zugriffsservices über die Konsole, und speichern Sie die Konfiguration:

```
set closeport none
```

```
saveconfiguration
```

Der `set closeport none` Befehl aktiviert alle Zugriffsservices auf der Bridge.

3. Deaktivieren Sie ggf. einen Dienst, indem Sie den ausstellen `set closeport` Befehl und Wiederholung des Befehls nach Bedarf, bis alle gewünschten Dienste deaktiviert sind:

   ```
   set closeport service
   ```

   Der `set closeport` Durch den Befehl wird ein einzelner Dienst gleichzeitig deaktiviert.

   Der Parameter *`service`* Kann wie folgt angegeben werden:

   - expressnav
   - ftp
   - icmp
   - quicknav
   - snmp
   - telnet

   Sie können mithilfe der überprüfen, ob ein bestimmtes Protokoll aktiviert oder deaktiviert ist `get closeport` Befehl.

4. Wenn Sie SNMP aktivieren, müssen Sie auch folgenden Befehl ausgeben:

   ```
   set SNMP enabled
   ```

   SNMP ist das einzige Protokoll, das einen separaten Enable-Befehl erfordert.

5. Konfiguration speichern:

   ```
   saveconfiguration
   ```

Konfigurieren Sie die FC-zu-SAS-Bridges

Bevor Sie das Modell der FC-zu-SAS-Brücken verkabeln, müssen Sie die Einstellungen in der FibreBridge-Software konfigurieren.

Bevor Sie beginnen

Sie sollten entscheiden, ob Sie die bandinterne Verwaltung der Brücken verwenden.

> 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.

Über diese Aufgabe

Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den

entsprechenden Schritten angegeben.

Schritte

1. Konfigurieren Sie den seriellen Konsolenport auf der ATTO FibreBridge, indem Sie die Portgeschwindigkeit auf 115000 Bauds einstellen:

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

   Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.

3. Wenn Sie die IP-Verwaltung konfigurieren, schließen Sie den Ethernet-Management-1-Port an jeder Bridge über ein Ethernet-Kabel an das Netzwerk an.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Der Ethernet Management 1 Port ermöglicht es Ihnen, schnell die Bridge-Firmware (über ATTO ExpressNAV oder FTP Management-Schnittstellen) herunterzuladen und Core-Dateien und Extrahieren von Logs abzurufen.

4. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

5. Konfigurieren Sie die Bridge.

   Notieren Sie sich den Benutzernamen und das Kennwort, den Sie bestimmen.

> Konfigurieren Sie die Zeitsynchronisierung auf ATTO FibreBridge 7600N oder 7500N nicht. Die Zeitsynchronisierung für ATTO FibreBridge 7600N oder 7500N ist auf die Cluster-Zeit eingestellt, nachdem die Brücke von ONTAP erkannt wurde. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle Verbindung mit der FibreBridge.

   Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

   ```
   set ipaddress mp1 ip-address

   set ipsubnetmask mp1 subnet-mask

   set ipgateway mp1 x.x.x.x

   set ipdhcp mp1 disabled

   set ethernetspeed mp1 1000
   ```

b. Konfigurieren Sie den Brückennamen.

   Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

   Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

   - Bridge_A_1a
   - Bridge_A_1b
   - Bridge_B_1a
   - Bridge_B_1b

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set bridgename bridge_name
   ```

c. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:

   ```
   set SNMP enabled
   ```

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

6. Konfigurieren Sie die Bridge-FC-Ports.

a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

   Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

   - Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
   - Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.

   > Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch vom FC-Port des Controller-Moduls unterstützt wird, mit dem der Bridge-Port verbunden wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set FCDataRate <port-number> <port-speed>
   ```

b. Wenn Sie eine FibreBridge 7500N-Bridge konfigurieren, konfigurieren Sie den Verbindungsmodus, den der Port für „ptp“ verwendet.

   > Die Einstellung FCConnMode ist nicht erforderlich, wenn Sie eine FibreBridge 7600N-Bridge konfigurieren.

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set FCConnMode <port-number> ptp
   ```

c. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, müssen Sie den FC2-Port konfigurieren oder deaktivieren.

   - Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
   - Wenn Sie den zweiten Port nicht verwenden, müssen Sie den Port deaktivieren:

     ```
     FCPortDisable <port-number>
     ```

   Im folgenden Beispiel wird die Deaktivierung von FC-Port 2 gezeigt:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, deaktivieren Sie die nicht verwendeten SAS-Ports:

   ```
   SASPortDisable sas-port
   ```

   > SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren.

Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein. Im folgenden Beispiel wird die Deaktivierung von SAS Port B gezeigt Sie müssen die SAS-Ports C und D ähnlich deaktivieren:

```
SASPortDisable b

SAS Port B has been disabled.
```

7. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration. Wählen Sie je nach Version des ONTAP, auf dem Ihr System ausgeführt wird, eine der folgenden Optionen aus.

ONTAP-Version	Schritte

ONTAP 9.5 oder höher	a. Den Status der Brücken anzeigen:
	`storage bridge show`
	Der Ausgang zeigt an, welche Brücke nicht gesichert ist.
	b. Sichern Sie die Brücke:
	`securebridge`

ONTAP 9.4 oder früher	a. Den Status der Brücken anzeigen:
	
	`storage bridge show`
	
	Der Ausgang zeigt an, welche Brücke nicht gesichert ist.
	
	b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:
	
	`info`
	
	Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.
	
	c. Wenn Ethernet-Port MP1 aktiviert ist, führen Sie folgende Schritte aus:
	
	`set EthernetPort mp1 disabled`
	
	Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.
	
	d. Die Konfiguration der Bridge speichern.
	
	Sie müssen die folgenden Befehle ausführen:
	
	`SaveConfiguration`
	
	`FirmwareRestart`
	
	Sie werden aufgefordert, die Bridge neu zu starten.

8. Verwenden Sie nach Abschluss der MetroCluster-Konfiguration das `flashimages` Befehl zum Überprüfen der Version der FibreBridge-Firmware und, wenn die Brücken nicht die neueste unterstützte Version verwenden, aktualisieren Sie die Firmware auf allen Brücken in der Konfiguration.

   "Warten von MetroCluster-Komponenten"

Verkabeln Sie die Platten-Shelfs mit den Bridges

Für die Verkabelung Ihrer Platten-Shelves müssen die richtigen FC-to-SAS-Bridges verwendet werden.

Wahlmöglichkeiten

- Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM12-Modulen
- Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM6- oder IOM3-Modulen

Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM12-Modulen

Nach der Konfiguration der Bridge können Sie mit der Verkabelung Ihres neuen Systems beginnen.

Über diese Aufgabe

Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche.

Schritte

1. Schalten Sie die Festplatten-Shelfs in den einzelnen Stacks in Reihe:

   a. Beginnend mit dem logischen ersten Shelf im Stack verbinden Sie IOM A-Port 3 mit IOM A-Port 1 im nächsten Shelf, bis jedes IOM A im Stack verbunden ist.

   b. Wiederholen Sie den vorherigen Unterschritt für IOM B.

   c. Wiederholen Sie die vorherigen Unterschritte für jeden Stack.

   Das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell bietet detaillierte Informationen zum Verketten von Platten-Shelfs in Reihe.

2. Schalten Sie die Festplatten-Shelfs ein und legen Sie dann 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.

3. Verkabeln Sie die Platten-Shelves mit den FibreBridge Bridges.

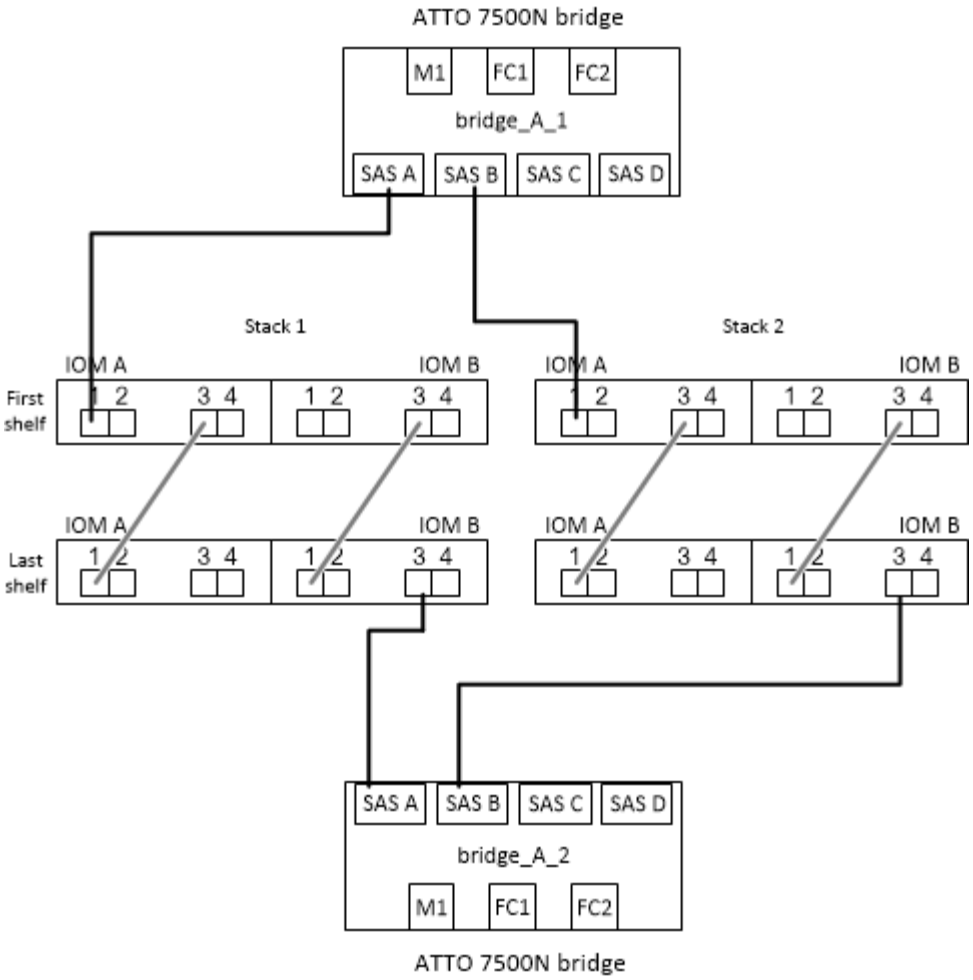
   a. Verkabeln Sie für den ersten Stack der Festplatten-Shelfs IOM A des ersten Shelfs zu SAS-Port A auf FibreBridge A und verkabeln Sie IOM B des letzten Shelfs zum SAS-Port A auf FibreBridge B

   b. Wiederholen Sie für weitere Shelf-Stacks den vorherigen Schritt mit dem nächsten verfügbaren SAS-Port der FibreBridge-Brücken, wobei Port B für den zweiten Stack, Port C für den dritten Stack und Port D für den vierten Stack verwendet wird.

   c. Schließen Sie während der Verkabelung die auf IOM12- und IOM3-/IOM6-Modulen basierenden Stacks an dieselbe Bridge an, solange sie mit separaten SAS-Ports verbunden sind.

   > Jeder Stack kann unterschiedliche IOM-Modelle verwenden. Alle Festplatten-Shelfs in einem Stack müssen jedoch dasselbe Modell verwenden.

   Die folgende Abbildung zeigt die mit einem Paar FibreBridge 7600N- oder 7500N-Brücken verbundenen Platten-Shelves:



Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Shelfs mit IOM6- oder IOM3-Modulen

Nach der Konfiguration der Bridge können Sie mit der Verkabelung Ihres neuen Systems beginnen. Die FibreBridge 7600N oder 7500N Bridge nutzt Mini-SAS-Anschlüsse und unterstützt Shelfs, die IOM6- oder IOM3-Module verwenden.

Über diese Aufgabe

IOM3-Module werden von FibreBridge 7600N-Brücken nicht unterstützt.

Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche.

Schritte

1. Schalten Sie die Regale in den einzelnen Stapeln in Reihe.

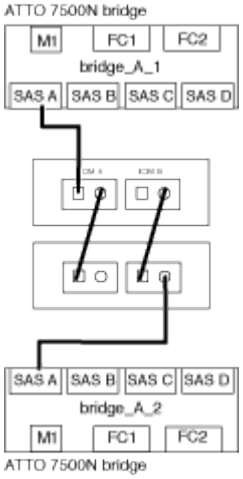
    a. Verkabeln Sie beim ersten Stapel von Shelves IOM Einen quadratischen Port des ersten Shelfs zu SAS-Port A auf FibreBridge A

    b. Verkabeln Sie für den ersten Stapel von Shelves IOM B-Kreis-Port des letzten Shelfs zu SAS-Port A auf FibreBridge B.

    Das *Installation and Service Guide* für Ihr Shelf-Modell enthält detaillierte Informationen zum Verketten von Shelfs.

    "Installation und Service Guide für SAS-Platten-Shelfs für DS4243, DS2246, DS4486 und DS4246"

Die folgende Abbildung zeigt eine Reihe von Brücken, die mit einem Regal verbunden sind:



2. Wiederholen Sie für weitere Shelf-Stacks die vorherigen Schritte mithilfe des nächsten verfügbaren SAS-Ports der FibreBridge-Brücken, wobei Port B für einen zweiten Stack, Port C für einen dritten Stack und Port D für einen vierten Stack verwendet wird.

   Die folgende Abbildung zeigt vier Stapel, die mit einem Paar FibreBridge 7600N oder 7500N-Brücken verbunden sind.

Überprüfen Sie die Bridge-Konnektivität und verkabeln Sie die Bridge-FC-Ports

Sie sollten überprüfen, ob jede Bridge alle Festplattenlaufwerke erkennen kann, und jede Bridge mit den lokalen FC-Switches verkabeln.

Schritte

1. Prüfen Sie, ob jede Bridge alle Festplattenlaufwerke und Platten-Shelfs erkennen kann, mit denen sie verbunden ist:

Wenn Sie den…	Dann…
ATTO ExpressNAV GUI	a. Geben Sie in einem unterstützten Webbrowser die IP-Adresse einer Bridge in das Browserfenster ein. Sie werden auf die ATTO FibreBridge Homepage der Brücke gebracht, für die Sie die IP-Adresse eingegeben haben, die einen Link hat. b. Klicken Sie auf den Link, und geben Sie dann Ihren Benutzernamen und das Passwort ein, das Sie beim Konfigurieren der Bridge festgelegt haben. Die ATTO FibreBridge-Statusseite der Brücke wird mit einem Menü links angezeigt. c. Klicken Sie Auf **Erweitert**. d. Zeigen Sie die angeschlossenen Geräte mit dem Befehl sastargets an, und klicken Sie dann auf **Senden**.

Serieller Anschluss	Anzeigen der angeschlossenen Geräte: `sastargets`

Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können. Die folgende Ausgabe zeigt beispielsweise, dass 10 Festplatten verbunden sind:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

Wenn der Text “response cumpfed” am Anfang der Ausgabe erscheint, können Sie Telnet verwenden, um eine Verbindung zur Bridge herzustellen und den gleichen Befehl einzugeben, um die gesamte Ausgabe anzuzeigen.

2. Überprüfen Sie, ob die Befehlsausgabe zeigt, dass die Bridge mit allen Festplatten und Festplatten-Shelfs im Stack verbunden ist, mit denen die Verbindung hergestellt werden soll.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Schritt 1 Für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie, ob sich lose SAS-Kabel befinden oder korrigieren Sie die SAS-Verkabelung, indem Sie die Verkabelung wiederholen. Verkabeln Sie die Platten-Shelfs mit den Bridges b. Wiederholen Schritt 1.

3. Verkabeln Sie jede Bridge mit den lokalen FC-Switches. Verwenden Sie dabei die in der Tabelle vorhandenen Kabel für Ihr Konfigurations- und Switch-Modell und das FC-to-SAS-Bridge-Modell:

Die zweite FC-Port-Verbindung auf der FibreBridge 7500N-Brücke sollte erst nach Abschluss des Zoning verkabelt werden.

Weitere Informationen finden Sie in den Portzuweisungen für Ihre Version von ONTAP.

4. Wiederholen Sie den vorherigen Schritt auf den Brücken am Partnerstandort.

Verwandte Informationen

Sie müssen beim Verkabeln der FC-Switches sicherstellen, dass Sie die angegebenen Portzuweisungen verwenden.

"Portzuweisungen für FC-Switches"

Sichern oder unsichern Sie die FibreBridge-Brücke

Um potenziell unsichere Ethernet-Protokolle auf einer Bridge einfach zu deaktivieren, können Sie ab ONTAP 9.5 die Bridge sichern. Dadurch werden die Ethernet-Ports der Bridge deaktiviert. Sie können auch den Ethernet-Zugriff erneut aktivieren.

Über diese Aufgabe

- Durch das Sichern der Brücke werden Telnet und andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) auf der Brücke deaktiviert.
- Bei diesem Verfahren wird die Out-of-Band-Verwaltung mithilfe der ONTAP-Eingabeaufforderung verwendet, die ab ONTAP 9.5 verfügbar ist.

  Sie können die Befehle aus der Bridge-CLI ausgeben, wenn Sie keine Out-of-Band-Verwaltung verwenden.

- Der `unsecurebridge` Mit dem Befehl können die Ethernet-Ports wieder aktiviert werden.
- In ONTAP 9.7 und früher, Ausführen der `securebridge` Durch den Befehl auf der ATTO FibreBridge wird der Bridge-Status auf dem Partner-Cluster möglicherweise nicht korrekt aktualisiert. Führen Sie in diesem Fall den aus `securebridge` Befehl aus dem Partner-Cluster.

> 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. Sichern Sie die Bridge an der ONTAP-Eingabeaufforderung des Clusters mit der Bridge oder unsichern Sie sie.
   - Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
     ```

   - Mit dem folgenden Befehl wird Bridge_A_1 aufgehoben:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
     ```

2. Speichern Sie in der ONTAP-Eingabeaufforderung des Clusters, der die Bridge enthält, die Bridge-Konfiguration:

   ```
   storage bridge run-cli -bridge bridge-name -command saveconfiguration
   ```

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. Starten Sie an der ONTAP-Eingabeaufforderung des Clusters, das die Bridge enthält, die Firmware der Bridge neu:

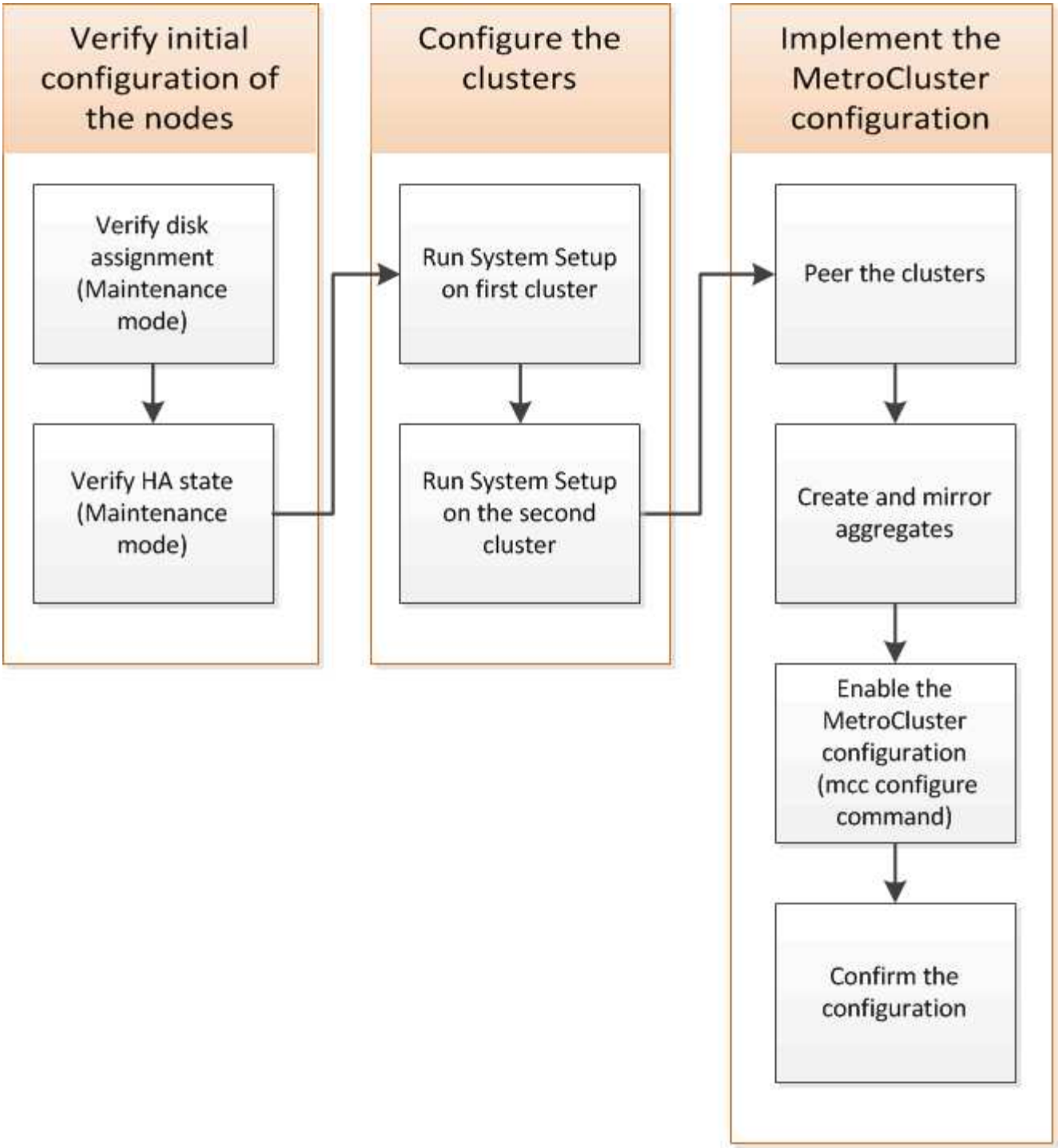
   ```
   storage bridge run-cli -bridge bridge-name -command firmwarerestart
   ```

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
   ```

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.



Sammeln der erforderlichen Informationen

Sie müssen die erforderlichen IP-Adressen für die Controller-Module erfassen, bevor Sie mit dem Konfigurationsprozess beginnen.

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.

Switch-Informationen Standort A (Switch-Cluster)

Wenn Sie das System verkabeln, benötigen Sie für jeden Cluster-Switch einen Host-Namen und eine Management-IP-Adresse. Diese Informationen sind nicht erforderlich, wenn Sie ein 2-Node-Cluster ohne Switches oder eine MetroCluster Konfiguration mit zwei Nodes (ein Node an jedem Standort) verwenden.

Cluster-Switch	Host-Name	IP-Adresse	Netzwerkmaske	Standard-Gateway
Verbindung 1				
Verbindung 2				
Management 1				
Management 2				

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, das in diesem Handbuch verwendet wird: 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 für dieses Handbuch: Controller_A_1				

Knoten 2 Nicht erforderlich, wenn eine MetroCluster Konfiguration mit zwei Nodes verwendet wird (ein Node an jedem Standort). Beispiel für dieses Handbuch: 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				
Knoten 2 IC LIF 1 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)				
Node 2 IC LIF 2 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)				

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	

Standort A 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			
Knoten 2 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)			

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.

Switch-Informationen an Standort B (Switch-Cluster)

Wenn Sie das System verkabeln, benötigen Sie für jeden Cluster-Switch einen Host-Namen und eine Management-IP-Adresse. Diese Informationen sind nicht erforderlich, wenn Sie ein 2-Node-Cluster ohne Switches oder eine MetroCluster Konfiguration mit zwei Nodes (ein Node an jedem Standort) verwenden.

Cluster-Switch	Host-Name	IP-Adresse	Netzwerkmaske	Standard-Gateway
Verbindung 1				
Verbindung 2				
Management 1				
Management 2				

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 dieses Handbuch: 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 In diesem Handbuch verwendetes Beispiel: Controller_B_1				

Knoten 2 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort) In diesem Handbuch verwendetes Beispiel: 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				
Knoten 2 IC LIF 1 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)				
Node 2 IC LIF 2 Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)				

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
	Partner	

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)			
Knoten 2 (Controller_B_2) Nicht erforderlich für MetroCluster Konfigurationen mit zwei Nodes (ein Node an jedem Standort)			

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	
Konfigurieren Sie Nodes im Cluster als HA-Paare	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	Nicht zutreffend	Erforderlich

Überprüfen und Konfigurieren des HA-Status von Komponenten im Wartungsmodus

Wenn Sie ein Speichersystem in einer MetroCluster FC-Konfiguration konfigurieren, müssen Sie sicherstellen, dass der Hochverfügbarkeitsstatus (HA) des Controller-Moduls und der Gehäusekomponenten mcc oder mcc-2n ist, damit diese Komponenten ordnungsgemäß booten. Obwohl dieser Wert auf werkseitig empfangene Systeme vorkonfiguriert sein sollte, sollten Sie die Einstellung dennoch überprüfen, bevor Sie fortfahren.

> Wenn der HA-Status des Controller-Moduls und des Chassis falsch ist, können Sie die MetroCluster nicht konfigurieren, ohne den Node neu zu initialisieren. Sie müssen die Einstellung mit diesem Verfahren korrigieren und dann das System mit einem der folgenden Verfahren initialisieren:
>
> - Führen Sie in einer MetroCluster IP-Konfiguration die Schritte in "Systemstandardwerte auf einem Controller-Modul wiederherstellen"aus.
> - Führen Sie in einer MetroCluster FC-Konfiguration die Schritte in "Stellen Sie die Systemstandardeinstellungen wieder her und konfigurieren Sie den HBA-Typ auf einem Controller-Modul"aus.

Bevor Sie beginnen

Vergewissern Sie sich, dass sich das System im Wartungsmodus befindet.

Schritte

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

```
ha-config show
```

Der richtige HA-Status hängt von Ihrer MetroCluster-Konfiguration ab.

MetroCluster-Konfigurationstyp	HA-Status für alle Komponenten…
MetroCluster FC-Konfiguration mit acht oder vier Nodes	mcc
MetroCluster FC-Konfiguration mit zwei Nodes	mcc-2n
MetroCluster IP-Konfiguration mit acht oder vier Nodes	Mccip

2. Wenn der angezeigte Systemstatus des Controllers nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Controller-Modul fest:

MetroCluster-Konfigurationstyp	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify controller mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mccip`

3. Wenn der angezeigte Systemstatus des Chassis nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Chassis fest:

MetroCluster-Konfigurationstyp	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify chassis mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mccip`

4. Booten des Node zu ONTAP:

```
boot_ontap
```

5. Wiederholen Sie dieses gesamte Verfahren, um den HA-Status auf jedem Node in der MetroCluster-Konfiguration zu überprüfen.

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

Über diese Aufgabe

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 acht oder vier Nodes

Vor dem vollständigen Booten des Systems zu ONTAP können Sie optional im Wartungsmodus booten und die Festplattenzuordnung auf den Nodes überprüfen. Die Laufwerke sollten einer vollständig symmetrischen aktiv/aktiv-Konfiguration zugewiesen werden, wobei jeder Pool eine gleiche Anzahl von Laufwerken zugewiesen hat.

Über diese Aufgabe

Neue MetroCluster Systeme haben vor dem Versand eine Festplattenzuordnung abgeschlossen.

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

Platten-Shelves an Standort A

Festplatten-Shelf (sample_Shelf_Name)…	Gehört zu…	Und ist diesem Node zugewiesen…
Festplatten-Shelf 1 (Shelf_A_1_1)	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)		
Platten-Shelf 5 (Shelf_A_2_1)	Knoten A 2	Pool 0
Platten-Shelf 6 (Shelf_A_2_3)		
Festplatten-Shelf 7 (Shelf_B_2_1)	Knoten B 2	Pool 1
Festplatten-Shelf 8 (Shelf_B_2_3)		
Platten-Shelf 1 (Shelf_A_3_1)	Knoten A 3	Pool 0
Festplatten-Shelf 2 (Shelf_A_3_3)		

Festplatten-Shelf 3 (Shelf_B_3_1)	Knoten B 3	Pool 1
Festplatten-Shelf 4 (Shelf_B_3_3)		
Platten-Shelf 5 (Shelf_A_4_1)	Knoten A 4	Pool 0
Platten-Shelf 6 (Shelf_A_4_3)		
Festplatten-Shelf 7 (Shelf_B_4_1)	Knoten B 4	Pool 1
Festplatten-Shelf 8 (Shelf_B_4_3)		

Platten-Shelves an Standort B

Festplatten-Shelf (sample_Shelf_Name)…	Gehört zu…	Und ist diesem Node zugewiesen…
Festplatten-Shelf 9 (Shelf_B_1_2)	Knoten B 1	Pool 0
Festplatten-Shelf 10 (Shelf_B_1_4)	Platten-Shelf 11 (Shelf_A_1_2)	Knoten A 1
Pool 1	Platten-Shelf 12 (Shelf_A_1_4)	Festplatten-Shelf 13 (Shelf_B_2_2)
Knoten B 2	Pool 0	Festplatten-Shelf 14 (Shelf_B_2_4)
Platten-Shelf 15 (Shelf_A_2_2)	Knoten A 2	Pool 1
Platten-Shelf 16 (Shelf_A_2_4)	Festplatten-Shelf 1 (Shelf_B_3_2)	Knoten A 3
Pool 0	Festplatten-Shelf 2 (Shelf_B_3_4)	Platten-Shelf 3 (Shelf_A_3_2)
Knoten B 3	Pool 1	Platten-Shelf 4 (Shelf_A_3_4)
Festplatten-Shelf 5 (Shelf_B_4_2)	Knoten A 4	Pool 0
Festplatten-Shelf 6 (Shelf_B_4_4)	Platten-Shelf 7 (Shelf_A_4_2)	Knoten B 4

Schritte

1. Bestätigen Sie die Shelf-Zuweisungen:

   ```
   disk show -v
   ```

2. Weisen Sie bei Bedarf explizit Festplatten auf den angeschlossenen Platten-Shelfs dem entsprechenden Pool zu:

   ```
   disk assign
   ```

   Wenn Sie im Befehl Platzhalter verwenden, können Sie alle Festplatten in einem Festplatten-Shelf mit einem Befehl zuweisen. Sie können die Festplatten-Shelf-IDs und Einschübe für jede Festplatte mit identifizieren `storage show disk -x` Befehl.

Zuweisung der Festplatteneigentümer in anderen Systemen außerhalb von All Flash FAS

Wenn auf den MetroCluster Nodes die Festplatten nicht korrekt zugewiesen sind oder wenn Sie in Ihrer Konfiguration DS460C Platten-Shelfs verwenden, müssen Sie jedem der Nodes der MetroCluster Konfiguration Shelf-einzeln Festplatten zuweisen. Sie erstellen eine Konfiguration, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Bevor Sie beginnen

Die Storage Controller müssen sich im Wartungsmodus befinden.

Über diese Aufgabe

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs nicht umfasst, ist diese Aufgabe nicht erforderlich, wenn die Festplatten bereits im Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören.
>
> Pool 1 enthält immer die Festplatten, die sich dem Speichersystem, zu dem sie gehören, fernhalten.

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

Diese Festplatten in der Schublade zuweisen…	Zu diesem Knoten und Pool…
0-2	Pool des lokalen Node 0
3 - 5	Pool 0 des HA-Partner-Node
6 - 8	DR-Partner des lokalen Knotens Pool 1
9 - 11	DR-Partner des HA-Partners Pool 1

Mit diesem Zuweisungsmuster wird sichergestellt, dass ein Aggregat minimal beeinträchtigt wird, wenn ein Einschub offline geht.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Platten-Shelfs den Nodes des ersten Standorts (Standort A) zu:

   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. Weisen Sie beim ersten Knoten systematisch die lokalen Festplatten-Shelfs dem Pool 0 und den Remote-Festplatten-Shelfs zu, und Pool 1:

      ```
      disk assign -shelf local-switch-name:shelf-name.port -p pool
      ```

      Wenn der Storage Controller Controller_A_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

b. Wiederholen Sie den Vorgang für den zweiten Node am lokalen Standort, indem Sie den Pool 0 und die Remote-Festplatten-Shelfs systematisch den Pool 1 zuweisen:

   `disk assign -shelf local-switch-name:shelf-name.port -p pool`

   Wenn der Storage Controller Controller_A_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Weisen Sie die Platten-Shelfs den Nodes am zweiten Standort (Standort B) zu:

   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. Weisen Sie beim ersten Knoten am Remote-Standort systematisch seine lokalen Festplatten-Shelfs dem Pool 0 und seinen Remote-Festplatten-Shelfs zu 1:

      `disk assign -shelf local-switch-nameshelf-name -p pool`

      Wenn der Storage Controller_B_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

   b. Wiederholen Sie den Vorgang für den zweiten Node am Remote-Standort, indem Sie seine lokalen Festplatten-Shelfs systematisch dem Pool 0 und den Remote-Festplatten-Shelfs Pool 1 zuordnen:

      `disk assign -shelf shelf-name -p pool`

      Wenn der Storage Controller_B_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Bestätigen Sie die Shelf-Zuweisungen:

   ```
   storage show shelf
   ```

5. Beenden des Wartungsmodus:

   ```
   halt
   ```

6. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

Zuweisung der Festplatteneigentümer für AFF Systeme

Wenn Sie in einer Konfiguration mit AFF Systemen und gespiegelten Aggregaten einsetzen und die Nodes die Festplatten (SSDs) nicht korrekt zugewiesen sind, sollten Sie den HA-Partner-Node jeweils halb so viele Festplatten an jedem Shelf einem lokalen Node und der anderen Hälfte der Festplatten zuweisen. Sie sollten eine Konfiguration erstellen, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Bevor Sie beginnen

Die Storage Controller müssen sich im Wartungsmodus befinden.

Über diese Aufgabe

Dies gilt nicht für Konfigurationen mit nicht gespiegelten Aggregaten, einer aktiv/Passiv-Konfiguration oder einer ungleichen Anzahl von Festplatten in lokalen und Remote-Pools.

Dieser Task ist nicht erforderlich, wenn Festplatten beim Empfang vom Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören.
>
> Pool 1 enthält immer die Festplatten, die sich dem Speichersystem, zu dem sie gehören, fernhalten.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Festplatten den Nodes des ersten Standorts (Standort A) zu:

   Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

   a. Weisen Sie beim ersten Knoten systematisch die Hälfte der Disks jedem Shelf zu, um 0 und die andere

Hälfte dem Pool des HA-Partners 0 zu bündeln:

```
disk assign -shelf <shelf-name> -p <pool> -n <number-of-disks>
```

Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Wiederholen Sie den Vorgang für den zweiten Node am lokalen Standort, indem Sie systematisch die Hälfte der Festplatten in jedem Shelf den Pool 1 und die andere Hälfte dem Pool des HA-Partners 1 zuweisen:

```
disk assign -disk disk-name -p pool
```

Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Weisen Sie die Festplatten den Nodes des zweiten Standorts (Standort B) zu:

Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

a. Weisen Sie auf dem ersten Knoten am Remote-Standort systematisch die Hälfte der Festplatten auf jedem Shelf zu, um den Pool 0 und die andere Hälfte dem Pool des HA-Partners 0 zu bündeln:

```
disk assign -disk disk-name -p pool
```

Wenn der Storage Controller Controller_B_1 vier Shelves mit jeweils 8 SSDs hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. Wiederholen Sie diesen Vorgang für den zweiten Node am Remote-Standort, indem Sie in jedem Shelf

systematisch die Hälfte der Festplatten dem Pool 1 und der anderen Hälfte dem Pool des HA-Partners 1 zuweisen:

```
disk assign -disk disk-name -p pool
```

Wenn der Storage Controller Controller_B_2 vier Shelfs mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Bestätigen Sie die Festplattenzuordnungen:

   ```
   storage show disk
   ```

5. Beenden des Wartungsmodus:

   ```
   halt
   ```

6. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

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 dem Versand eine Festplattenzuordnung 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	Pool 1
Platten-Shelf 12 (Shelf_A_1_4)			

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 mithilfe des Befehls Disk assign Festplatten in den angeschlossenen Platten-Shelfs dem entsprechenden Pool zuweisen.

   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 Festplatten-Shelfs dem Pool 0 und den Remote-Festplatten-Shelfs zu 1:

      ```
      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 bündeln:

   `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`

Einrichtung von ONTAP

Sie müssen ONTAP auf jedem Controller-Modul einrichten.

Wenn Sie die neuen Controller als Netzboot ausführen müssen, finden Sie unter "Netbootting der neuen Controller-Module" Im *MetroCluster Upgrade, Transition and Expansion Guide*.

Wahlmöglichkeiten

- Einrichten von ONTAP in einer MetroCluster Konfiguration mit zwei Nodes
- Einrichten von ONTAP in einer MetroCluster Konfiguration mit acht oder vier Nodes

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 Cluster-Setup-Befehl verwenden, um den Node als Single Node Cluster zu konfigurieren.

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.

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

Weitere allgemeine Informationen zum Einrichten von ONTAP finden Sie unter "ONTAP einrichten".

Schritte

1. Schalten Sie den ersten Node ein.

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

   Der Node bootet. Anschließend startet der Cluster-Setup-Assistent auf der Konsole, sodass Sie informiert werden, 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. Akzeptieren Sie die Standardeinstellung des Systems `yes` Drücken Sie die Eingabetaste, oder geben Sie Ihre eigenen Werte ein, indem Sie eingeben `no`, Und drücken Sie dann die Eingabetaste.
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
   ```

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

Einrichten von ONTAP in einer MetroCluster Konfiguration mit acht oder vier Nodes

Nachdem Sie jeden Node gebootet haben, werden Sie aufgefordert, das System Setup Tool auszuführen, um die grundlegende Node- und Cluster-Konfiguration durchzuführen. Nach dem Konfigurieren des Clusters kehren Sie zur ONTAP-CLI zurück, um Aggregate zu erstellen und die MetroCluster-Konfiguration zu erstellen.

Bevor Sie beginnen

Sie müssen die MetroCluster-Konfiguration verkabelt haben.

Über diese Aufgabe

Diese Aufgabe gilt für MetroCluster Konfigurationen mit acht oder vier Nodes mithilfe von nativem NetApp Storage.

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

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

Dieses Verfahren verwendet das System-Setup-Tool. Wenn gewünscht, können Sie stattdessen den CLI-Cluster-Setup-Assistenten verwenden.

Schritte

1. Falls noch nicht geschehen, schalten Sie jeden Knoten ein und lassen Sie ihn vollständig booten.

   Wenn sich das System im Wartungsmodus befindet, geben Sie den Befehl stop ein, um den Wartungsmodus zu beenden, und geben Sie dann den folgenden Befehl an der LOADER-Eingabeaufforderung aus:

   ```
   boot_ontap
   ```

   Die Ausgabe sollte wie folgt aussehen:

   ```
   Welcome to node setup

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

   To accept a default or omit a question, do not enter a value.
   .
   .
   .
   ```

2. Aktivieren Sie das AutoSupport-Tool, indem Sie den vom System bereitgestellten Anweisungen folgen.
3. Befolgen Sie die Aufforderungen zur Konfiguration der Node-Managementoberfläche.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

   ```
   Enter the node management interface port: [e0M]:
   Enter the node management interface IP address: 10.228.160.229
   Enter the node management interface netmask: 225.225.252.0
   Enter the node management interface default gateway: 10.228.160.1
   ```

4. Sicherstellen, dass die Nodes im Hochverfügbarkeits-Modus konfiguriert sind:

   ```
   storage failover show -fields mode
   ```

   Wenn nicht, müssen Sie für jeden Node den folgenden Befehl eingeben und den Node neu booten:

   ```
   storage failover modify -mode ha -node localhost
   ```

   Dieser Befehl konfiguriert den Hochverfügbarkeits-Modus, ermöglicht jedoch kein Storage Failover. Das Storage-Failover wird automatisch aktiviert, wenn die MetroCluster-Konfiguration zu einem späteren Zeitpunkt im Konfigurationsprozess durchgeführt wird.

5. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

```
network port show
```

Im folgenden Beispiel wird die Ausgabe für „Cluster_A“ angezeigt:

```
cluster_A::> network port show
                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Wenn Sie einen 2-Node-Cluster ohne Switches (ein Cluster ohne Cluster-Interconnect-Switches) erstellen, aktivieren Sie den Networking-Modus ohne Switches:

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   Sie können antworten `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen. Die Eingabeaufforderung für den erweiterten Modus wird angezeigt (*).

   a. Aktivieren des Cluster-Modus ohne Switches:

   ```
   network options switchless-cluster modify -enabled true
   ```

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

7. Starten Sie das System-Setup-Tool gemäß den Informationen, die nach dem ersten Booten auf der Systemkonsole angezeigt werden.
8. Verwenden Sie das System Setup Tool, um jeden Node zu konfigurieren und den Cluster zu erstellen, jedoch keine Aggregate zu erstellen.

> Sie erstellen gespiegelte Aggregate in späteren Aufgaben.

Nachdem Sie fertig sind

Kehren Sie zur ONTAP-Befehlszeilenschnittstelle zurück und führen Sie die MetroCluster-Konfiguration durch. Führen Sie dazu die folgenden Aufgaben aus.

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.

Über diese Aufgabe

Bevor Sie ausführen `metrocluster configure`, HA-Modus und DR-Spiegelung sind nicht aktiviert und Sie können eine Fehlermeldung in Bezug auf dieses erwartete Verhalten sehen. Sie aktivieren später den HA-Modus und die DR-Spiegelung, wenn Sie den Befehl ausführen `metrocluster configure` Um die Konfiguration zu implementieren.

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.

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.

Wahlmöglichkeiten

- Konfigurieren von Intercluster-LIFs auf dedizierten Ports
- Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports

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.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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

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

   Das folgende Beispiel weist den Failover-Gruppe intercluster01 Ports „e0e“ und „e0f“ auf dem System „SVMcluster01“ zu:

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

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

   `network interface failover-groups show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  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 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_ic.01“ 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 9.6 und höher

Führen Sie den Befehl aus: `network interface show -service-policy default-intercluster`

ONTAP 9.5 und früher

Führen Sie den Befehl aus: `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 9.6 und höher

Führen Sie den Befehl aus: `network interface show -service-policy default-intercluster -failover`

ONTAP 9.5 und früher

Führen Sie den Befehl aus: `network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem SVM „e0e“-Port an den „e0f“-Port scheitern.

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

Verwandte Informationen

"Überlegungen bei der Verwendung von dedizierten Ports"

Wenn Sie bestimmen, 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.

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 Netzwerkports in cluster01 angezeigt:

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

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

ONTAP 9.6 und höher

Führen Sie den Befehl aus: `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

Führen Sie den Befehl aus:
`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_ic.01 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 9.6 und höher

Führen Sie den Befehl aus: `network interface show -service-policy default-intercluster`

ONTAP 9.5 und früher

Führen Sie den Befehl aus: `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 9.6 und höher

Führen Sie den Befehl aus: `network interface show –service-policy default-intercluster -failover`

ONTAP 9.5 und früher

Führen Sie den Befehl aus:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern wird.

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

Verwandte Informationen

"Überlegungen bei der Freigabe von Datenports"

Erstellen einer Cluster-Peer-Beziehung

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

Über diese Aufgabe

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 im 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.
- Cluster-Administratoren müssen der Passphrase zugestimmt 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 Option *-ipspace* ignorieren, wenn Sie keinen benutzerdefinierten IPspace verwenden. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel erstellt eine Cluster-Peer-Beziehung zum Remote-Cluster bei intercluster LIF IP-Adressen „192.168.2.201“ und „192.168.2.202“:

   ```
   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
   ```

   Der folgende Befehl spiegelt das Root-Aggregat für Controller_A_1:

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

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

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

Verwandte Informationen

"Logisches Storage-Management mit der CLI"

Erstellung eines gespiegelten Datenaggregats auf jedem Node

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

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

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   ```
   storage disk show -spare -owner node_name
   ```

2. Erstellen Sie das Aggregat mit dem Storage-Aggregat create -mirror TRUE Befehl.

   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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen

- Anzahl der zu einführenden Laufwerke

> In der minimal unterstützten Konfiguration, bei der eine begrenzte Anzahl von Laufwerken verfügbar ist, müssen Sie den verwenden `force-small-aggregate` Option zum Erstellen eines RAID-DP Aggregats mit drei Festplatten.

- Prüfsummenstil, den Sie für das Aggregat verwenden möchten
- Typ der zu verwendenden Laufwerke
- Die Größe der zu verwendenden Laufwerke
- Fahrgeschwindigkeit zu verwenden
- RAID-Typ für RAID-Gruppen auf dem Aggregat
- Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
- Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

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

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

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

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

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

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

> 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.

- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

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

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- *Festplatten- und Aggregatmanagement* enthält weitere Informationen zur Spiegelung von Aggregaten.

Schritte

1. 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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

   Weitere Informationen zu diesen Optionen finden Sie auf der „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`

Verwandte Informationen

"Festplatten- und Tier-Management (Aggregat)"

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.

  Sie können dies mit dem überprüfen `storage aggregate show` Befehl.

  > Wenn Sie ein einzelnes gespiegeltes Datenaggregat verwenden möchten, finden Sie weitere Informationen unter Schritt 1 Weitere Anweisungen.

- Der HA-Konfigurationsstatus der Controller und des Chassis muss „mcc“ sein.

Über diese Aufgabe

Sie stellen das aus `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.

Der `metrocluster configure` Befehl koppelt die beiden Nodes automatisch mit den niedrigsten System-IDs in jedem der beiden Cluster als Disaster Recovery (DR) Partner. In einer MetroCluster Konfiguration mit vier Nodes gibt es zwei DR-Partnerpaare. Das zweite DR-Paar wird aus den beiden Knoten mit höheren System-IDs erstellt.

> Sie müssen vor Ausführung des Befehls * Onboard Key Manager (OKM) oder externe Schlüsselverwaltung nicht konfigurieren `metrocluster configure`.

Schritte

1. [[step1_aggr] 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 reagieren `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus (*>) angezeigt.
	
	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 Administratorberechtigungsebene:
	
	`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 Knoten 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 in einer MetroCluster Konfiguration mit vier Nodes 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
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

   a. Überprüfen Sie die Konfiguration von Standort A:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show

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

   b. Überprüfen Sie die Konfiguration von Standort B:

   ```
   metrocluster show
   ```

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

Konfigurieren von in-Order-Lieferung oder Lieferung von Frames auf ONTAP Software außerhalb der Reihenfolge

Sie müssen entweder in-Order-Lieferung (IOD) oder Out-of-Order-Lieferung (OOD) von Frames entsprechend der Fibre-Channel (FC) Switch-Konfiguration konfigurieren.

Über diese Aufgabe

Wenn der FC-Switch für IOD konfiguriert ist, muss die ONTAP-Software für IOD konfiguriert werden. Gleiches gilt, wenn der FC-Switch für OOD konfiguriert ist, dann muss ONTAP für OOD konfiguriert werden.

> Sie müssen den Controller neu booten, um die Konfiguration zu ändern.

Schritt

1. Konfigurieren Sie ONTAP für den Betrieb von IOD oder OOD von Frames.
   - Standardmäßig ist IOD von Frames in ONTAP aktiviert. So prüfen Sie die Konfigurationsdetails:
     i. Erweiterten Modus aufrufen:

     ```
     set advanced
     ```

     ii. Überprüfen Sie die Einstellungen:

     ```
     metrocluster interconnect adapter show
     ```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

- Die folgenden Schritte müssen auf jedem Knoten ausgeführt werden, um OOD von Frames zu konfigurieren:

  i. Erweiterten Modus aufrufen:

  ```
  set advanced
  ```

  ii. Überprüfen Sie die MetroCluster-Konfigurationseinstellungen:

  ```
  metrocluster interconnect adapter show
  ```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

iii. OOD auf Knoten „`mcc4-b1`“ und Knoten „`mcc4-b2`“ aktivieren:

```
metrocluster interconnect adapter modify -node node_name -is-ood-enabled
true
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true
```

i. Starten Sie den Controller neu, indem Sie in beide Richtungen eine HA-Übernahme durchführen.

ii. Überprüfen Sie die Einstellungen:

```
metrocluster interconnect adapter show
```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI   Up     true      17.0.1.2       6a
mcc4-b1      fcvi_device_1   FC-VI   Up     true      18.0.0.2      6b
mcc4-b1      mlx4_0          IB      Down   false     192.0.5.193   ib2a
mcc4-b1      mlx4_0          IB      Up     false     192.0.5.194   ib2b
mcc4-b2      fcvi_device_0   FC-VI   Up     true      17.0.2.2      6a
mcc4-b2      fcvi_device_1   FC-VI   Up     true      18.0.1.2      6b
mcc4-b2      mlx4_0          IB      Down   false     192.0.2.9     ib2a
mcc4-b2      mlx4_0          IB      Up     false     192.0.2.10    ib2b
8 entries were displayed.
```

Konfigurieren von SNMPv3 in einer MetroCluster-Konfiguration

Bevor Sie beginnen

Die Authentifizierungs- und Datenschutzprotokolle auf den Switches und auf dem ONTAP System müssen identisch sein.

Über diese Aufgabe

ONTAP unterstützt derzeit AES-128-Verschlüsselung.

Schritte

1. Erstellen Sie einen SNMP-Benutzer für jeden Switch von der Controller-Eingabeaufforderung:

   `security login create`

   ```
   Controller_A_1::> security login create -user-or-group-name snmpv3user
   -application snmp -authentication-method usm -role none -remote-switch
   -ipaddress 10.10.10.10
   ```

2. Beantworten Sie bei Bedarf an Ihrem Standort die folgenden Fragen:

   Drücken Sie für EngineID die **Eingabetaste**, um den Standardwert zuzuweisen.

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

Derselbe Benutzername kann zu verschiedenen Switches mit unterschiedlichen IP-Adressen hinzugefügt werden.

3. Erstellen Sie einen SNMP-Benutzer für den Rest der Switches.

   Das folgende Beispiel zeigt, wie ein Benutzername für einen Switch mit der IP-Adresse 10.10.10.11 erstellt wird.

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.
10.10.11
```

4. Überprüfen Sie, ob für jeden Switch ein Anmeldeeintrag vorhanden ist:

```
security login show
```

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

------------ ------------------ ----------- ---------------------
-----------------------

node_A_1 SVM 1 snmpv3user     snmp        usm
10.10.10.10

node_A_1 SVM 2 snmpv3user     snmp        usm
10.10.10.11

node_A_1 SVM 3 snmpv3user    snmp        usm
10.10.10.12

node_A_1 SVM 4 snmpv3user     snmp        usm
10.10.10.13

4 entries were displayed.
```

5. Konfigurieren Sie SNMPv3 an den Switches über die Switch-Eingabeaufforderung:

Brocade -Switches (FOS 9.0 und höher)

```
snmpconfig --add snmpv3 -index <index> -user <user_name> -groupname <rw/ro>
-auth_proto <auth_protocol> -auth_passwd <auth_password> -priv_proto
<priv_protocol> -priv_passwd <priv_password>
```

Brocade -Switches (FOS 8.x und früher)

```
snmpconfig --set snmpv3
```

Das Beispiel zeigt, wie ein schreibgeschützter Benutzer konfiguriert wird. Sie können die RW-Benutzer bei Bedarf anpassen. Wenn Sie RO-Zugriff benötigen, geben Sie nach „Benutzer (ro):“ den „snmpv3user“ an.

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [3]
```

Cisco Switches

```
snmp-server user <user_name> auth [md5/sha/sha-256] <auth_password> priv
(aes-128) <priv_password>
```

Sie sollten auch Passwörter für nicht verwendete Konten festlegen, um diese zu sichern und die beste in Ihrer ONTAP-Version verfügbare Verschlüsselung zu verwenden.

6. Konfigurieren Sie die Verschlüsselung und Passwörter für die übrigen Switch-Benutzer nach Bedarf an Ihrem Standort.

Konfigurieren von MetroCluster Komponenten für das Monitoring des Systemzustands

Sie müssen einige spezielle Konfigurationsschritte durchführen, bevor Sie die Komponenten einer MetroCluster-Konfiguration überwachen.

Zur Verbesserung der Sicherheit empfiehlt NetApp, SNMPv2 oder SNMPv3 zur Überwachung des Switch-Zustands zu konfigurieren.

Über diese Aufgabe

Diese Aufgaben gelten nur für Systeme mit FC-to-SAS-Bridges.

Ab Fabric OS 9.0 wird SNMPv2 für die Integritätsüberwachung auf Brocade-Switches nicht unterstützt. Stattdessen müssen Sie SNMPv3 verwenden. Wenn Sie SNMPv3 verwenden, müssen Sie SNMPv3 in

ONTAP konfigurieren, bevor Sie mit dem folgenden Abschnitt fortfahren. Weitere Informationen finden Sie unter Konfigurieren von SNMPv3 in einer MetroCluster-Konfiguration.

- Sie sollten Bridges und eine Node-Management-LIF in einem dedizierten Netzwerk platzieren, um eine Interferenz von anderen Quellen zu vermeiden.
- Wenn Sie ein dediziertes Netzwerk für die Statusüberwachung verwenden, muss jeder Node über eine Node-Management-LIF in diesem dedizierten Netzwerk verfügen.

NetApp unterstützt nur die folgenden Tools zur Überwachung der Komponenten in einer MetroCluster FC-Konfiguration:

- Brocade Network Advisor (BNA)
- Brocade Sannav
- Active IQ Config Advisor
- NetApp Zustandsüberwachung (ONTAP)
- MetroCluster-Datensammler (MC_DC)

Konfigurieren von MetroCluster FC-Switches für das Monitoring des Systemzustands

In einer Fabric-Attached MetroCluster-Konfiguration müssen Sie einige zusätzliche Konfigurationsschritte durchführen, um die FC-Switches zu überwachen.

Ab ONTAP 9.8 wird der `storage switch` Befehl durch ersetzt `system switch fibre-channel`. Im Folgenden wird der Befehl angezeigt `storage switch`. Wenn Sie jedoch ONTAP 9.8 oder höher ausführen, ist der `system switch fibre-channel` Befehl bevorzugt.

Schritte

1. Fügen Sie jedem MetroCluster-Knoten einen Switch mit einer IP-Adresse hinzu:

   Der Befehl, den Sie ausführen, hängt davon ab, ob Sie SNMPv2 oder SNMPv3 verwenden.

   Switch mit SNMPv3 hinzufügen:

   ```
   storage switch add -address <ip_adddress> -snmp-version SNMPv3 -snmp
   -community-or-username <SNMP_user_configured_on_the_switch>
   ```

   Switch mit SNMPv2 hinzufügen:

   ```
   storage switch add -address ipaddress
   ```

   Dieser Befehl muss bei allen vier Switches der MetroCluster-Konfiguration wiederholt werden.

   Brocade 7840 FC-Switches und alle Warnmeldungen werden in der Statusüberwachung unterstützt, außer NoISLPresent_Alert.

   Das folgende Beispiel zeigt den Befehl zum Hinzufügen eines Switches mit der IP-Adresse 10.10.10.10:

```
controller_A_1::> storage switch add -address 10.10.10.10
```

2. Überprüfen Sie, ob alle Switches richtig konfiguriert sind:

   ```
   storage switch show
   ```

   Es kann bis zu 15 Minuten dauern, bis alle Daten aufgrund des 15-minütigen Abrufintervalls reflektiert werden.

   Im folgenden Beispiel wird der Befehl angezeigt, der zur Überprüfung der Konfiguration der MetroCluster FC-Switches gegeben wurde:

   ```
   controller_A_1::> storage switch show
   Fabric           Switch Name     Vendor  Model        Switch WWN
   Status
   ---------------- --------------- ------- ------------ ----------------
   ------
   1000000533a9e7a6 brcd6505-fcs40  Brocade Brocade6505  1000000533a9e7a6
   OK
   1000000533a9e7a6 brcd6505-fcs42  Brocade Brocade6505  1000000533d3660a
   OK
   1000000533ed94d1 brcd6510-fcs44  Brocade Brocade6510  1000000533eda031
   OK
   1000000533ed94d1 brcd6510-fcs45  Brocade Brocade6510  1000000533ed94d1
   OK
   4 entries were displayed.

   controller_A_1::>
   ```

   Wenn der weltweite Name (WWN) des Switches angezeigt wird, kann die ONTAP-Systemzustandsüberwachung den FC-Switch kontaktieren und überwachen.

Verwandte Informationen

"Systemadministration"

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

Bei Systemen mit ONTAP-Versionen vor 9.8 müssen Sie einige besondere Konfigurationsschritte durchführen, um die FC-zu-SAS-Bridges in der MetroCluster-Konfiguration zu überwachen.

Über diese Aufgabe

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

Ab ONTAP 9.8 beginnt der `storage bridge` Befehl wird durch 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
9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
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 bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „Status“ „ok“ lautet und weitere Informationen, z. B. der weltweite Name (WWN), angezeigt werden.

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

```
controller_A_1::> storage bridge show

Bridge              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.

Über diese Aufgabe

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

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

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

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

   ```
   cluster_A::> metrocluster check show

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

2. Zeigen Sie detailliertere Ergebnisse der letzten Zeit an `metrocluster check run` Befehl:

   ```
   metrocluster check aggregate show

   metrocluster check cluster show
   ```

```
metrocluster check config-replication show

metrocluster check lif show

metrocluster check node show
```

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

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

```
cluster_A::> metrocluster check aggregate show

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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
                                                 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.

Über diese Aufgabe

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

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

Schritte

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

   "NetApp Downloads: Config Advisor"

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

Überprüfen des lokalen HA-Vorgangs

Wenn Sie über eine MetroCluster Konfiguration mit vier Nodes verfügen, sollten Sie den Betrieb der lokalen HA-Paare in der MetroCluster Konfiguration überprüfen. Dies ist nicht für Konfigurationen mit zwei Nodes erforderlich.

Über diese Aufgabe

MetroCluster-Konfigurationen mit zwei Nodes bestehen nicht aus lokalen HA-Paaren, und diese Aufgabe gilt nicht.

In den Beispielen für diese Aufgabe werden standardmäßige Namenskonventionen verwendet:

- Cluster_A
  - Controller_A_1
  - Controller_A_2
- Cluster_B
  - Controller_B_1
  - Controller_B_2

Schritte

1. Führen Sie auf Cluster_A Failover und Giveback in beide Richtungen durch.

   a. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

      ```
      storage failover show
      ```

      Die Ausgabe sollte darauf hinweisen, dass ein Takeover für beide Knoten möglich ist:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ---------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

b. Übernehmen Sie Controller_A_2 von Controller_A_1:

   `storage failover takeover controller_A_2`

   Sie können das verwenden `storage failover show-takeover` Befehl zum Überwachen des Fortschritts des Übernahmvorgangs.

c. Bestätigen Sie, dass der Takeover abgeschlossen ist:

   `storage failover show`

   Die Ausgabe sollte angeben, dass Controller_A_1 sich im Übernahmemodus befindet, was bedeutet, dass sie seinen HA-Partner übernommen hat:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -----------------
controller_A_1 controller_A_2 false    In takeover

controller_A_2 controller_A_1 -        Unknown
2 entries were displayed.
```

d. Controller_A_2 zurückgeben:

   `storage failover giveback controller_A_2`

   Sie können das verwenden `storage failover show-giveback` Befehl zum Überwachen des Fortschritts für den Giveback-Vorgang

e. Bestätigen Sie, dass der Speicher-Failover wieder in einen normalen Status zurückkehrt:

   `storage failover show`

   Die Ausgabe sollte darauf hinweisen, dass ein Takeover für beide Knoten möglich ist:

```
cluster_A::> storage failover show
                                Takeover
Node            Partner         Possible State Description
-------------- -------------- -------- --------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

a. Wiederholen Sie die vorherigen Teilschritte, und dieses Mal wird Controller_A_1 von Controller_A_2 verwendet.

2. Wiederholen Sie die vorherigen Schritte auf Cluster_B.

Verwandte Informationen

"Hochverfügbarkeitskonfiguration"

Überprüfung von Umschaltung, Reparatur und Wechsel zurück

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

Schritt

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.

Schritt

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

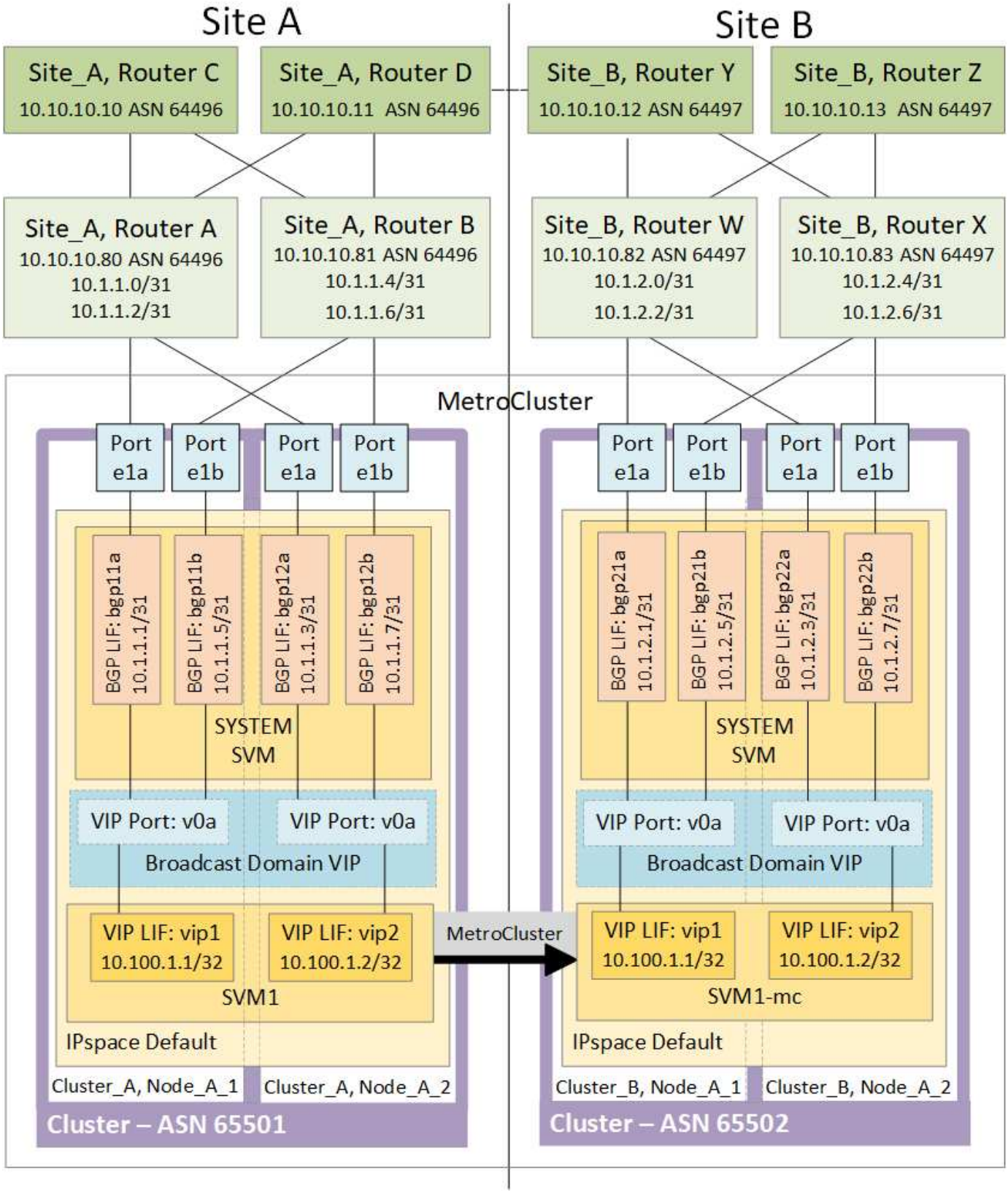
   `system configuration backup settings modify` *`URL-of-destination`*

   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 unter "Konfigurieren Sie virtuelle IP 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.

Nach der Konfiguration validiert die v0a (v0b usw.) kontinuierlich die Konnektivität und garantiert damit eine LIF-Migration oder ein Failover (im Gegensatz zu L2, wo eine kaputte 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 die ausgehandelte (geplante) Umschaltung testen, um die unterbrechungsfreie Datenverfügbarkeit zu bestätigen.

Über diese Aufgabe

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.

Über diese Aufgabe

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. Überprüfen der Spiegelung aller Aggregate:

   `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. Starten Sie die Nodes vom Disaster-Site 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. Den 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.

Über diese Aufgabe

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.

Über diese Aufgabe

Als Best Practice empfiehlt es sich, jede Netzteileinheit (PSU) einer Komponente mit separaten Netzteilen zu verbinden. Wenn beide Netzteile mit derselben Stromverteilereinheit (Power Distribution Unit, PDU) verbunden sind und eine elektrische Störung auftritt, kann der Standort ausfallen oder ein komplettes Shelf 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:

```
system environment sensors show -state fault

storage shelf show -errors
```

```
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 einem Switch Fabric-Ausfall

Sie können eine Switch-Fabric deaktivieren, um zu zeigen, dass die Datenverfügbarkeit nicht durch den Verlust beeinträchtigt wird.

Über diese Aufgabe

Dieser Test dauert etwa 15 Minuten.

Das erwartete Ergebnis dieses Verfahrens ist, dass das Deaktivieren einer Fabric dazu führt, dass der gesamte Cluster-Interconnect- und Festplattenverkehr zur anderen Fabric geleitet wird.

In den gezeigten Beispielen ist Switch Fabric 1 deaktiviert. Diese Fabric besteht aus zwei Switches, einer an jedem MetroCluster-Standort:

- FC_Switch_A_1 auf Cluster_A
- FC_Switch_B_1 auf Cluster_B

Schritte

1. Deaktivieren Sie die Verbindung zu einer der zwei Switch-Fabrics in der MetroCluster Konfiguration:

   a. Deaktivieren des ersten Switch in der Fabric:

   ```
   switchdisable
   ```

   ```
   FC_switch_A_1::> switchdisable
   ```

   b. Deaktivierung des zweiten Switch in der Fabric:

   ```
   switchdisable
   ```

   ```
   FC_switch_B_1::> switchdisable
   ```

2. Überwachen Sie das Ergebnis auf der Konsole der Controller-Module.

   Sie können die folgenden Befehle verwenden, um die Cluster-Nodes zu überprüfen, ob alle Daten noch verfügbar sind. In der Ausgabe des Befehls werden fehlende Pfade zu Festplatten angezeigt. Dies wird erwartet.

   - vserver zeigen
   - Netzwerkschnittstelle wird angezeigt
   - aggr-Show
   - System Node runnodename-Command Storage show Disk -p
   - Fehler auf der Speicherfestplatte wird angezeigt

3. Die Konnektivität mit einer der beiden Switch-Fabrics in der MetroCluster Konfiguration reaktivieren:

   a. Den ersten Switch in der Fabric wieder aktivieren:

   ```
   switchenable
   ```

   ```
   FC_switch_A_1::> switchenable
   ```

   b. Zweiten Switch in der Fabric wieder aktivieren:

   ```
   switchenable
   ```

```
FC_switch_B_1::> switchenable
```

4. Warten Sie mindestens 10 Minuten, und wiederholen Sie die oben genannten Schritte auf der anderen Switch-Struktur.

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.

Über diese Aufgabe

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 show

   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
```

MetroCluster-Konfigurationen entfernen

Wenden Sie sich an den technischen Support, wenn Sie die MetroCluster Konfiguration entfernen müssen.

Kontaktieren Sie den technischen Support von NetApp und lesen Sie das entsprechende Handbuch für Ihre Konfiguration von "Entfernen von Knoten aus einer MetroCluster Konfiguration - Auflösungsleitfaden."

Die Konfiguration von MetroCluster kann nicht rückgängig gemacht werden. Dieses Verfahren sollte nur mit Unterstützung durch den technischen Support erfolgen. Nach dem Entfernen der MetroCluster-Konfiguration sollten alle Festplatten-Konnektivität und Interconnects auf einen unterstützten Zustand eingestellt werden.

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

Weitere Konfigurations- und Überwachungsfunktionen sind mit dem Active IQ Unified Manager und dem ONTAP System Manager möglich

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-Dokumentation"

Synchronisieren Sie die Systemzeit mit NTP

Jedes Cluster benötigt einen eigenen NTP-Server (Network Time Protocol), um die Zeit zwischen den Nodes und ihren Clients zu synchronisieren.

Über diese Aufgabe

- Nach dem Takeover können Sie 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 Server verfügen, die von den Nodes, FC-Switches und FC-to-SAS-Bridges an diesem MetroCluster-Standort verwendet werden.
- Wenn Sie die MetroCluster Tiebreaker Software verwenden, sollte es auch einen eigenen separaten NTP-Server haben.

Abhängig von Ihrer ONTAP-Version können Sie den NTP über die Registerkarte **Cluster** oder **Insights** in der Benutzeroberfläche des Systemmanagers konfigurieren.

Cluster

In System Manager können Sie den NTP auf der Registerkarte **Cluster** mit zwei verschiedenen Optionen konfigurieren, je nach ONTAP-Version:

ONTAP 9.8 oder höher:

Führen Sie die folgenden Schritte aus, um das NTP von der Registerkarte **Cluster** in ONTAP 9.8 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Wählen Sie dann die Option und dann

Bearbeiten.
3. Wählen Sie im Fenster **Cluster-Details bearbeiten** die Option **+Hinzufügen** unter NTP-Servern aus.
4. Fügen Sie den Namen und den Speicherort hinzu, und geben Sie die IP-Adresse des Zeitservers an.
5. Wählen Sie dann **Speichern**.
6. Wiederholen Sie die Schritte für weitere Zeitserver.

ONTAP 9.11.1 oder höher:

Führen Sie die folgenden Schritte aus, um den NTP vom Fenster **Insights** auf der Registerkarte **Cluster** in ONTAP 9.11.1 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Scrollen Sie auf der Seite nach unten zum Fenster **Insights**, suchen Sie **zu wenige NTP-Server sind konfiguriert**, und wählen Sie dann **Fix IT**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Einblick

In ONTAP 9.11.1 oder höher können Sie NTP auch über die Registerkarte **Insights** in System Manager konfigurieren:

Schritte

1. Wechseln Sie in der System Manager-Benutzeroberfläche zur Registerkarte **Insights**.
2. Scrollen Sie nach unten zu **zu wenige NTP-Server sind konfiguriert** und wählen Sie **Fix it**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

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

Für FlexCache-Beziehungen zu einem Cluster außerhalb der MetroCluster-Konfiguration muss nach einem Switchover das Peering 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.
- 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

Verwandte Informationen

"Management von FlexCache Volumes mit der CLI"

FabricPool-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.7 unterstützen MetroCluster Konfigurationen FabricPool Storage Tiers.

Allgemeine Informationen zur Verwendung von FabricPool finden Sie unter "Festplatten- und Tier-Management (Aggregat)".

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 oder ein IP-Speicherplatz sein, 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 zum externen Objektspeicher gelangen kann.
- FabricPool unterstützt die SVM-Migration nicht, wenn die Quelle oder das Ziel ein MetroCluster-Cluster ist.

  "Erfahren Sie mehr über SVM-Datenmobilität".

Konfigurieren eines Aggregats zur Verwendung in einer gespiegelten FabricPool

> Bevor Sie das Aggregat konfigurieren, müssen Sie Objektspeicher wie in beschrieben einrichten "Richten Sie Objektspeicher für FabricPool in einer MetroCluster-Konfiguration ein".

Schritte

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 ist physisch weiter entfernt zum Cluster als der primäre Objektspeicher.

> Es wird empfohlen, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

FlexGroup-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.6 unterstützen MetroCluster Konfigurationen FlexGroup Volumes.

Unterstützung von Konsistenzgruppen in MetroCluster Konfigurationen

Ab ONTAP 9.11.1 "Konsistenzgruppen" Werden in MetroCluster-Konfigurationen unterstützt.

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

- "Netzwerk- und LIF-Management"
- 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.

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

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

Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration

- 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.

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

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.

Verwandte Informationen

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

  Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration

- 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.

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

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
- Sie sollten ein Subnetz-Objekt erstellen, bevor Sie eine LIF erstellen. Mithilfe eines Subnetzobjekts kann ONTAP Failover-Ziele auf dem Zielcluster ermitteln, da ihm eine Broadcast-Domäne zugeordnet ist.

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.

Verwandte Informationen

- 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.

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

- 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.

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

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.

LIFs sind nach einem Switchover nicht zugänglich

Wenn Änderungen in der FC Switch Fabric vorgenommen werden, an die die FC-Ziel-Ports der Quell- und DR-Nodes verbunden sind, sind die FC-LIFs, die am DR-Partner platziert werden, nach einem Switchvorgang möglicherweise für die Hosts unzugänglich.

Sie sollten den ausführen `metrocluster check lif repair-placement` Befehl an der Quelle sowie die DR-Nodes, nachdem eine Änderung in der FC-Switch-Fabric vorgenommen wurde, um die Host-Konnektivität der LIFs zu überprüfen. Die Änderungen in der Switch-Fabric können dazu führen, dass LIFs verschiedene Ziel-FC-Ports am DR-Partner-Node platziert werden.

Verwandte Informationen

- 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.

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

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

  Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration

Volume-Erstellung auf einem Root-Aggregat

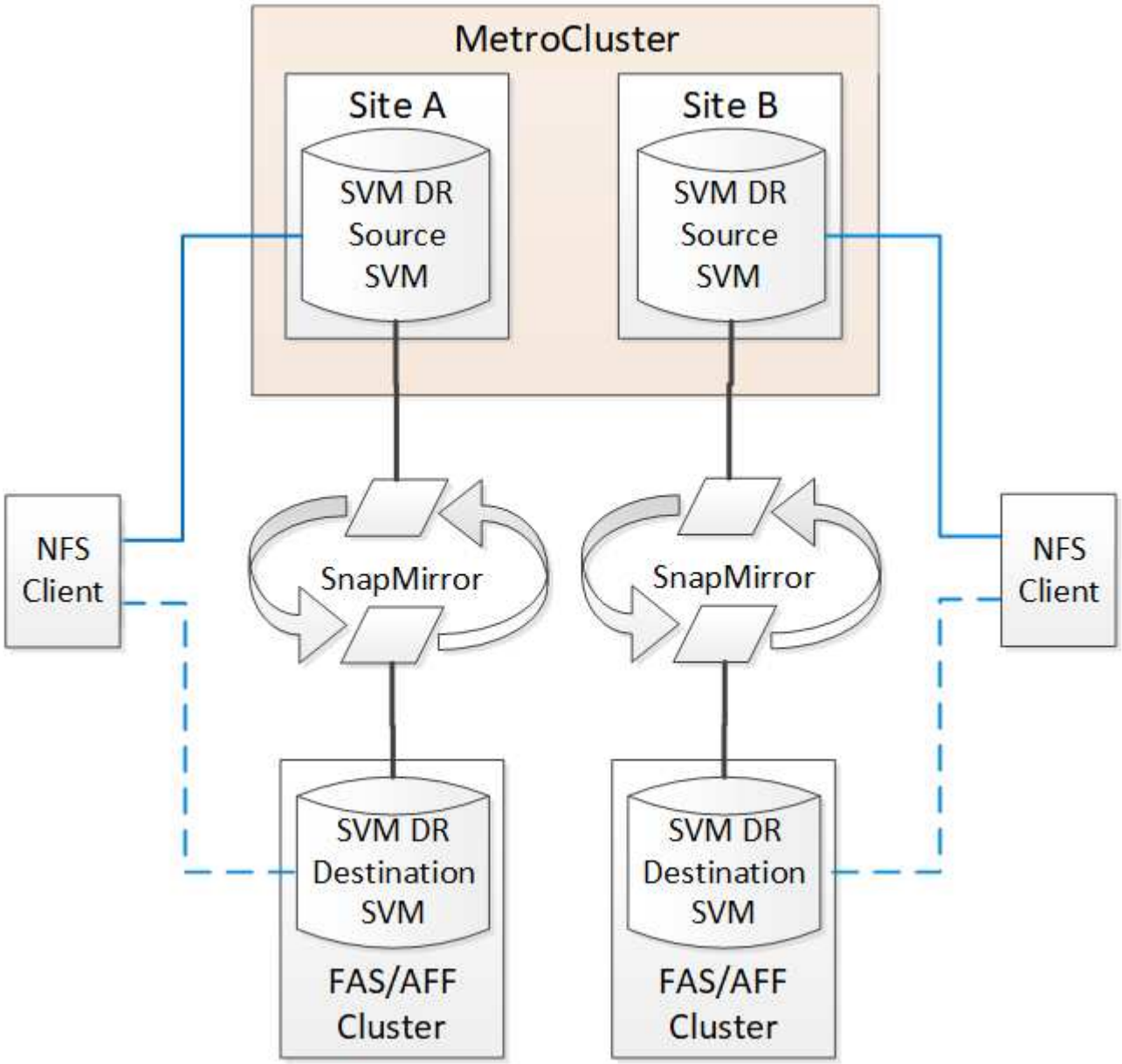
Das System lässt nicht die Erstellung neuer Volumes im Root-Aggregat (ein Aggregat mit einer HA-Richtlinie von CFO) eines Knotens in einer MetroCluster-Konfiguration zu.

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.

Ab ONTAP 9.11.1 können beide Standorte innerhalb einer MetroCluster-Konfiguration die Quelle für eine SVM-DR-Beziehung mit einem FAS oder einem AFF-Ziel-Cluster sein, wie im folgenden Image dargestellt.



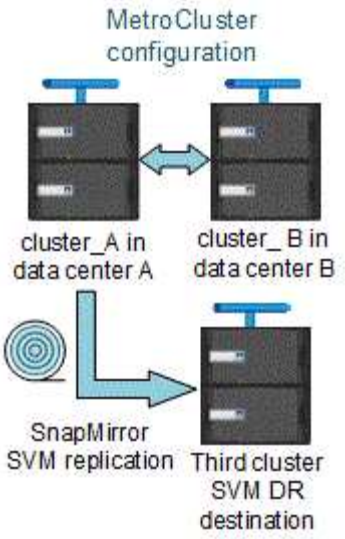
Bei der Verwendung von SVMs mit SnapMirror Disaster Recovery sollten Sie die folgenden Anforderungen und Einschränkungen beachten:

- 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.

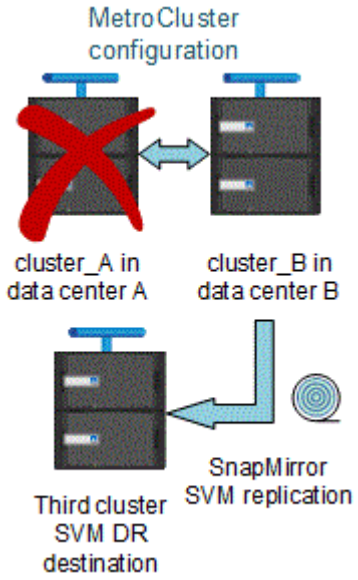
- Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind.

  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.

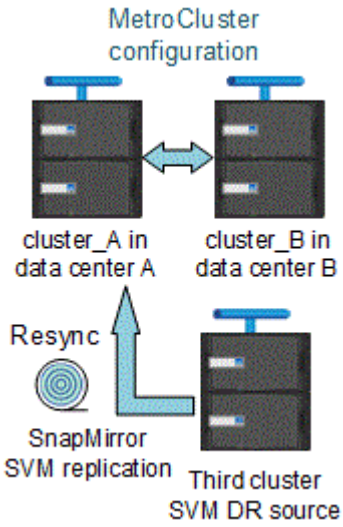
  Nach Abschluss des Switchover- oder Switch-Prozesses werden jedoch die nächsten geplanten SVM-DR-Updates erfolgreich durchgeführt.

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.

Die Ausgabe des Befehls „Storage Aggregate Plex show“ 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 „fehlgeschlagen“ angezeigt. 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.

Über diese Aufgabe

> 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.

Schritt

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
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"ONTAP 9-Dokumentation"	• Alle MetroCluster-Informationen
"NetApp MetroCluster Lösungsarchitektur und Design, TR-4705"	• Technische Übersicht über Konfiguration und Betrieb von MetroCluster FC • Best Practices für die MetroCluster FC-Konfiguration.
"Architektur und Design der MetroCluster IP-Lösung, TR-4689"	• Eine technische Übersicht über die Konfiguration und den Betrieb der MetroCluster IP-Adresse. • Best Practices für eine MetroCluster-IP-Konfiguration.
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • 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

"Warten der MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes
"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 Digital Advisor 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

Installieren Sie eine MetroCluster IP-Konfiguration

MetroCluster IP-Installationsworkflow

Um Ihre MetroCluster IP-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".
- "Verkabeln Sie die Komponenten"
- "Konfigurieren der Software"
- "Konfigurieren Sie den ONTAP Mediator" (Optional)
- "Testen Sie die Konfiguration"

Bereiten Sie sich auf die MetroCluster Installation vor

Supportmatrix für 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[1]	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 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.

Hinweise

1. Lesen Sie die folgenden Überlegungen für MetroCluster IP-Konfigurationen mit acht Nodes:
    - 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.

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".

Unterschiede zwischen ONTAP Mediator und MetroCluster Tiebreaker

Ab ONTAP 9.7 können Sie entweder die ONTAP Mediator-gestützte automatische ungeplante Umschaltung (MAUSO) in der MetroCluster IP-Konfiguration verwenden oder die MetroCluster Tiebreaker Software verwenden. Es ist nicht erforderlich, die MAUSO- oder Tiebreaker-Software zu verwenden; wenn Sie jedoch einen dieser Dienste nicht nutzen möchten, müssen Sie dies tun "Führen Sie eine manuelle Wiederherstellung durch" Bei einem Ausfall.

Die verschiedenen MetroCluster Konfigurationen führen unter unterschiedlichen Umständen automatische Umschaltung durch:

- **MetroCluster FC-Konfigurationen mit der AUSO-Fähigkeit (nicht in MetroCluster IP-Konfigurationen vorhanden)**

  In diesen Konfigurationen wird AUSO initiiert, wenn Controller ausfallen, der Speicher (und ggf. Brücken) jedoch betriebsbereit bleiben.

- **MetroCluster-IP-Konfigurationen mit ONTAP Mediator (ONTAP 9.7 und höher)**

  In diesen Konfigurationen wird MAUSO unter denselben Umständen wie AUSO wie oben beschrieben initiiert, aber auch nach einem kompletten Standortausfall (Controller, Storage und Switches).

  "Erfahren Sie, wie der ONTAP Mediator die automatische ungeplante Umschaltung unterstützt".

- **MetroCluster IP- oder FC-Konfigurationen mit der Tiebreaker Software im aktiven Modus**

  Bei diesen Konfigurationen initiiert der Tiebreaker eine ungeplante Umschaltung nach einem vollständigen Standortausfall.

  Bevor Sie die Tiebreaker Software verwenden, überprüfen Sie das "Installation und Konfiguration der MetroCluster Tiebreaker Software"

Interoperabilität von ONTAP Mediator mit anderen Anwendungen und Geräten

Es ist nicht möglich, Applikationen oder Appliances von Drittanbietern zu verwenden, die in Kombination mit ONTAP Mediator eine Umschaltung auslösen können. Darüber hinaus wird das Monitoring einer MetroCluster-Konfiguration mit MetroCluster Tiebreaker Software bei Verwendung des ONTAP Mediator nicht unterstützt.

Erfahren Sie mehr über Remote-Speicher und MetroCluster IP-Konfigurationen

Sie sollten verstehen, wie die Controller auf den Remote-Storage zugreifen und wie die MetroCluster-IP-Adressen funktionieren.

Zugriff auf Remote-Speicher in MetroCluster IP-Konfigurationen

In MetroCluster IP Konfigurationen erfolgt die einzige Möglichkeit, wie die lokalen Controller die Remote Speicherpools über die Remote-Controller erreichen können. Die IP-Switches sind mit den Ethernet-Ports der Controller verbunden. Sie verfügen nicht über direkte Verbindungen zu Festplatten-Shelfs. Wenn der Remote-Controller ausfällt, können die lokalen Controller die Remote-Speicherpools nicht erreichen.

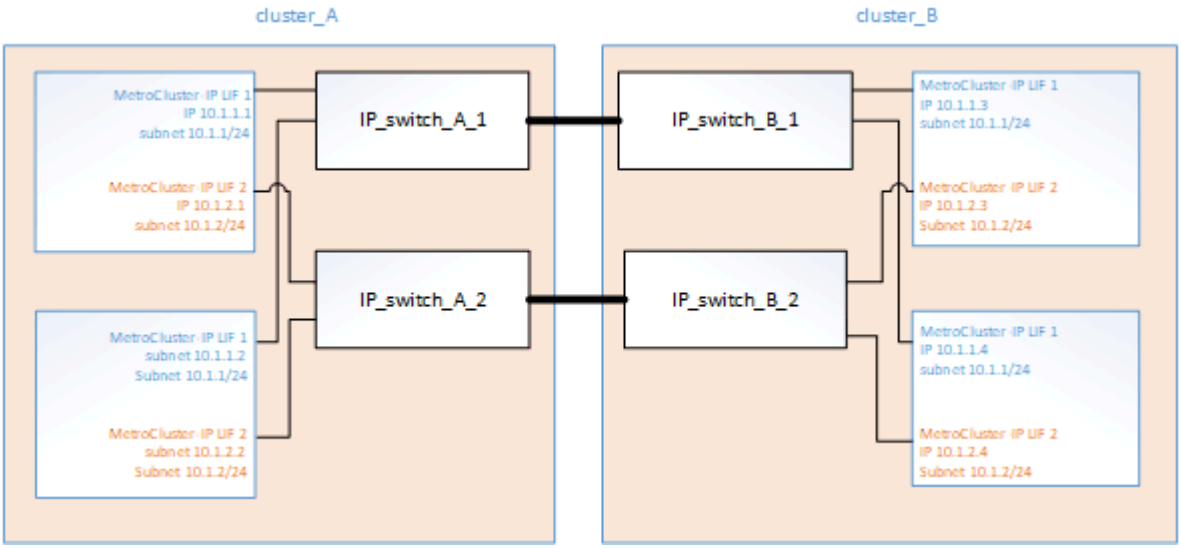
Dies unterscheidet sich von MetroCluster FC-Konfigurationen, in denen die Remote-Storage-Pools über die

FC-Fabric- oder SAS-Verbindungen mit den lokalen Controllern verbunden werden. Die lokalen Controller haben noch Zugriff auf den Remote-Storage, selbst wenn die Remote-Controller ausgefallen sind.

MetroCluster-IP-Adressen

Sie sollten wissen, wie die MetroCluster IP-Adressen und Schnittstellen in einer MetroCluster IP-Konfiguration implementiert werden, sowie welche Anforderungen damit verbunden sind.

In einer MetroCluster IP-Konfiguration werden die Replizierung von Storage und nichtflüchtigem Cache zwischen den HA-Paaren und den DR-Partnern über dedizierte Links mit hoher Bandbreite im MetroCluster IP-Fabric durchgeführt. Für die Storage-Replikation werden iSCSI-Verbindungen verwendet. Die IP-Switches werden auch für den gesamten clusterinternen Datenverkehr innerhalb der lokalen Cluster verwendet. Der MetroCluster-Datenverkehr wird mithilfe separater IP-Subnetze und VLANs vom clusterinternen Datenverkehr getrennt. Die MetroCluster IP Fabric unterscheidet sich von dem Cluster-Peering-Netzwerk.



Die MetroCluster IP-Konfiguration erfordert auf jedem Node zwei IP-Adressen, die dem Back-End MetroCluster IP Fabric vorbehalten sind. Die reservierten IP-Adressen werden während der Erstkonfiguration MetroCluster IP Logical Interfaces (LIFs) zugewiesen. Sie haben folgende Anforderungen:

> Sie müssen die MetroCluster-IP-Adressen sorgfältig auswählen, da Sie sie nach der ersten Konfiguration nicht ändern können.

- Sie müssen in einen eindeutigen IP-Bereich fallen.

  Sie dürfen sich nicht mit IP-Speicherplatz in der Umgebung überschneiden.

- Sie müssen sich in einem von zwei IP-Subnetzen befinden, die sie von allen anderen Traffic trennen.

Beispielsweise können die Nodes mit den folgenden IP-Adressen konfiguriert werden:

Knoten	Schnittstelle	IP-Adresse	Subnetz
Node_A_1	MetroCluster IP-Schnittstelle 1	10.1.1.1	10.1.1/24

Node_A_1	MetroCluster IP-Schnittstelle 2	10.1.2.1	10.1.2/24
Node_A_2	MetroCluster IP-Schnittstelle 1	10.1.1.2	10.1.1/24
Node_A_2	MetroCluster IP-Schnittstelle 2	10.1.2.2	10.1.2/24
Knoten_B_1	MetroCluster IP-Schnittstelle 1	10.1.1.3	10.1.1/24
Knoten_B_1	MetroCluster IP-Schnittstelle 2	10.1.2.3	10.1.2/24
Knoten_B_2	MetroCluster IP-Schnittstelle 1	10.1.1.4	10.1.1/24
Knoten_B_2	MetroCluster IP-Schnittstelle 2	10.1.2.4	10.1.2/24

Merkmale der MetroCluster IP-Schnittstellen

Die MetroCluster IP-Schnittstellen gelten speziell für MetroCluster IP-Konfigurationen. Sie weisen verschiedene Merkmale von anderen ONTAP Schnittstellentypen auf:

- Sie werden von der geschaffen `metrocluster configuration-settings interface create` Befehl als Teil der Erstkonfiguration von MetroCluster.

  > Ab ONTAP 9.9 müssen Sie auch die angeben, wenn Sie eine Layer 3-Konfiguration verwenden `-gateway` Parameter beim Erstellen von MetroCluster-IP-Schnittstellen. Siehe "Überlegungen für Layer 3-Weitbereichs-Netzwerke".

  Sie werden nicht durch die Befehle der Netzwerkschnittstelle erstellt oder geändert.

- Sie erscheinen nicht in der Ausgabe des `network interface show` Befehl.
- Sie führen kein Failover durch, bleiben aber mit dem Port verbunden, auf dem sie erstellt wurden.
- Bei den MetroCluster IP-Konfigurationen werden bestimmte Ethernet-Ports (je nach Plattform) für die MetroCluster IP-Schnittstellen verwendet.

> Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

MetroCluster IP-Überlegungen für automatische Laufwerkszuweisung und ADP-Systeme

Ab ONTAP 9.4 unterstützen MetroCluster IP-Konfigurationen neue Installationen mithilfe

von automatischer Festplattenzuweisung und ADP (Advanced Drive Partitioning).

Bei der Verwendung von ADP mit MetroCluster IP-Konfigurationen sollten Sie die folgenden Überlegungen beachten:

- ONTAP 9.4 und höher ist für die Verwendung von ADP mit MetroCluster IP Konfigurationen auf AFF und ASA Systemen erforderlich.
- ADPv2 wird in MetroCluster IP-Konfigurationen unterstützt.
- Das Root-Aggregat muss sich in Partition 3 für alle Knoten auf beiden Standorten befinden.
- Die Partitionierung und Festplattenzuordnung erfolgt automatisch bei der Erstkonfiguration der MetroCluster Standorte.
- Pool 0-Festplattenzuordnungen werden werkseitig ausgeführt.
- Die unverspiegelte Root wird werkseitig erstellt.
- Die Zuweisung der Daten erfolgt während des Setups am Standort des Kunden.
- In den meisten Fällen erfolgt die Laufwerkszuweisung und -Partitionierung automatisch während des Setup-Verfahrens.
- Eine Festplatte und alle Partitionen müssen im Besitz von Nodes in demselben HA-Paar (Hochverfügbarkeit) sein. Die Partitionen oder Laufwerkseigentümer innerhalb eines einzelnen Laufwerks können nicht zwischen dem lokalen HA-Paar und dem Disaster Recovery-Partner (DR) oder dem DR-Zusatzpartner gemischt werden.

  Beispiel einer unterstützten Konfiguration:

Laufwerk/Partition	Eigentümer
Laufwerk:	`ClusterA-Node01`
Partition 1:	`ClusterA-Node01`
Partition 2:	`ClusterA-Node02`
Partition 3:	`ClusterA-Node01`

> Beim Upgrade von ONTAP 9.4 auf 9.5 erkennt das System die vorhandenen Festplattenzuordnungen.

Automatische Partitionierung

ADP wird automatisch während der Erstkonfiguration des Systems durchgeführt.

> Ab ONTAP 9.5 muss die automatische Festplattenzuordnung mit dem aktiviert werden `storage disk option modify -autoassign on` Befehl.

Sie müssen den ha-config-Status auf festlegen `mccip` Vor der automatischen Bereitstellung, um sicherzustellen, dass die richtigen Partitionsgrößen ausgewählt sind, um eine entsprechende Root-Volume-Größe zu ermöglichen. Weitere Informationen finden Sie unter "Überprüfen des HA-Konfigurationsstatus von Komponenten".

Bis zu 96 Laufwerke können während der Installation automatisch partitioniert werden. Nach der Erstinstallation können Sie zusätzliche Laufwerke hinzufügen.

Wenn Sie interne und externe Laufwerke verwenden, initialisieren Sie zuerst die MetroCluster mit nur den internen Laufwerken unter Verwendung von ADP. Anschließend schließen Sie das externe Shelf manuell an, nachdem Sie die Installation oder Einrichtung abgeschlossen haben.

Sie müssen sicherstellen, dass für die internen Shelfs die empfohlene Mindestanzahl an Laufwerken wie in beschrieben angegeben angegeben angegeben ist Unterschiede bei der ADP- und Festplattenzuordnung nach System.

Sowohl für die internen als auch für die externen Laufwerke müssen Sie die teilweise vollständigen Shelfs ausfüllen, wie in beschrieben Wie partielle Shelves befüllt werden.

Die automatische Zuweisung von Shelfs für Shelfs

Wenn pro Standort vier externe Shelfs vorhanden sind, wird jedem Shelf ein anderer Node und ein anderer Pool zugewiesen, wie im folgenden Beispiel dargestellt:

- Alle Festplatten an Site_A-Shelf_1 werden automatisch Pool 0 von Node_A_1 zugewiesen
- Alle Festplatten auf Site_A-Shelf_3 werden automatisch dem Pool 0 der Node_A_2 zugewiesen
- Alle Festplatten an Site_B-Shelf_1 werden automatisch dem Pool 0 der Node_B_1 zugewiesen
- Alle Festplatten an Site_B-Shelf_3 werden automatisch dem Pool 0 der Node_B_2 zugewiesen
- Alle Festplatten an Site_B-Shelf_2 werden Pool 1 der Node_A_1 automatisch zugewiesen
- Alle Festplatten an Site_B-Shelf_4 werden Pool 1 der Node_A_2 automatisch zugewiesen
- Alle Festplatten an Site_A-Shelf_2 werden Pool 1 der Node_B_1 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_4 werden automatisch Pool 1 der Node_B_2 zugewiesen

Wie partielle Shelves befüllt werden

Wenn Ihre Konfiguration Shelfs verwendet, die nicht vollständig befüllt sind (über leere Laufwerksschächte), müssen Sie die Laufwerke je nach Richtlinien für die Festplattenzuordnung gleichmäßig im Shelf verteilen. Die Richtlinie für die Festplattenzuweisung hängt davon ab, wie viele Shelfs an jedem MetroCluster Standort vorhanden sind.

Wenn Sie an jedem Standort ein einzelnes Shelf verwenden (oder nur das interne Shelf auf einem AFF A800 System), werden Festplatten anhand einer ViertelShelf-Richtlinie zugewiesen. Wenn das Shelf nicht vollständig gefüllt ist, installieren Sie die Laufwerke gleichmäßig auf allen Quartalen.

Die folgende Tabelle zeigt ein Beispiel dafür, wie 24 Festplatten in einem internen Shelf mit 48 Laufwerken platziert werden. Das Eigentum an den Laufwerken wird ebenfalls angezeigt.

Die 48 Laufwerkschächte sind in vier Quartale unterteilt:	Installieren Sie sechs Laufwerke in den ersten sechs Schächten in jedem Quartal…
Quartal: Buchten 0-11	Schächte 0-5
Quartal: Buchten 12-23	Schächte 12-17
Quartal 3: Buchten 24-35	Schächte 24-29
Quartal 4: Buchten 36-47	Schächte 36-41

Die folgende Tabelle zeigt ein Beispiel zum Platzieren von 16 Festplatten in ein internes Shelf mit 24 Laufwerken.

Die 24 Laufwerkschächte sind in vier Quartale unterteilt:	Installieren Sie vier Laufwerke in den ersten vier Schächten pro Quartal…
Quartal: Buchten 0-5	Schächte 0-3
Quartal 2: Buchten 6-11	Schächte 6-9
Quartal 3: Buchten 12-17	Schächte 12-15
Quartal 4: Buchten 18-23	Schächte 18-21

Wenn Sie zwei externe Shelfs an jedem Standort verwenden, werden Festplatten anhand einer halben Shelf-Richtlinie zugewiesen. Wenn die Shelfs nicht vollständig gefüllt sind, installieren Sie die Laufwerke an beiden Enden des Shelfs gleich.

Wenn Sie beispielsweise 12 Laufwerke in einem Shelf mit 24 Laufwerken installieren, installieren Sie Laufwerke in den Einschüben 0-5 und 18-23.

Manuelle Laufwerkszuweisung (ONTAP 9.5)

In ONTAP 9.5 ist bei Systemen mit den folgenden Shelf-Konfigurationen eine manuelle Laufwerkszuweisung erforderlich:

- Drei externe Shelves pro Standort.

  Zwei Shelfs werden automatisch anhand einer Richtlinie für die Zuweisung halber Shelfs zugewiesen, das dritte Shelf muss jedoch manuell zugewiesen werden.

- Mehr als vier Shelves pro Standort und die Gesamtzahl der externen Shelves ist kein Vielfaches von vier.

  Zusätzliche Shelves über dem nächstgelegenen Mehrfach von vier werden nicht zugewiesen und die Laufwerke müssen manuell zugewiesen werden. Wenn z. B. an dem Standort fünf externe Shelfs vorhanden sind, müssen dann fünf Shelfs manuell zugewiesen werden.

Sie müssen nur ein einziges Laufwerk für jedes nicht zugewiesene Shelf manuell zuweisen. Die restlichen Laufwerke auf dem Shelf werden dann automatisch zugewiesen.

Manuelle Laufwerkszuweisung (ONTAP 9.4)

In ONTAP 9.4 ist bei Systemen mit den folgenden Shelf-Konfigurationen eine manuelle Laufwerkszuweisung erforderlich:

- Weniger als vier externe Shelfs pro Standort.

  Die Laufwerke müssen manuell zugewiesen werden, um eine symmetrische Zuweisung der Laufwerke zu gewährleisten, wobei jeder Pool eine gleiche Anzahl von Laufwerken hat.

- Pro Standort mehr als vier externe Shelves und die Gesamtzahl der externen Shelves ist kein Vielfaches von vier.

Zusätzliche Shelves über dem nächstgelegenen Mehrfach von vier werden nicht zugewiesen und die Laufwerke müssen manuell zugewiesen werden.

Wenn Laufwerke manuell zugewiesen werden, sollten Sie Festplatten symmetrisch zuweisen, wobei jeder Pool eine gleiche Anzahl von Laufwerken zugewiesen ist. Wenn die Konfiguration beispielsweise zwei Storage-Shelfs an jedem Standort umfasst, würden Sie ein Shelf zum lokalen HA-Paar und ein Shelf zum Remote HA-Paar verwenden:

- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_1 dem Pool 0 von Node_A_1 zu.
- Weisen Sie die Hälfte der Festplatten auf site_A-Shelf_1 dem Pool 0 von Node_A_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_2 Pool 1 von Node_B_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_2 Pool 1 von Node_B_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_1 dem Pool 0 von Node_B_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_1 dem Pool 0 von Node_B_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_2 Pool 1 von Node_A_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_2 Pool 1 von Node_A_2 zu.

Hinzufügen von Shelfs zu einer vorhandenen Konfiguration

Die automatische Laufwerkszuweisung unterstützt das symmetrische Hinzufügen von Shelfs zu einer vorhandenen Konfiguration.

Beim Hinzufügen neuer Shelves wendet das System dieselbe Zuweisungsrichtlinie auf neu hinzugefügte Shelfs an. Wenn beispielsweise bei einem einzelnen Shelf pro Standort ein zusätzliches Shelf hinzugefügt wird, wenden die Systeme die vierteljährlichen Regeln für die Zuweisung von Shelfs auf das neue Shelf an.

Verwandte Informationen

"Erforderliche MetroCluster IP-Komponenten und Namenskonventionen"

"Festplatten- und Aggregatmanagement"

ADP- und Festplattenzuordnungsunterschiede nach System in MetroCluster IP-Konfigurationen

Der Betrieb von ADP (Advanced Drive Partitioning) und die automatische Festplattenzuordnung in MetroCluster IP Konfigurationen variiert je nach Systemmodell.

> In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird. Das Root-Aggregat wird mithilfe von P3-Partitionen erstellt.

Sie müssen die MetroCluster-Grenzwerte für die maximale Anzahl unterstützter Laufwerke und anderer Richtlinien einhalten.

"NetApp Hardware Universe"

ADP und Festplattenzuordnung auf AFF A320-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP- und Festplattenzuordnung für AFF Systeme A150, ASA A150 und AFF A220

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	Nur interne Laufwerke	Die internen Laufwerke sind in vier gleiche Gruppen unterteilt. Jede Gruppe wird automatisch einem separaten Pool zugewiesen, und jeder Pool wird einem separaten Controller in der Konfiguration zugewiesen. **Hinweis:** die Hälfte der internen Laufwerke bleibt nicht zugewiesen, bevor MetroCluster konfiguriert wird.	Das lokale HA-Paar verwendet zwei Quartale. Die anderen zwei Quartale werden von dem Remote HA-Paar verwendet. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

Mindestens unterstützte Laufwerke (pro Standort)	16 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen. Zwei Viertel auf einem Regal können den gleichen Pool haben. Der Pool wird basierend auf dem Knoten ausgewählt, der das Quartal besitzt: • Wenn der Eigentümer des lokalen Knotens ist, wird Pool0 verwendet. • Wenn der Remote-Knoten im Besitz ist, wird Pool1 verwendet. Ein Shelf mit den Quartalen Q1 bis Q4 kann beispielsweise folgende Aufgaben haben: • Q1: Node_A_1 pool0 • Q2: Node_A_2 pool0 • Q3: Node_B_1 pool1 • Q4:Node_B_2 Pool1 **Hinweis:** die Hälfte der internen Laufwerke bleibt nicht zugewiesen, bevor MetroCluster konfiguriert wird.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzteile

ADP- und Festplattenzuweisung für AFF A250, AFF C250, ASA A250, ASA C250, FAS500f, AFF A20, AFF A30 und AFF C30 Systeme

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	16 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzpartitionen

ADP und Festplattenzuweisung auf AFF A50 und AFF C60 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Das lokale HA-Paar verwendet ein Shelf. Das Remote-HA-Paar verwendet das zweite Shelf. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzpartitionen

ADP und Festplattenzuordnung auf AFF A300 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP- und Festplattenzuweisung auf AFF C400-, AFF A400-, ASA C400- und ASA A400-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen

Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP und Festplattenzuordnung auf AFF A700 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP und Festplattenzuweisung auf AFF C800, ASA C800, ASA A800 und AFF A800 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Aggregat

Minimal empfohlene Laufwerke (pro Standort)	Interne Laufwerke und 96 externe Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Shelfs werden automatisch Shelf-einzeln zugewiesen, wobei allen Laufwerken in jedem Shelf einer der vier Nodes in der MetroCluster-Konfiguration zugewiesen ist.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen **Hinweis:** das Root-Aggregat wird mit 12 Root-Partitionen auf dem internen Regal erstellt.
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartitionen **Hinweis:** das Root-Aggregat wird mit 12 Root-Partitionen auf dem internen Regal erstellt.

ADP- und Festplattenzuweisung auf AFF A70-, AFF A90- und AFF C80-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Aggregat

Minimal empfohlene Laufwerke (pro Standort)	Interne Laufwerke und 96 externe Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Shelfs werden automatisch Shelf-einzeln zugewiesen, wobei allen Laufwerken in jedem Shelf einer der vier Nodes in der MetroCluster-Konfiguration zugewiesen ist.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartitionen

ADP- und Festplattenzuordnung für AFF Systeme A900, ASA A900 und AFF A1K

Richtlinie	Shelves pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

Festplattenzuordnung bei FAS2750 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	24 interne Laufwerke und 24 externe Laufwerke	Die internen und externen Regale sind in zwei gleiche Hälften unterteilt. Jede Hälfte wird automatisch einem anderen Pool zugewiesen	Keine Angabe
Minimal unterstützte Laufwerke (pro Standort) (aktiv/Passiv HA-Konfiguration)	Nur interne Laufwerke	Manuelle Zuweisung erforderlich	Keine Angabe

Festplattenzuordnung bei FAS8200 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf den externen Shelfs sind in zwei gleiche Gruppen (Hälften) unterteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
Minimal unterstützte Laufwerke (pro Standort) (aktiv/Passiv HA-Konfiguration)	24 Laufwerke	Manuelle Zuweisung erforderlich.	Keine Angabe

Festplattenzuordnung auf FAS500f Systemen

Für FAS500f Systeme gelten die gleichen Richtlinien und Regeln für die Festplattenzuordnung bei AFF C250 und AFF A250 Systemen. Informationen zur Festplattenzuordnung bei FAS500f Systemen finden Sie im [ADP_FAS500f] Tabelle:

Festplattenzuordnung auf FAS9000, FAS9500, FAS70 und FAS90 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Keine Angabe

Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe

Festplattenzuordnung auf FAS50 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe

Anforderungen für Cluster-Peering in MetroCluster IP-Konfigurationen

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.

ISL-Anforderungen

Inter-Switch-Link-Anforderungen für MetroCluster IP-Konfigurationen

Überprüfen Sie, ob Ihre MetroCluster IP-Konfiguration und Ihr Netzwerk alle ISL-Anforderungen (Inter-Switch Link) erfüllen. Obwohl bestimmte Anforderungen nicht auf Ihre Konfiguration zutreffen, sollten Sie dennoch alle ISL-Anforderungen kennen, um ein besseres Verständnis der Gesamtkonfiguration zu erhalten.

Die folgende Tabelle bietet einen Überblick über die in diesem Abschnitt behandelten Themen.

Titel	Beschreibung
"Von NetApp validierte und MetroCluster-konforme Switches"	Beschreibt die Switch-Anforderungen. Gilt für alle in MetroCluster-Konfigurationen verwendeten Switches, einschließlich Backend-Switches.
"Überlegungen für ISLs"	Beschreibt die ISL-Anforderungen. Gilt für alle MetroCluster Konfigurationen, unabhängig von der Netzwerktopologie und ob Sie NetApp validierte Switches oder MetroCluster konforme Switches verwenden.
"Überlegungen bei der Bereitstellung von MetroCluster in einem gemeinsam genutzten Layer-2- oder Layer-3-Netzwerk"	Beschreibt die Anforderungen für gemeinsam genutzte Layer-2- oder Layer-3-Netzwerke. Gilt für alle Konfigurationen mit Ausnahme von MetroCluster Konfigurationen mit von NetApp validierten Switches und mit direkt verbundenen ISLs.
"Überlegungen beim Einsatz von MetroCluster-kompatiblen Switches"	Beschreibt die Anforderungen für MetroCluster-konforme Switches. Gilt für alle MetroCluster Konfigurationen ohne NetApp validierte Switches.
"Beispiele für MetroCluster Netzwerktopologien"	Enthält Beispiele verschiedener MetroCluster-Netzwerktopologien. Gilt für alle MetroCluster Konfigurationen.

NetApp-validierte und MetroCluster-kompatible Switches in einer MetroCluster IP-Konfiguration

Alle in der Konfiguration verwendeten Switches, einschließlich Backend-Switches, müssen entweder NetApp-validiert oder MetroCluster konform sein.

Von NetApp validierte Switches

Ein Switch wird von NetApp validiert, wenn er die folgenden Anforderungen erfüllt:

- Der Switch wird von NetApp im Rahmen der MetroCluster IP Konfiguration bereitgestellt
- Der Switch ist im aufgeführt "NetApp Hardware Universe" Als unterstützter Switch unter *MetroCluster-over-IP-connections*
- Der Switch wird nur verwendet, um MetroCluster IP-Controller und in einigen Konfigurationen NS224-Laufwerk-Shelfs zu verbinden
- Der Switch wird mit der von NetApp bereitgestellten Referenzkonfigurationsdatei (RCF) konfiguriert

Jeder Switch, der diese Anforderungen nicht erfüllt, ist **nicht** ein von NetApp validierter Switch.

MetroCluster-konforme Switches

Ein MetroCluster-konformer Switch ist nicht von NetApp validiert, kann aber in einer MetroCluster IP-Konfiguration verwendet werden, wenn er bestimmte Anforderungen und Konfigurationsrichtlinien erfüllt.

> NetApp bietet keine Services zur Fehlerbehebung oder Konfiguration von Support für nicht validierte MetroCluster-kompatible Switches.

Anforderungen für Inter-Switch Links (ISLs) in MetroCluster -IP-Konfigurationen

Inter-Switch Links (ISLs), die MetroCluster-Datenverkehr auf allen MetroCluster IP-Konfigurationen und Netzwerktopologien übertragen, haben bestimmte Anforderungen. Diese Anforderungen gelten für alle ISLs, die MetroCluster-Datenverkehr tragen, unabhängig davon, ob die ISLs direkt sind oder von den Kunden-Switches gemeinsam genutzt werden.

Allgemeine MetroCluster-ISL-Anforderungen

Folgendes gilt für ISLs in allen MetroCluster IP-Konfigurationen:

- Beide Fabrics müssen die gleiche Anzahl von ISLs aufweisen.
- ISLs in einer Fabric müssen alle dieselbe Geschwindigkeit und Länge haben.
- ISLs müssen in beiden Fabrics dieselbe Geschwindigkeit und Länge haben.
- Die maximale unterstützte Differenz im Abstand zwischen Fabric 1 und Fabric 2 beträgt 20 km oder 0,2 ms.
- Die ISLs müssen über dieselbe Topologie verfügen. Sie sollten beispielsweise alle direkte Links sein, oder wenn die Konfiguration WDM verwendet, müssen alle WDM verwenden.
- Die ISL-Geschwindigkeit muss mindestens 10 Gbit/s betragen.
- Es muss mindestens ein 10 Gbit/s-ISL-Port pro Fabric geben.

Grenzwerte für Latenz und Paketverlust in den ISLs

Folgendes gilt für den Rundreiseverkehr zwischen den MetroCluster-IP-Switches an Standort_A und Standort_B, wobei die MetroCluster-Konfiguration im stabilen Betrieb ist:

- Mit zunehmender Entfernung zwischen zwei MetroCluster Standorten steigt die Latenz, in der Regel im Bereich von 1 ms Paketumlaufzeit pro 100 km (62 Meilen). Die Latenz hängt auch von der SLA (Network Service Level Agreement) ab, was die Bandbreite der ISL-Verbindungen, die Paketdrop-Rate und den Jitter im Netzwerk betrifft. Geringe Bandbreite, hoher Jitter und zufällige Paketabbrüche führen zu verschiedenen Wiederherstellungsmechanismen durch die Switches oder die TCP-Engine auf den Controller-Modulen für eine erfolgreiche Paketzustellung. Diese Recovery-Mechanismen können die Latenz insgesamt erhöhen. Spezifische Informationen zur Latenz bei und für die maximale Entfernung Ihrer Konfiguration finden Sie im "Hardware Universe:"
- Geräte, die zur Latenz beitragen, müssen berücksichtigt werden.
- Der "Hardware Universe:" Bietet die Entfernung in km. Sie müssen für alle 100 km 1 ms zuweisen. Der maximale Abstand wird durch das zuerst erreichte definiert, entweder durch die maximale Rundreisezeit (RTT) in ms oder durch den Abstand in km Beispiel: Wenn *das Hardware Universe* eine Entfernung von 300 km auflistet, die auf 3 ms übersetzt wird, kann Ihr ISL nicht weiter als 300 km sein und der maximale RTT nicht mehr als 3 ms überschreiten – je nachdem, welcher Wert zuerst erreicht wird.
- Paketverlust muss kleiner oder gleich 0.01 % sein. Der maximale Paketverlust ist die Summe aller Verluste auf allen Verbindungen auf dem Pfad zwischen den MetroCluster-Knoten und der Verlust auf den lokalen MetroCluster-IP-Schnittstellen.
- Der unterstützte Jitter-Wert beträgt 3 ms für die Rundreise (oder 1,5 ms für die einfache Strecke).
- Das Netzwerk sollte die für den MetroCluster-Datenverkehr erforderliche SLA-Bandbreite zuweisen und aufrechterhalten, unabhängig von Mikroplatzausbrüchen und Spitzen im Datenverkehr.
- Bei Verwendung von ONTAP 9.7 oder höher muss das Zwischennetzwerk zwischen den beiden Standorten eine Mindestbandbreite von 4,5 Gbit/s für die MetroCluster IP-Konfiguration bereitstellen.

Hinweise zu Transceiver und Kabeln

SFPs oder QSFPs, die vom Geräteanbieter unterstützt werden, werden von den MetroCluster ISLs unterstützt. SFP-Module und QSFPs von NetApp oder vom Geräteanbieter müssen von der Switch- und Switch-Firmware unterstützt werden.

Beim Anschließen der Controller an die Switches und die lokalen Cluster-ISLs müssen Sie die Transceiver und Kabel verwenden, die von NetApp mit dem MetroCluster bereitgestellt werden.

Wenn Sie einen QSFP-SFP-Adapter verwenden, hängt es vom Switch-Modell und der Firmware ab, ob Sie den Port im Breakout- oder im nativen Geschwindigkeitsmodus konfigurieren. Beispielsweise muss der Port bei der Verwendung eines QSFP-SFP-Adapters mit Cisco 9336C Switches mit der NX-OS-Firmware 9.x oder 10.x im nativen Geschwindigkeitsmodus konfiguriert werden.

> Wenn Sie eine RCF konfigurieren, überprüfen Sie, ob Sie den richtigen Geschwindigkeitsmodus auswählen oder einen Port mit einem geeigneten Geschwindigkeitsmodus verwenden.

Verwenden von xWDM, TDM und externen Verschlüsselungsgeräten

Wenn Sie xWDM-/TDM-Geräte oder -Geräte verwenden, die in einer MetroCluster IP-Konfiguration verschlüsselt werden, muss Ihre Umgebung die folgenden Anforderungen erfüllen:

- Beim Anschluss der MetroCluster IP-Switches an den xWDM/TDM müssen die externen Verschlüsselungsgeräte oder xWDM/TDM-Geräte vom Hersteller für den Switch und die Firmware

zertifiziert sein. Die Zertifizierung muss den Betriebsmodus abdecken (z. B. Trunking und Verschlüsselung).

- Die gesamte End-to-End-Latenz und der Jitter, einschließlich der Verschlüsselung, darf nicht höher sein als die in der IMT und in dieser Dokumentation angegebene Höchstmenge.

Unterstützte Anzahl von ISLs und Breakout-Kabeln

Die folgende Tabelle zeigt die unterstützte maximale Anzahl von ISLs, die auf einem MetroCluster IP-Switch mithilfe der RCF-Konfiguration (Reference Configuration File) konfiguriert werden können.

MetroCluster IP-Switch-Modell	Porttyp	Maximale Anzahl von ISLs
Von Broadcom unterstützte BES-53248-Switches	Native Ports	4 ISLs mit 10 Gbit/s oder 25 Gbit/s.
Von Broadcom unterstützte BES-53248-Switches	Native Ports (Hinweis 1)	2 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 3132Q-V	Native Ports	6 ISLs mit 40 Gbit/s.
Cisco 3132Q-V	Breakout-Kabel	16 ISLs mit 10 Gbit/s
Cisco 3232C	Native Ports	6 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 3232C	Breakout-Kabel	16 ISLs mit 10 Gbit/s oder 25 Gbit/s.
Cisco 9336C-FX2 (kein Anschluss von NS224-Shelfs)	Native Ports	6 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 9336C-FX2 (kein Anschluss von NS224-Shelfs)	Breakout-Kabel	16 ISLs mit 10 Gbit/s oder 25 Gbit/s.
Cisco 9336C-FX2 (Anschluss von NS224-Shelfs)	Native Ports (Hinweis 2)	4 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 9336C-FX2 (Anschluss von NS224-Shelfs)	Breakout-Kabel (Hinweis 2)	16 ISLs mit 10 Gbit/s oder 25 Gbit/s.
NVIDIA SN2100	Native Ports (Hinweis 2)	2 ISLs mit 40 Gbit/s oder 100 Gbit/s.
NVIDIA SN2100	Breakout-Kabel (Hinweis 2)	8 ISLs mit 10 Gbit/s oder 25 Gbit/s.

Hinweis 1: Die Verwendung von 40 Gbit/s oder 100 Gbit/s ISLs auf einem BES-53248 Switch erfordert eine zusätzliche Lizenz.

Hinweis 2: Die gleichen Ports werden für den nativen Geschwindigkeits- und Breakout-Modus verwendet. Sie

müssen beim Erstellen der RCF-Datei Ports im einheitlichen Geschwindigkeitsmodus oder im Breakout-Modus verwenden.

- Alle ISLs an einem MetroCluster IP-Switch müssen die gleiche Geschwindigkeit aufweisen. Es wird nicht unterstützt, verschiedene ISL-Ports mit unterschiedlichen Geschwindigkeiten gleichzeitig zu verwenden.
- Um eine optimale Leistung zu erzielen, sollten Sie mindestens eine 40-Gbit/s-ISL pro Netzwerk verwenden. Sie sollten für FAS9000, AFF A700 oder andere Plattformen mit hoher Kapazität keine ISL mit 10 Gbit/s pro Netzwerk verwenden.

> NetApp empfiehlt, eine kleine Anzahl von ISLs mit hoher Bandbreite zu konfigurieren, anstatt eine hohe Anzahl von ISLs mit niedriger Bandbreite. Es wird beispielsweise bevorzugt, eine 40-Gbit/s-ISL anstelle von vier 10-Gbit/s-ISLs zu konfigurieren. Bei Verwendung mehrerer ISLs kann sich der statistische Lastausgleich auf den maximalen Durchsatz auswirken. Bei einer ungleichmäßigen Verteilung kann der Durchsatz auf einen einzelnen ISL reduziert werden.

Voraussetzungen für die Bereitstellung von MetroCluster IP-Konfigurationen in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken

Je nach Ihren Anforderungen können Sie gemeinsam genutzte Layer-2- oder Layer-3-Netzwerke zur Implementierung von MetroCluster verwenden.

Ab ONTAP 9.6 können MetroCluster IP-Konfigurationen mit unterstützten Switches vorhandene Netzwerke für ISLs (Inter-Switch Links) gemeinsam nutzen, anstatt dedizierte MetroCluster-ISLs zu verwenden. Diese Topologie wird als *Shared Layer 2 Networks* bezeichnet.

Ab ONTAP 9.9 können MetroCluster IP-Konfigurationen mit IP-Routing (Layer 3)-Backend-Verbindungen implementiert werden. Diese Topologie wird als *Shared Layer 3 Networks* bezeichnet.

> - Nicht alle Funktionen werden in allen Netzwerktopologien unterstützt.
> - Sie müssen überprüfen, ob Sie über ausreichende Netzwerkkapazität verfügen und ob die ISL-Größe für Ihre Konfiguration geeignet ist. Eine niedrige Latenz ist für die Replizierung von Daten zwischen den MetroCluster Standorten von großer Bedeutung. Latenzprobleme auf diesen Verbindungen können sich nachteilig auf das Client-I/O auswirken
> - Alle Verweise auf MetroCluster Backend-Switches beziehen sich auf NetApp validierte Switches oder MetroCluster konforme Switches. Siehe "Von NetApp validierte und MetroCluster-konforme Switches" Entnehmen.

ISL-Anforderungen für Layer-2- und Layer-3-Netzwerke

Folgendes gilt für Layer-2- und Layer-3-Netzwerke:

- Die Geschwindigkeit und Anzahl der ISLs zwischen den MetroCluster Switches und den mittleren Netzwerk-Switches müssen nicht übereinstimmen. Ebenso muss die Geschwindigkeit zwischen den mittleren Netzwerk-Switches nicht übereinstimmen.

  MetroCluster Switches können beispielsweise über eine 40-Gbit/s-ISL mit den Intermediate Switches verbunden werden, wobei die Intermediate Switches über zwei 100-Gbit/s-ISLs miteinander verbunden werden können.

- Die Netzwerküberwachung sollte im Zwischennetzwerk konfiguriert werden, um die ISLs auf Auslastung, Fehler (Abgänge, Verbindungsklappen, Beschädigungen usw.) zu überwachen. und Ausfällen.

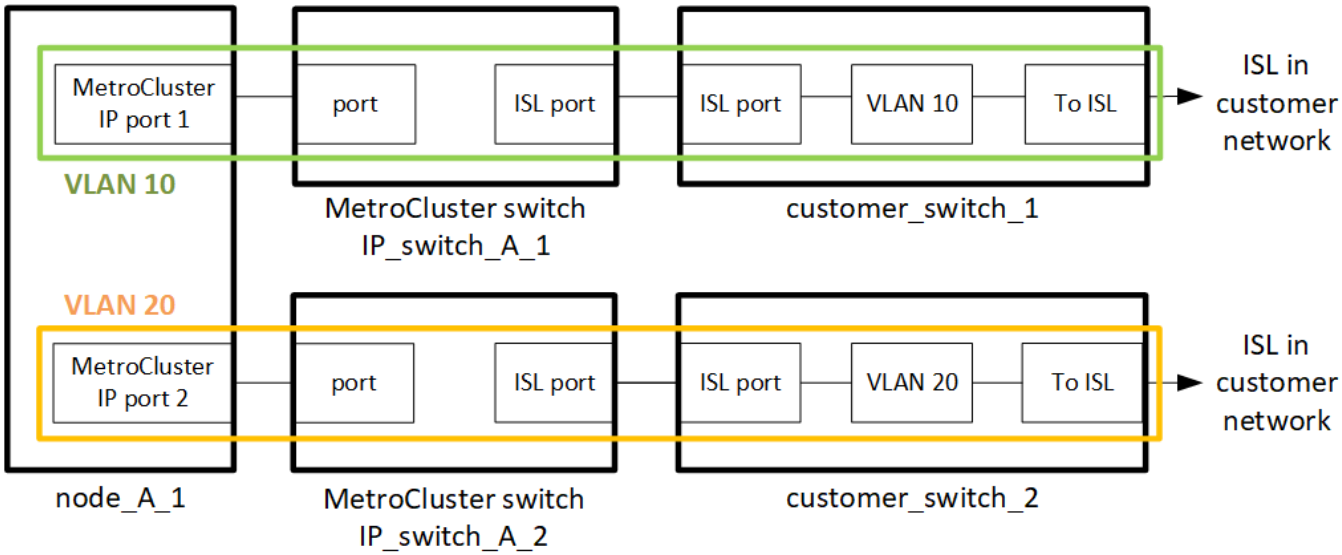
- Die MTU-Größe muss für alle Ports mit MetroCluster-End-to-End-Datenverkehr auf 9216 eingestellt sein.
- Kein anderer Datenverkehr kann mit einer höheren Priorität konfiguriert werden als Class of Service (COS) 5.
- Die explizite Staubenachrichtigung (ECN) muss auf allen Pfaden konfiguriert werden, die End-to-End-MetroCluster-Datenverkehr übertragen.
- ISLs, die MetroCluster Traffic tragen, müssen native Links zwischen den Switches sein.

  Link-Sharing-Dienste wie Multiprotocol Label Switching (MPLS)-Links werden nicht unterstützt.

- Die Layer-2-VLANs müssen nativ über die Standorte hinweg eingesetzt werden. VLAN-Overlay wie Virtual Extensible LAN (VXLAN) wird nicht unterstützt.
- Die Anzahl der Zwischenschalter ist nicht begrenzt. NetApp empfiehlt jedoch, die Anzahl der Switches auf die erforderliche Mindestzahl zu beschränken.
- ISLs in MetroCluster Switches sind mit folgenden Konfigurationen konfiguriert:
  - Switch Port-Modus 'Trunk' als Teil eines LACP Port-Channels
  - Die MTU-Größe beträgt 9216
  - Es ist kein natives VLAN konfiguriert
  - Nur VLANs, die standortübergreifenden MetroCluster-Datenverkehr übertragen, sind zulässig
  - Das Standard-VLAN des Switches ist nicht zulässig

Überlegungen für Layer-2-Netzwerke

Die MetroCluster Backend-Switches sind mit dem Kundennetzwerk verbunden.



Die vom Kunden bereitgestellten Zwischenschalter müssen die folgenden Anforderungen erfüllen:

- Das Zwischennetzwerk muss die gleichen VLANs zwischen den Standorten bereitstellen. Dies muss mit den in der RCF-Datei festgelegten MetroCluster-VLANs übereinstimmen.
- Der RcfFileGenerator erlaubt das Erstellen einer RCF-Datei nicht mit VLANs, die von der Plattform nicht unterstützt werden.
- Der RcfFileGenerator kann beispielsweise die Verwendung bestimmter VLAN-IDs einschränken, wenn diese für die zukünftige Verwendung vorgesehen sind. Im Allgemeinen sind reservierte VLANs bis

einschließlich 100.

- Layer-2-VLANs mit IDs, die zu den MetroCluster-VLAN-IDs passen, müssen das gemeinsam genutzte Netzwerk umfassen.

VLAN-Konfiguration in ONTAP

Sie können das VLAN nur während der Schnittstellenerstellung angeben. Sie können die Standard-VLANs 10 und 20 oder VLANs im Bereich von 101 bis 4096 (oder die vom Switch-Anbieter unterstützte Anzahl, je nachdem, welcher Wert niedriger ist) konfigurieren. Nachdem die MetroCluster-Schnittstellen erstellt wurden, können Sie die VLAN-ID nicht mehr ändern.

> Einige Switch-Anbieter reservieren möglicherweise die Nutzung bestimmter VLANs.

Für die folgenden Systeme ist keine VLAN-Konfiguration innerhalb von ONTAP erforderlich. Das VLAN wird durch die Switch-Port-Konfiguration festgelegt:

- FAS8200 UND AFF A300
- AFF A320
- FAS9000 und AFF A700
- AFF A800, ASA A800, AFF C800 und ASA C800

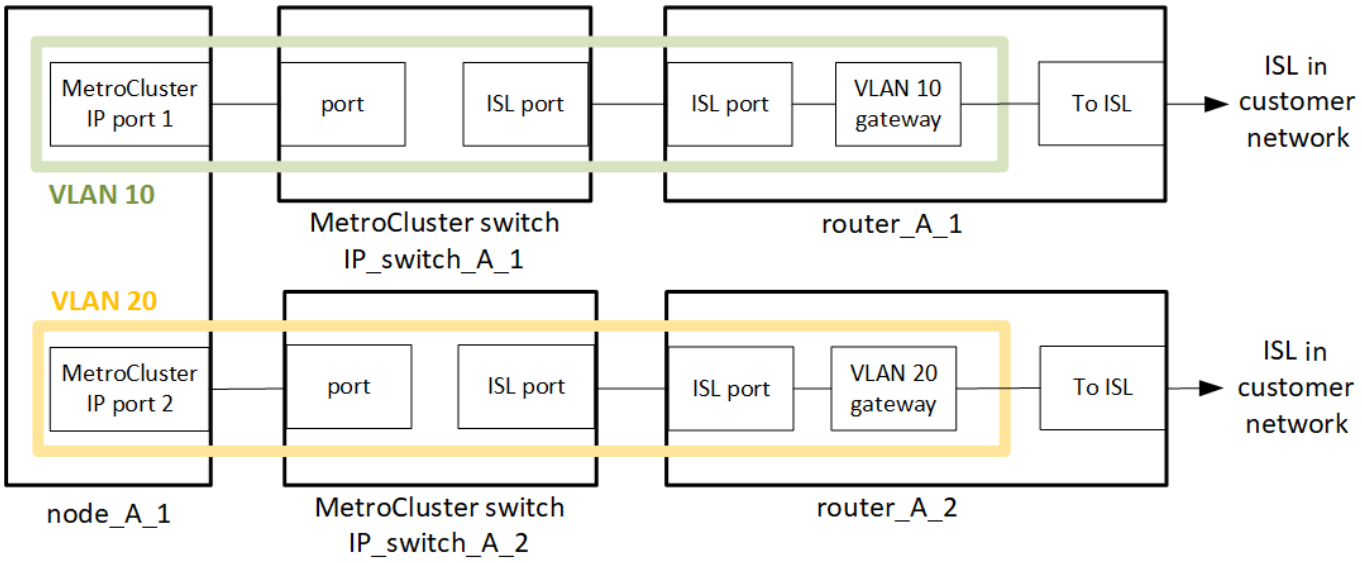
> Die oben aufgeführten Systeme können mit VLANs 100 und niedriger konfiguriert werden. Einige VLANs in diesem Bereich sind jedoch möglicherweise für andere oder zukünftige Zwecke reserviert.

Bei allen anderen Systemen müssen Sie das VLAN konfigurieren, wenn Sie die MetroCluster-Schnittstellen in ONTAP erstellen. Es gelten die folgenden Einschränkungen:

- Das Standard-VLAN ist 10 und 20
- Wenn Sie ONTAP 9.7 oder früher verwenden, können Sie nur die Standard-VLAN 10 und 20 verwenden.
- Wenn Sie ONTAP 9.8 oder höher verwenden, können Sie das Standard-VLAN 10 und 20 verwenden, und ein VLAN über 100 (101 und höher) kann auch verwendet werden.

Überlegungen für Layer-3-Netzwerke

Die Back-End-Switches von MetroCluster sind mit dem gerouteten IP-Netzwerk verbunden, entweder direkt mit Routern (wie im folgenden vereinfachten Beispiel dargestellt) oder über andere intervenierenden Switches.



Die MetroCluster Umgebung ist wie in beschrieben als MetroCluster IP-Standardkonfiguration konfiguriert und verkabelt "Konfigurieren Sie die Hardwarekomponenten von MetroCluster". Wenn Sie das Installations- und Verkabelungsverfahren durchführen, müssen Sie die für eine Layer-3-Konfiguration spezifischen Schritte ausführen. Folgendes gilt für Layer-3-Konfigurationen:

- Sie können MetroCluster-Switches direkt an den Router oder an einen oder mehrere dazwischenliegenden Switches anschließen.
- Sie können MetroCluster IP-Schnittstellen direkt an den Router oder an einen der dazwischen liegenden Switches anschließen.
- Das VLAN muss auf das Gateway-Gerät erweitert werden.
- Sie verwenden das `-gateway parameter` So konfigurieren Sie die IP-Schnittstellenadresse des MetroCluster mit einer IP-Gateway-Adresse.
- Die VLAN-IDs für die MetroCluster-VLANs müssen an jedem Standort identisch sein. Die Subnetze können jedoch anders sein.
- Dynamisches Routing wird für den MetroCluster-Datenverkehr nicht unterstützt.
- Die folgenden Funktionen werden nicht unterstützt:
  - MetroCluster Konfigurationen mit acht Nodes
  - Aktualisieren einer MetroCluster-Konfiguration mit vier Nodes
  - Umstellung von MetroCluster FC auf MetroCluster IP
- An jedem MetroCluster Standort sind zwei Subnetze erforderlich – eins in jedem Netzwerk.
- Die Auto-IP-Zuweisung wird nicht unterstützt.

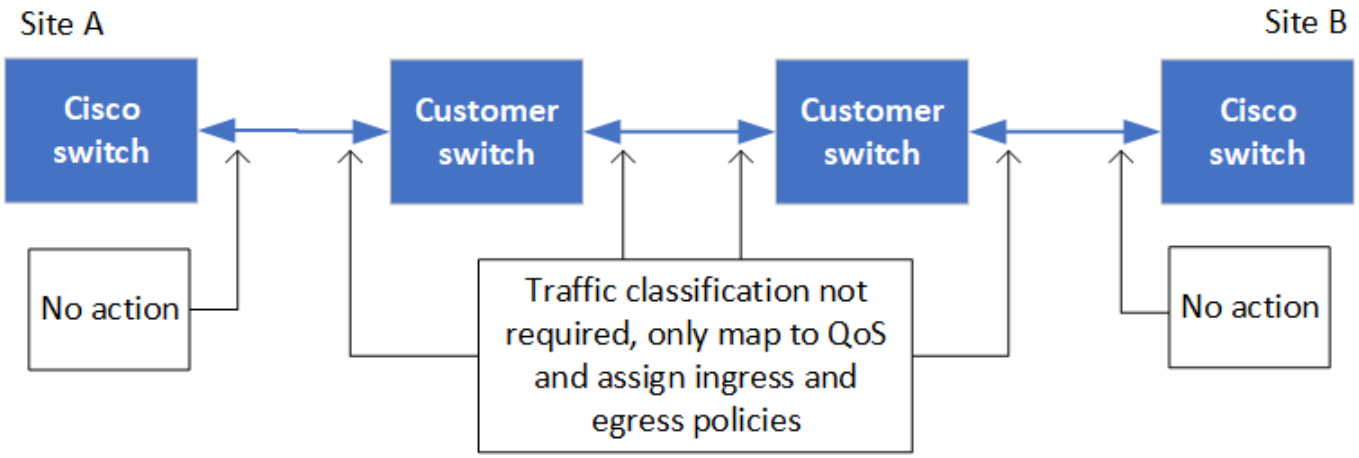
Wenn Sie Router und Gateway-IP-Adressen konfigurieren, müssen Sie die folgenden Anforderungen erfüllen:

- Zwei Schnittstellen auf einem Node können nicht die gleiche Gateway-IP-Adresse aufweisen.
- Die entsprechenden Schnittstellen auf den HA-Paaren an jedem Standort müssen über dieselbe Gateway-IP-Adresse verfügen.
- Die entsprechenden Schnittstellen auf einem Node und seinen DR- und AUX-Partnern können nicht dieselbe Gateway-IP-Adresse haben.
- Die entsprechenden Schnittstellen auf einem Node und seinen DR- und AUX-Partnern müssen dieselbe VLAN-ID aufweisen.

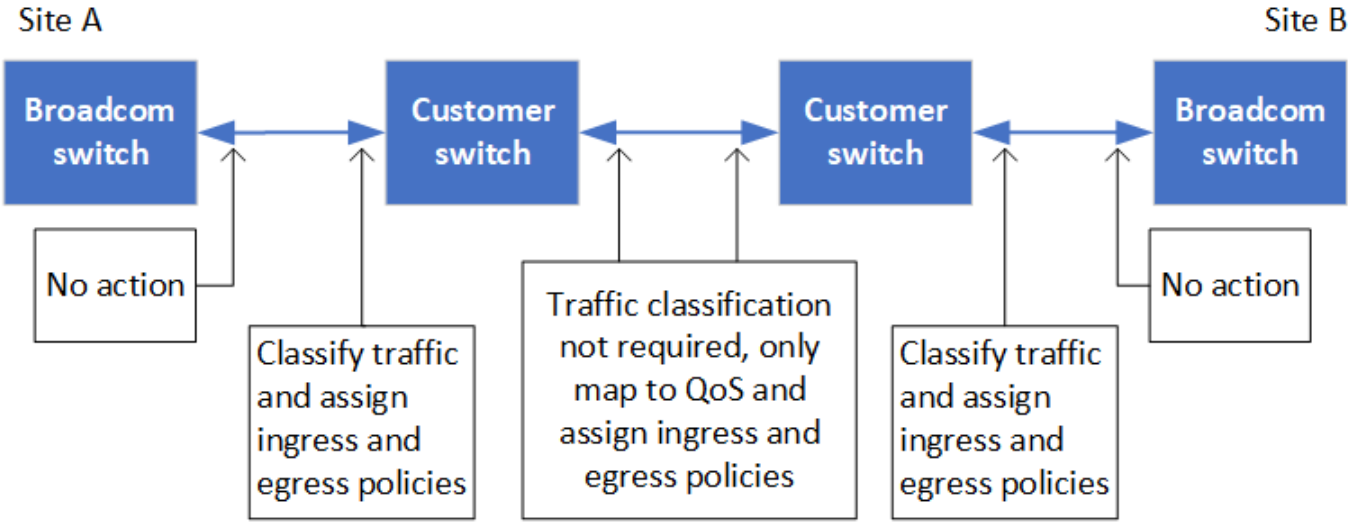
Erforderliche Einstellungen für Zwischenschalter

Wenn MetroCluster-Verkehr in einem mittleren Netzwerk eine ISL durchquert, sollten Sie überprüfen, ob die Konfiguration der mittleren Switches sicherstellt, dass der MetroCluster-Verkehr (RDMA und Storage) über den gesamten Pfad zwischen den MetroCluster Standorten die erforderlichen Service-Level erfüllt.

Das folgende Diagramm gibt eine Übersicht über die erforderlichen Einstellungen bei Verwendung von NetApp Validated Cisco Switches:



Das folgende Diagramm gibt einen Überblick über die erforderlichen Einstellungen für ein freigegebenes Netzwerk, wenn es sich bei den externen Switches um Broadcom-IP-Switches handelt.



In diesem Beispiel werden für den MetroCluster-Datenverkehr die folgenden Richtlinien und Zuordnungen erstellt:

- Der `MetroClusterIP_ISL_Ingress` Die Richtlinie wird auf Ports auf dem Zwischenswitch angewendet, der eine Verbindung zu den MetroCluster IP-Switches herstellt.

  Der `MetroClusterIP_ISL_Ingress` Die Richtlinie ordnet den eingehenden gekennzeichneten Datenverkehr der entsprechenden Warteschlange auf dem Zwischenswitch zu.

- A `MetroClusterIP_ISL_Egress` Die Richtlinie wird auf Ports auf dem Zwischenswitch angewendet, die mit ISLs zwischen Zwischenswitches verbunden sind.

- Sie müssen die Zwischen-Switches mit übereinstimmenden QoS-Zugriffskarten, Klassenkarten und Richtlinienzuordnungen zwischen den MetroCluster IP-Switches konfigurieren. Die Zwischen-Switches weisen den RDMA-Datenverkehr auf COS5 und den Storage-Datenverkehr auf COS4 zu.

Die folgenden Beispiele gelten für Cisco Nexus 3232C- und 9336C-FX2-Switches. Je nach Switch-Hersteller und -Modell müssen Sie überprüfen, ob Ihre Zwischenswitches über eine geeignete Konfiguration verfügen.

Konfigurieren Sie die Klassenzuordnung für den ISL-Port des Zwischenswitters

Das folgende Beispiel zeigt die Klassenzuordnungsdefinitionen, je nachdem, ob der Datenverkehr beim Eindringen klassifiziert oder abgeglichen werden muss.

Klassifizieren des Datenverkehrs beim Eindringen:

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

Datenverkehr beim Eindringen abgleichen:

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

Erstellen Sie eine Eingangs-Policy Map auf dem ISL-Port des Intermediate Switch:

Die folgenden Beispiele zeigen, wie Sie eine Eingangs-Policy-Map erstellen, je nachdem, ob Sie den Datenverkehr beim Eindringen klassifizieren oder abgleichen müssen.

Klassifizieren Sie den Verkehr beim Eindringen:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Gleichen Sie den Datenverkehr beim Eindringen ab:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Konfigurieren Sie die Ausgangs-Queuing-Richtlinie für die ISL-Ports

Das folgende Beispiel zeigt, wie die Richtlinie für die Ausgangs-Warteschlange konfiguriert wird:

```
policy-map type queuing MetroClusterIP_ISL_Egress
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2
   class type queuing c-out-8q-q5
      priority level 3
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q4
      priority level 4
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q3
      priority level 5
   class type queuing c-out-8q-q2
      priority level 6
   class type queuing c-out-8q-q1
      priority level 7
   class type queuing c-out-8q-q-default
      bandwidth remaining percent 100
      random-detect threshold burst-optimized ecn
```

Diese Einstellungen müssen auf alle Switches und ISLs angewendet werden, die MetroCluster-Datenverkehr tragen.

In diesem Beispiel werden Q4 und Q5 mit konfiguriert `random-detect threshold burst-optimized ecn`. Abhängig von Ihrer Konfiguration müssen Sie möglicherweise die minimalen und maximalen Schwellenwerte festlegen, wie im folgenden Beispiel gezeigt:

```
class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
kbytes drop-probability 0 weight 0 ecn
```

Die Mindest- und Höchstwerte variieren je nach Switch und Ihren Anforderungen.

Beispiel 1: Cisco

Wenn Ihre Konfiguration über Cisco Switches verfügt, müssen Sie den ersten Ingress-Port des Intermediate Switch nicht klassifizieren. Anschließend konfigurieren Sie die folgenden Zuordnungen und Richtlinien:

- `class-map type qos match-any c5`

- `class-map type qos match-any c4`
- `MetroClusterIP_ISL_Ingress_Match`

Sie weisen die zu `MetroClusterIP_ISL_Ingress_Match` Richtlinienzuordnung zu den ISL-Ports, die MetroCluster-Datenverkehr übertragen.

Beispiel 2: Broadcom

Wenn Ihre Konfiguration über Broadcom-Switches verfügt, müssen Sie den ersten Ingress-Port des Intermediate-Switches klassifizieren. Anschließend konfigurieren Sie die folgenden Zuordnungen und Richtlinien:

- `ip access-list rdma`
- `ip access-list storage`
- `class-map type qos match-all rdma`
- `class-map type qos match-all storage`
- `MetroClusterIP_ISL_Ingress_Classify`
- `MetroClusterIP_ISL_Ingress_Match`

Sie zuweisen `the MetroClusterIP_ISL_Ingress_Classify` Die Richtlinien werden den ISL-Ports auf dem Zwischenswitch zugeordnet, der den Broadcom-Switch verbindet.

Sie weisen die zu `MetroClusterIP_ISL_Ingress_Match` Die Richtlinien werden den ISL-Ports auf dem Zwischenswitch zugeordnet, der MetroCluster-Datenverkehr ausführt, aber keinen Broadcom-Switch verbindet.

Beispiele für die Netzwerktopologie der MetroCluster IP-Konfiguration

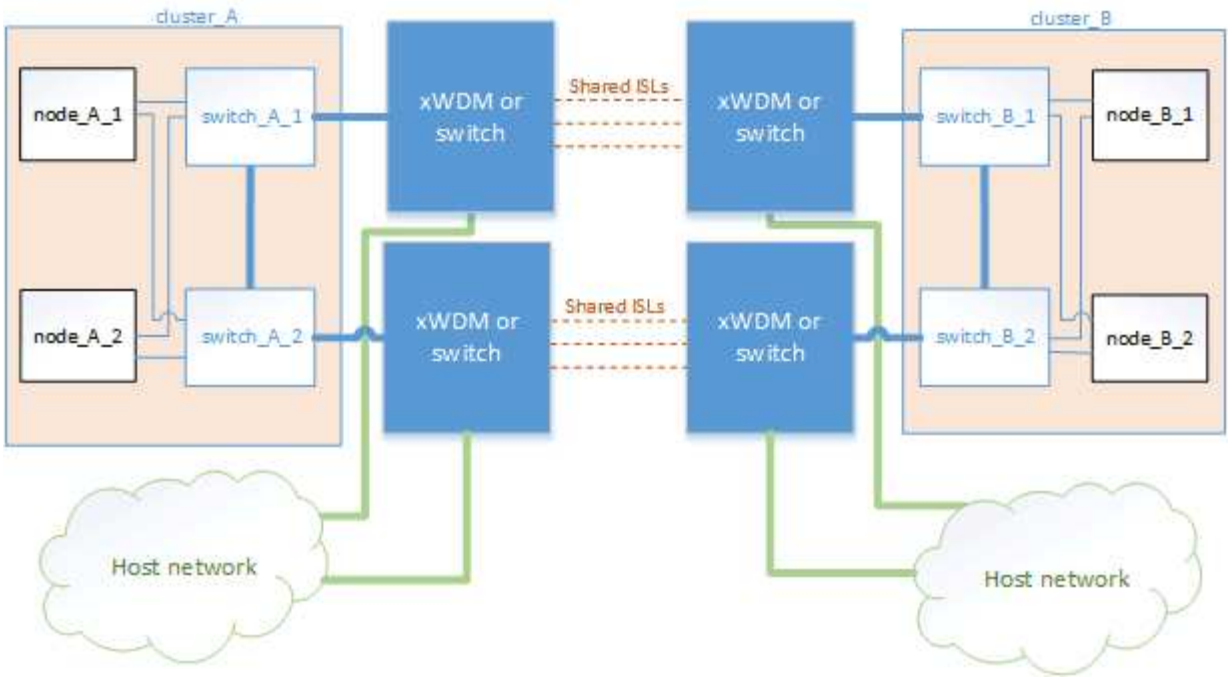
Ab ONTAP 9.6 werden einige zusätzliche Netzwerkkonfigurationen für MetroCluster IP-Konfigurationen unterstützt. Dieser Abschnitt enthält einige Beispiele für unterstützte Netzwerkkonfigurationen. Es werden nicht alle unterstützten Topologien aufgeführt.

In diesen Topologien wird davon ausgegangen, dass das ISL- und das Zwischennetzwerk entsprechend den in beschriebenen Anforderungen konfiguriert ist "Überlegungen für ISLs".

> Wenn Sie eine ISL für nicht-MetroCluster Verkehr freigeben, müssen Sie sicherstellen, dass die MetroCluster jederzeit mindestens über die erforderliche Mindestbandbreite verfügt.

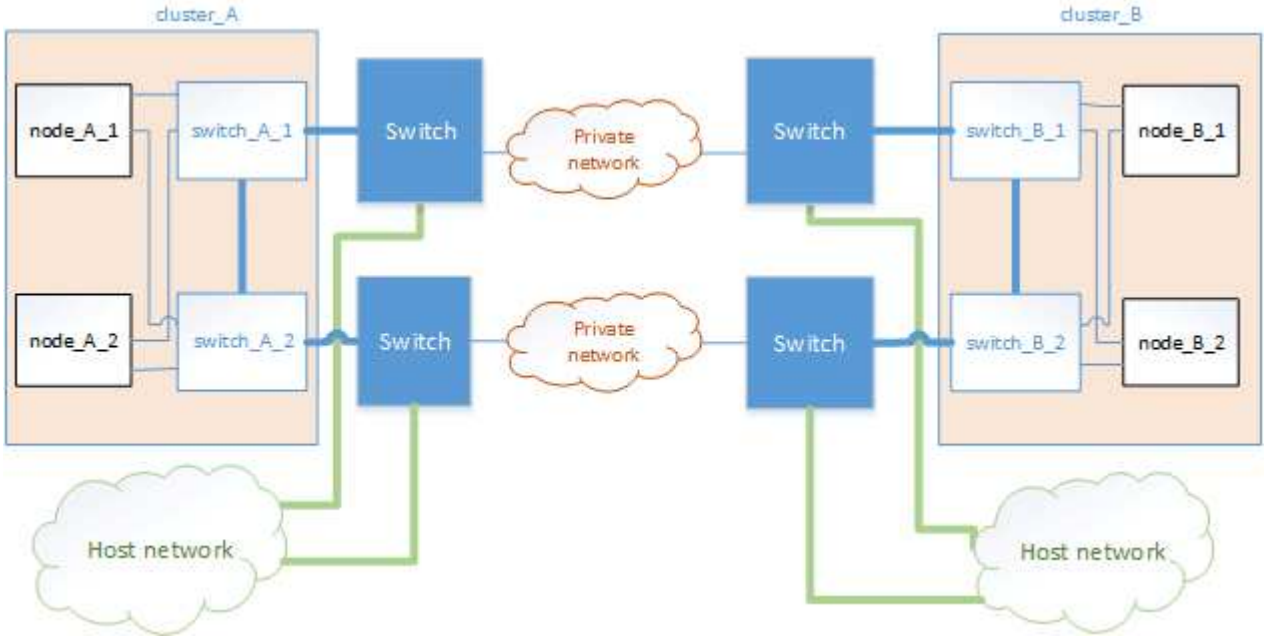
Konfiguration für gemeinsam genutztes Netzwerk mit direkten Links

In dieser Topologie sind zwei unterschiedliche Standorte durch direkte Links verbunden. Diese Verbindungen können zwischen xWDM- und TDM-Geräten oder -Switches bestehen. Die Kapazität der ISLs ist nicht für den MetroCluster-Verkehr reserviert, wird aber für anderen nicht-MetroCluster Verkehr freigegeben.



Gemeinsam genutzte Infrastruktur mit Zwischennetzen

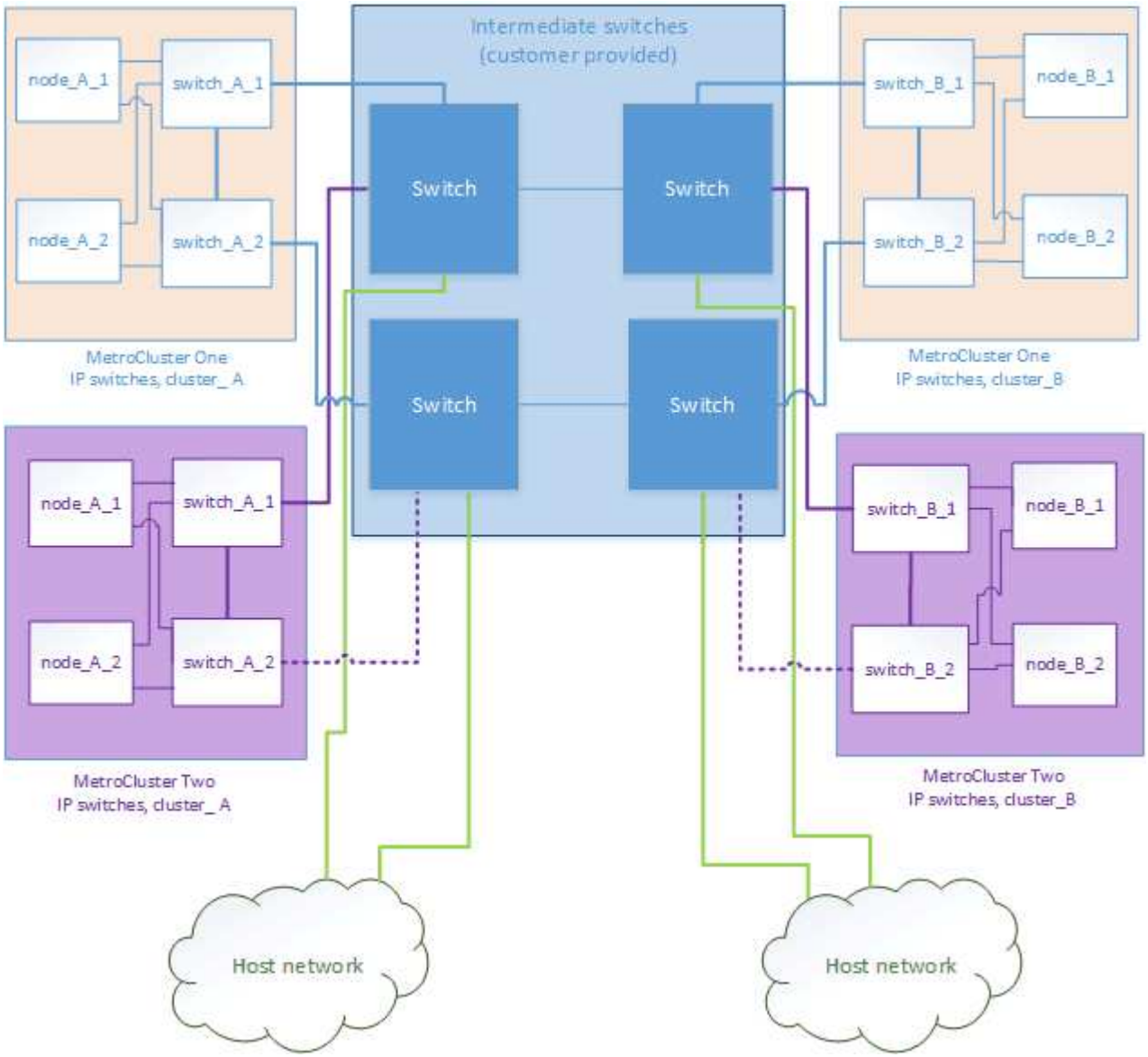
In dieser Topologie sind die MetroCluster-Standorte nicht direkt verbunden, sondern MetroCluster und der Host-Datenverkehr werden über ein Netzwerk geleitet.
Das Netzwerk kann aus einer Reihe von xWDM und TDM und Switches bestehen, aber im Gegensatz zur gemeinsamen Konfiguration mit direkten ISLs sind die Verbindungen nicht direkt zwischen den Standorten. Je nach Infrastruktur zwischen den Standorten ist eine beliebige Kombination von Netzwerkkonfigurationen möglich.



Mehrere MetroCluster-Konfigurationen nutzen ein Zwischennetzwerk

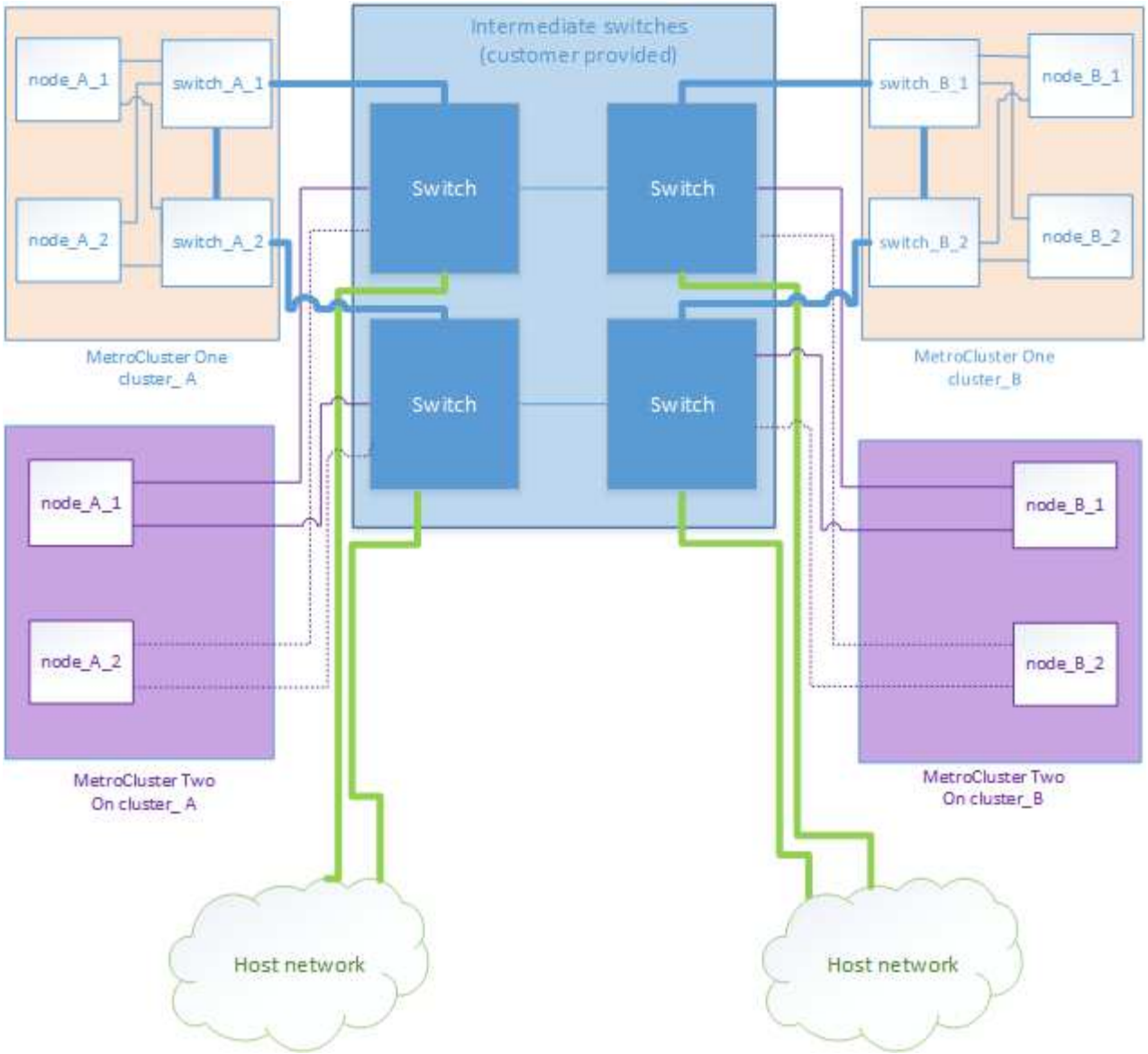
In dieser Topologie teilen sich zwei separate MetroCluster-Konfigurationen dasselbe Zwischennetzwerk. Im Beispiel MetroCluster One Switch_A_1 und MetroCluster Two Switch_A_1 verbinden sich beide mit demselben Zwischenswitch.

Sowohl „MetroCluster One“ als auch „MetroCluster Two“ kann eine MetroCluster Konfiguration mit acht Nodes oder zwei MetroCluster Konfigurationen mit vier Nodes sein.



Kombination einer MetroCluster Konfiguration mit validierten NetApp Switches und einer Konfiguration mit MetroCluster konformen Switches

Zwei separate MetroCluster Konfigurationen nutzen denselben Intermediate Switch, bei dem ein MetroCluster mit validierten NetApp Switches in einer Shared Layer 2-Konfiguration (MetroCluster One) konfiguriert ist und der andere MetroCluster mithilfe von MetroCluster-konformen Switches konfiguriert wird, die direkt mit den Intermediate Switches verbinden (MetroCluster Two).



Überlegungen zur Verwendung von MetroCluster-konformen Switches

Anforderungen und Einschränkungen für MetroCluster-kompatible Switches

Ab ONTAP 9.7 können in MetroCluster IP Konfigurationen MetroCluster-konforme Switches verwendet werden. Dabei handelt es sich um Switches, die nicht von NetApp validiert wurden, die jedoch die Spezifikationen von NetApp erfüllen. NetApp bietet jedoch keine Fehlerbehebungs- oder Konfigurationsunterstützung für nicht validierte Switches an. Die allgemeinen Anforderungen und Einschränkungen bei der Verwendung von MetroCluster-konformen Switches sollten Sie sich bewusst sein.

MetroCluster-konform und NetApp validierte Switches

Ein Switch wird von NetApp validiert, wenn er die folgenden Anforderungen erfüllt:

- Der Switch wird von NetApp im Rahmen der MetroCluster IP Konfiguration bereitgestellt
- Der Switch ist im aufgeführt "NetApp Hardware Universe" Als unterstützter Switch unter *MetroCluster-over-*

IP-connections

- Der Switch wird nur verwendet, um MetroCluster IP-Controller und in einigen Konfigurationen NS224-Laufwerk-Shelfs zu verbinden
- Der Switch wird mit der von NetApp bereitgestellten Referenzkonfigurationsdatei (RCF) konfiguriert

Jeder Switch, der diese Anforderungen nicht erfüllt, ist **nicht** ein von NetApp validierter Switch.

Ein MetroCluster-konformer Switch ist nicht von NetApp validiert, kann aber in einer MetroCluster IP-Konfiguration verwendet werden, wenn er bestimmte Anforderungen und Konfigurationsrichtlinien erfüllt.

> NetApp bietet keine Services zur Fehlerbehebung oder Konfiguration von Support für nicht validierte MetroCluster-kompatible Switches.

Allgemeine Anforderungen für MetroCluster-konforme Switches

Der Switch, der die MetroCluster IP-Schnittstellen verbindet, muss die folgenden allgemeinen Anforderungen erfüllen:

- Die Switches müssen für Quality of Service (QoS) und Traffic-Klassifizierung sorgen.
- Die Schalter müssen eine explizite Benachrichtigung über eine Staumeldung (ECN) unterstützen.
- Die Switches müssen eine Load-Balancing-Richtlinie unterstützen, um die Reihenfolge entlang des Pfads beizubehalten.
- Die Switches müssen L2 Flow Control (L2FC) unterstützen.
- Der Switch-Port muss eine dedizierte Rate bereitstellen und darf nicht überlastet sein.
- Die Kabel und Transceiver, die die Nodes mit den Switches verbinden, müssen von NetApp bereitgestellt werden. Diese Kabel müssen vom Switch-Anbieter unterstützt werden. Wenn Sie optische Kabel verwenden, wird der Transceiver im Switch möglicherweise nicht von NetApp bereitgestellt. Sie müssen überprüfen, ob es mit dem Transceiver im Controller kompatibel ist.
- Die Switches, die die MetroCluster Nodes verbinden, können keinen MetroCluster Datenverkehr übertragen.
- Nur Plattformen, die dedizierte Ports für Cluster Interconnects ohne Switches bereitstellen, können mit einem MetroCluster-konformen Switch verwendet werden. Plattformen wie FAS2750 und AFF A220 können nicht verwendet werden, da sich MetroCluster Traffic und der MetroCluster Interconnect Traffic auf dieselben Netzwerk-Ports befinden.
- Der MetroCluster-kompatible Switch darf nicht für lokale Cluster-Verbindungen verwendet werden.
- Die MetroCluster IP-Schnittstelle kann an jeden Switch-Port angeschlossen werden, der entsprechend den Anforderungen konfiguriert werden kann.
- Es sind vier IP-Switches erforderlich, zwei für jede Switch-Fabric. Wenn Sie Directors verwenden, können Sie einen einzelnen Director auf jeder Seite verwenden, aber die MetroCluster IP-Schnittstellen müssen sich mit zwei verschiedenen Blades in zwei verschiedenen Ausfall-Domains auf diesem Director verbinden.
- Die MetroCluster-Schnittstellen von einem Node müssen mit zwei Netzwerk-Switches oder Blades verbunden werden. Die MetroCluster-Schnittstellen eines Node können nicht mit demselben Netzwerk, Switch oder Blade verbunden werden.
- Das Netzwerk muss die in den folgenden Abschnitten beschriebenen Anforderungen erfüllen:
  - "Überlegungen für ISLs"
  - "Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken"

- Die maximale Übertragungseinheit (MTU) von 9216 muss auf allen Switches mit MetroCluster-IP-Datenverkehr konfiguriert werden.
- Das Zurücksetzen auf ONTAP 9.6 oder eine frühere Version wird nicht unterstützt.

Alle Zwischenschalter, die Sie zwischen den Switches verwenden, die die MetroCluster IP-Schnittstellen an beiden Standorten verbinden, müssen die Anforderungen erfüllen und wie in beschrieben konfiguriert werden "Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken".

Einschränkungen bei Verwendung von MetroCluster-konformen Switches

Sie können keine Konfiguration oder Funktion verwenden, die erfordert, dass lokale Cluster-Verbindungen mit einem Switch verbunden sind. Mit einem MetroCluster-kompatiblen Switch können Sie beispielsweise die folgenden Konfigurationen und Verfahren nicht verwenden:

- MetroCluster Konfigurationen mit acht Nodes
- Der Wechsel von MetroCluster FC- zu MetroCluster IP-Konfigurationen
- Aktualisieren einer MetroCluster IP-Konfiguration mit vier Knoten
- Plattformen mit einer physischen Schnittstelle für lokalen Cluster und MetroCluster-Datenverkehr. Siehe "Plattformspezifische Netzwerkgeschwindigkeiten und Switch Port-Modi für MetroCluster-konforme Switches" Für unterstützte Geschwindigkeiten.

ONTAP -plattformspezifische Netzwerkgeschwindigkeiten und Switch-Port-Modi für MetroCluster-kompatible Switches

Wenn Sie MetroCluster-kompatible Switches verwenden, sollten Sie die plattformspezifischen Netzwerkgeschwindigkeiten und die Anforderungen für den Switch-Port-Modus kennen.

Die folgende Tabelle bietet plattformspezifische Netzwerkgeschwindigkeiten und Switch Port-Modi für MetroCluster-konforme Switches. Sie sollten den Switch-Port-Modus gemäß der Tabelle konfigurieren.

- Fehlende Werte geben an, dass die Plattform nicht mit einem MetroCluster-konformen Switch verwendet werden kann.
- Für die Systeme AFF A30, AFF C30, AFF C60 und FAS50 ist ein QSFP-zu-SFP+ Adapter in der Karte des Controllers erforderlich, um eine Netzwerkgeschwindigkeit von 25 Gbit/s zu unterstützen.

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-
AFF A20	25Gbps	trunk mode
AFF A30	25Gbps or 100Gbps	trunk mode
AFF C30	25Gbps or 100Gbps	trunk mode
AFF C60	25Gbps or 100Gbps	trunk mode
FAS50	25Gbps or 100Gbps	trunk mode
AFF A50	100Gbps	trunk mode
AFF A70	100Gbps	trunk mode
AFF A90	100Gbps	trunk mode
AFF A1K	100Gbps	trunk mode
AFF C80	100Gbps	trunk mode
FAS70	100Gbps	trunk mode
FAS90	100Gbps	trunk mode

Beispiele für die Konfiguration von MetroCluster IP-Switches

Erfahren Sie mehr über die verschiedenen Switch-Port-Konfigurationen.

> In den folgenden Beispielen werden Dezimalwerte verwendet. Die Tabelle ist für Cisco Switches gültig. Je nach Switch-Anbieter benötigen Sie möglicherweise unterschiedliche Werte für DSCP. Informationen zur Bestätigung des korrekten Werts finden Sie in der entsprechenden Tabelle Ihres Switch-Anbieters.

DSCP-Wert	Dezimal	Sechskant	Bedeutung
101 000	16	0x10	CS2
011 000	24	0x18	CS3
100 000	32	0x20	CS4
101 000	40	0x28	CS5

Switch-Port zum Anschließen einer MetroCluster-Schnittstelle

- Klassifizierung für RDMA-Datenverkehr (Remote Direct Memory Access):
  - Übereinstimmung : TCP-Port 10006, Quelle, Ziel oder beides
  - Optionale Übereinstimmung: COS 5
  - Optionales Match: DSCP 40
  - Legen Sie DSCP 40 fest
  - COS 5 einstellen
  - Optional : Ratenformung bis 20Gbps
- Klassifizierung für iSCSI-Datenverkehr:
  - Übereinstimmung : TCP-Port 62500, Quelle, Ziel oder beides
  - Optionale Übereinstimmung: COS 4
  - Optionales Match: DSCP 32
  - Legen Sie DSCP 32 fest
  - COS 4 einstellen
- L2FlowControl (Pause), RX und TX

ISL-Ports

- Klassifizierung:
  - Übereinstimmung mit COS 5 oder DSCP 40
    - Legen Sie DSCP 40 fest
    - COS 5 einstellen
  - Übereinstimmung mit COS 4 oder DSCP 32
    - Legen Sie DSCP 32 fest

        - COS 4 einstellen
- Warteschlange für ausgehenden Datenverkehr
    - Die COS-Gruppe 4 hat einen minimalen Konfigurationsschwellenwert von 2000 und einen maximalen Schwellenwert von 3000
    - Die COS-Gruppe 5 hat einen minimalen Konfigurationsschwellenwert von 3500 und einen maximalen Schwellenwert von 6500.

> Die Konfigurationsschwellenwerte können je nach Umgebung variieren. Sie müssen die Konfigurationsschwellenwerte entsprechend Ihrer individuellen Umgebung bewerten.

    - ECN aktiviert für Q4 und Q5
    - ROT aktiviert für Q4 und Q5

Bandbreitenzuordnung (Switch Ports, die MetroCluster-Schnittstellen und ISL-Ports verbinden)

- RDMA, COS 5 / DSCP 40: 60 %
- ISCSI, COS 4/DSCP 32: 40 %
- Mindestanforderungen für die Kapazität pro MetroCluster-Konfiguration und Netzwerk: 10 GB/s

> Wenn Sie die Tarifgrenzen verwenden, sollte der Verkehr **geformt** werden, ohne dass es zu einem Verlust kommt.

Beispiele für die Konfiguration von Switch-Ports, die den MetroCluster-Controller verbinden

Die angegebenen Beispielbefehle gelten für Cisco NX332- oder Cisco NX9336-Switches. Befehle variieren je nach Switch-Typ.

Wenn eine in den Beispielen abgebildete Funktion oder ihr Äquivalent auf dem Switch nicht verfügbar ist, erfüllt der Switch nicht die Mindestanforderungen und kann nicht für die Bereitstellung einer MetroCluster-Konfiguration verwendet werden. Dies gilt für alle Switches, die eine Verbindung zu einer MetroCluster-Konfiguration herstellen, und für alle Zwischenswitches.

> In den folgenden Beispielen wird möglicherweise nur die Konfiguration für ein Netzwerk angezeigt.

Basiskonfiguration

In jedem Netzwerk muss ein virtuelles LAN (VLAN) konfiguriert werden. Das folgende Beispiel zeigt, wie ein VLAN in Netzwerk 10 konfiguriert wird.

Beispiel:

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

Beispiel:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

Beispiele für die Konfiguration der Klassifizierung

Sie müssen Zugriffs- und Klassenzuordnungen konfigurieren, um RDMA- und iSCSI-Datenverkehr den entsprechenden Klassen zuzuordnen.

Im folgenden Beispiel wird der gesamte TCP-Datenverkehr von und zu Port 65200 der Storage-Klasse (iSCSI) zugeordnet. Der gesamte TCP-Datenverkehr zum und vom Port 10006 ist der RDMA-Klasse zugeordnet. Diese Richtlinienzuordnungen werden an Switch-Ports verwendet, die die MetroCluster-Schnittstellen verbinden.

Beispiel:

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
match access-group name rdma
```

Sie müssen eine Eingangs-Richtlinie konfigurieren. Eine Ingress-Richtlinie ordnet den Datenverkehr verschiedenen COS-Gruppen zu. In diesem Beispiel wird der RDMA-Verkehr der COS-Gruppe 5 zugeordnet und iSCSI-Verkehr der COS-Gruppe 4 zugeordnet. Die Ingress-Richtlinie wird auf Switch-Ports verwendet, die die MetroCluster-Schnittstellen verbinden, und auf den ISL-Ports, die MetroCluster-Datenverkehr übertragen.

Beispiel:

```
policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

NetApp empfiehlt, den Datenverkehr an Switch-Ports, die eine MetroCluster-Schnittstelle verbinden, wie im folgenden Beispiel gezeigt zu gestalten:

Beispiel:

```
policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn
```

Beispiele für die Konfiguration der Node-Ports

Möglicherweise müssen Sie einen Node-Port im Breakout-Modus konfigurieren. Im folgenden Beispiel sind die Ports 25 und 26 im Breakout-Modus 4 x 25 Gbit/s konfiguriert.

Beispiel:

```
interface breakout module 1 port 25-26 map 25g-4x
```

Sie müssen möglicherweise die Port-Geschwindigkeit der MetroCluster-Schnittstelle konfigurieren. Das folgende Beispiel zeigt, wie die Geschwindigkeit auf **Auto** oder in den 40-Gbit/s-Modus konfiguriert wird:

Beispiel:

```
    speed auto

    speed 40000
```

Das folgende Beispiel zeigt einen Switch-Port, der für den Anschluss einer MetroCluster-Schnittstelle konfiguriert ist. Es handelt sich um einen Access-Mode-Port in VLAN 10 mit einer MTU von 9216 und arbeitet in nativer Geschwindigkeit. Die symmetrische Flusssteuerung (Senden und Empfangen) ist aktiviert (Pause) und den MetroCluster-Richtlinien für ein- und ausgehenden Datenverkehr sind zugewiesen.

Beispiel:

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown
```

Bei 25-Gbit/s-Ports müssen Sie möglicherweise die Einstellung Vorwärts-Fehlerkorrektur (FEC) auf „aus“ setzen, wie im folgenden Beispiel gezeigt.

Beispiel:

```
fec off
```

Beispiele für die Konfiguration von ISL-Ports im gesamten Netzwerk

Ein MetroCluster-konformer Switch gilt als Zwischenschalter, selbst er verbindet die MetroCluster-Schnittstellen direkt. Die ISL-Ports, die MetroCluster-Datenverkehr auf dem MetroCluster-konformen Switch übertragen, müssen auf die gleiche Weise wie die ISL-Ports an einem Zwischen-Switch konfiguriert werden. Siehe "Erforderliche Einstellungen an Zwischenschaltern" Für Anleitungen und Beispiele.

> Einige Richtlinienzuordnungen sind für Switch-Ports, die MetroCluster-Schnittstellen verbinden, und ISLs mit MetroCluster-Datenverkehr identisch. Sie können für beide Portnutzungsarten dieselbe Richtlinienzuordnung verwenden.

Erfahren Sie mehr über nicht gespiegelte Aggregate in MetroCluster -IP -Konfigurationen

Wenn Ihre Konfiguration nicht gespiegelte Aggregate umfasst, müssen potenzielle Zugriffsprobleme nach dem Switchover berücksichtigt werden.

Ungespiegelte 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.

Ungespiegelte Aggregate und Wartung, die eine Stromabschaltung erfordert

Wenn Sie zu Wartungszwecken eine vereinbarte Umschaltung durchführen, die eine standortweite Stromabschaltung erfordert, sollten Sie zunächst alle nicht gespiegelten Aggregate im Besitz des Notfallstandorts manuell offline schalten.

Wenn Sie die nicht gespiegelten Aggregate des Notfallstandorts nicht offline schalten, können Knoten am verbleibenden Standort aufgrund von Multi-Disk-Panics ausfallen. Dies kann passieren, wenn umgeschaltete nicht gespiegelte Aggregate offline gehen oder fehlen, weil die Verbindung zum Speicher am Notfallstandort nach einem Stromausfall oder dem Verlust von ISLs verloren geht.

Ungespiegelte Aggregate, CRS-Metadatenvolumes und Daten-SVM-Root-Volumes

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, werden ausgehandelte Switchover- und Switchback-Operationen blockiert und die `metrocluster check` Befehl gibt eine Warnung zurück.

Ungespiegelte Aggregate und SVMs

Sie sollten SVMs nur auf gespiegelten oder nicht gespiegelten Aggregaten konfigurieren. Die Konfiguration von SVMs auf einer Mischung aus nicht gespiegelten und gespiegelten Aggregaten kann zu einem Umschaltvorgang führen, der länger als 120 Sekunden dauert. Dies kann zu einem Datenausfall führen, wenn die nicht gespiegelten Aggregate nicht online gehen.

Ungespiegelte Aggregate und SAN

Vor ONTAP 9.9.1 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.

Lagerregale für ungespiegelte Aggregate hinzufügen

Wenn Sie Regale hinzufügen und diese für nicht gespiegelte Aggregate in einer MetroCluster -IP-Konfiguration verwenden möchten, müssen Sie Folgendes tun:

1. Bevor Sie das Verfahren zum Hinzufügen der Shelves starten, geben Sie den folgenden Befehl ein:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Vergewissern Sie sich, dass die automatische Festplattenzuordnung deaktiviert ist:

   ```
   disk option show
   ```

3. Befolgen Sie die Schritte des Verfahrens, um das Regal hinzuzufügen.
4. Weisen Sie den Node, der im Besitz des nicht gespiegelten Aggregats oder der Aggregate ist, manuell alle Festplatten aus dem neuen Shelf zu.
5. Erstellen Sie die Aggregate:

   ```
   storage aggregate create
   ```

6. Geben Sie nach Abschluss des Verfahrens den folgenden Befehl ein:

```
metrocluster modify -enable-unmirrored-aggr-deployment false
```

7. Vergewissern Sie sich, dass die automatische Festplattenzuordnung aktiviert ist:

```
disk option show
```

Firewall-Portanforderungen für MetroCluster IP-Konfigurationen

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

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.

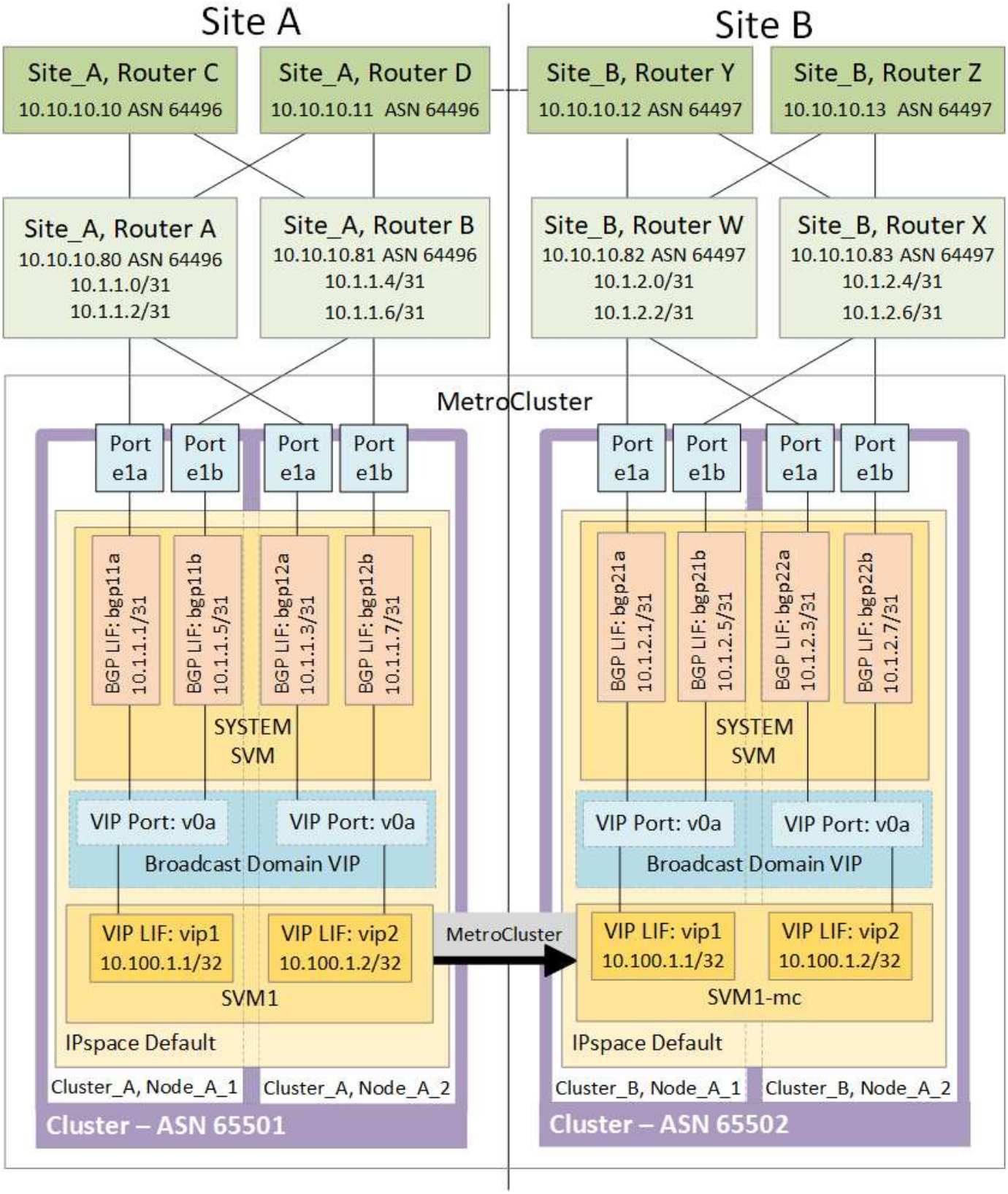
Verkehrstyp	Port/Services
Cluster-Peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP Intercluster LIFs	65200 / TCP 10006 / TCP und UDP
Hardwareunterstützung	4444 / TCP

Erfahren Sie mehr über die Verwendung von virtueller IP und Border Gateway Protocol mit einer MetroCluster -IP-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. Im Jahr 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 des v0a (v0b usw.) 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).

Konfigurieren Sie die Hardwarekomponenten von MetroCluster

Erfahren Sie mehr über die Verbindungen von Hardwarekomponenten in einer MetroCluster -IP-Konfiguration

Bei der Planung Ihrer MetroCluster IP-Konfiguration sollten Sie sich mit den Hardwarekomponenten und den zugehörigen Verbindungen vertraut machen.

Wichtige Hardwarekomponenten

Eine MetroCluster IP-Konfiguration umfasst die folgenden wichtigen Hardwarekomponenten:

- Storage Controller

  Die Storage Controller sind als zwei-Node-Cluster konfiguriert.

- IP-Netzwerk

  Dieses Back-End-IP-Netzwerk bietet Konnektivität für zwei unterschiedliche Anwendungen:

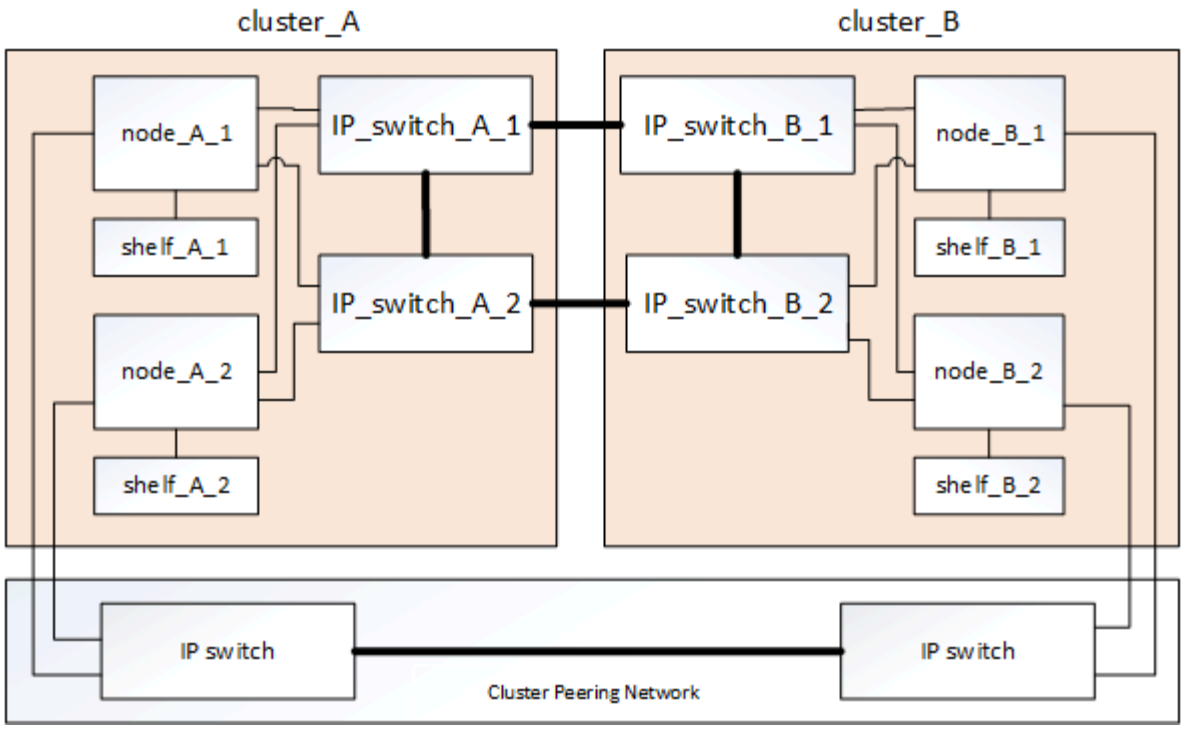
  - Standardmäßige Cluster-Konnektivität für die Cluster-interne Kommunikation

    Dies ist dieselbe Cluster-Switch-Funktion, die auch in nicht-MetroCluster-ONTAP-Clustern mit Switch verwendet wird.

  - MetroCluster Back-End-Konnektivität für die Replizierung von Storage-Daten und nichtflüchtigem Cache

- Cluster-Peering-Netzwerk

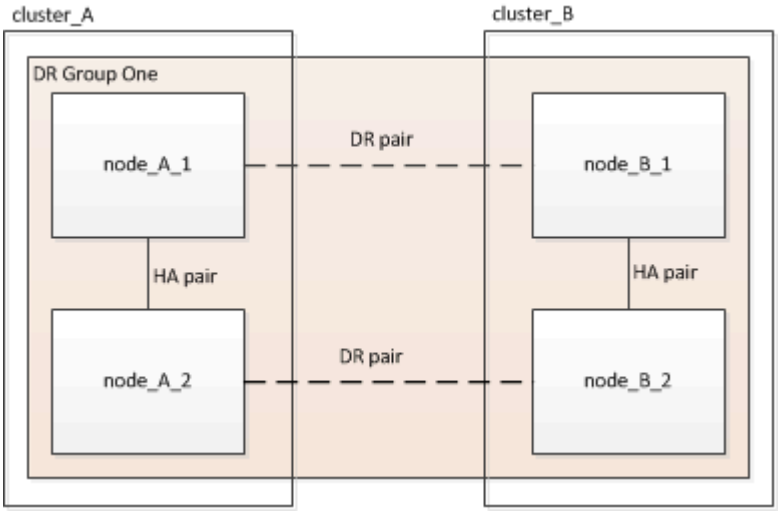
  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der Cluster-Konfiguration, einschließlich der Storage Virtual Machine (SVM)-Konfiguration. Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.



Disaster-Recovery-Gruppen (DR)

Eine MetroCluster IP-Konfiguration besteht aus einer DR-Gruppe mit vier Nodes.

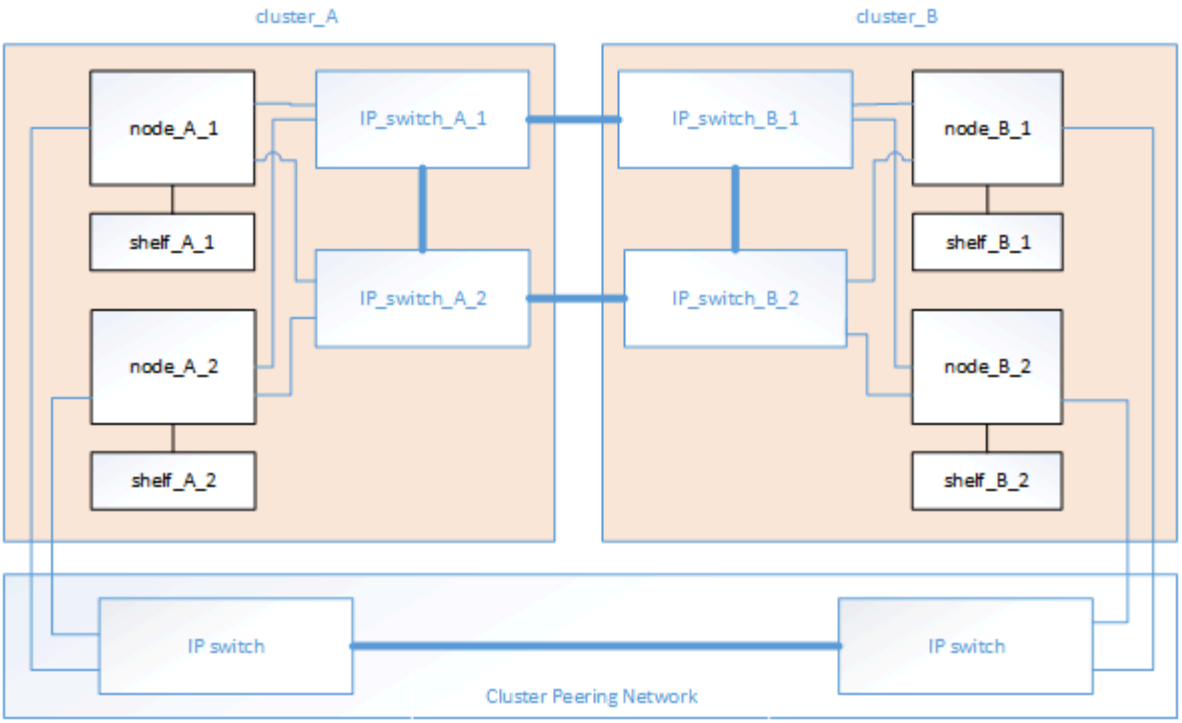
Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit vier Nodes:



Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration

Jeder MetroCluster Standort besteht aus Storage Controllern, die als HA-Paar konfiguriert sind. Dadurch wird lokale Redundanz ermöglicht, sodass der lokale HA-Partner übernimmt, wenn ein Storage Controller ausfällt. Solche Ausfälle können ohne MetroCluster-Switchover-Operation behoben werden.

Lokale HA-Failover- und Giveback-Vorgänge werden mit Storage Failover-Befehlen auf gleiche Weise durchgeführt wie eine andere Konfiguration von MetroCluster.

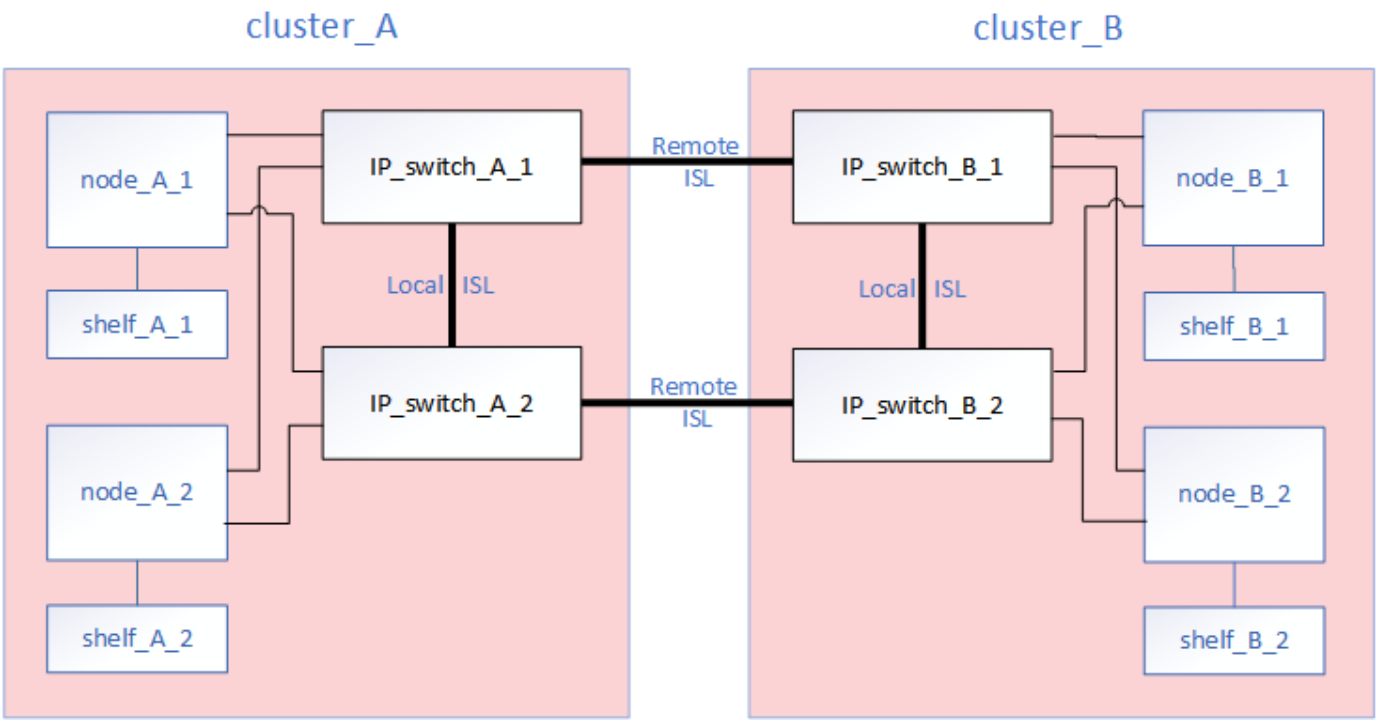


Verwandte Informationen

"ONTAP-Konzepte"

Darstellung des MetroCluster IP- und Cluster Interconnect-Netzwerks

ONTAP Cluster verfügen normalerweise über ein Cluster-Interconnect-Netzwerk für den Datenverkehr zwischen den Nodes im Cluster. In MetroCluster IP-Konfigurationen wird dieses Netzwerk auch für das übertragen von Daten-Replizierungsdatenverkehr zwischen den MetroCluster Standorten verwendet.

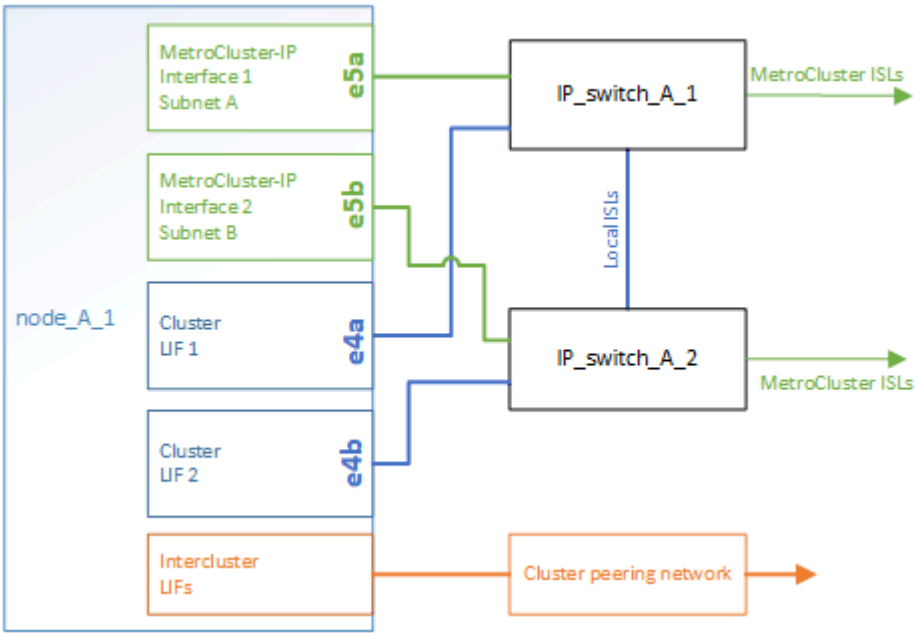


Jeder Node in der MetroCluster IP-Konfiguration verfügt über dedizierte Schnittstellen zur Verbindung mit dem

Back-End IP-Netzwerk:

- Zwei MetroCluster IP-Schnittstellen
- Zwei lokale Cluster-Schnittstellen

Die folgende Abbildung zeigt diese Schnittstellen. Die angegebene Port-Nutzung gilt für ein AFF A700 oder FAS9000 System.



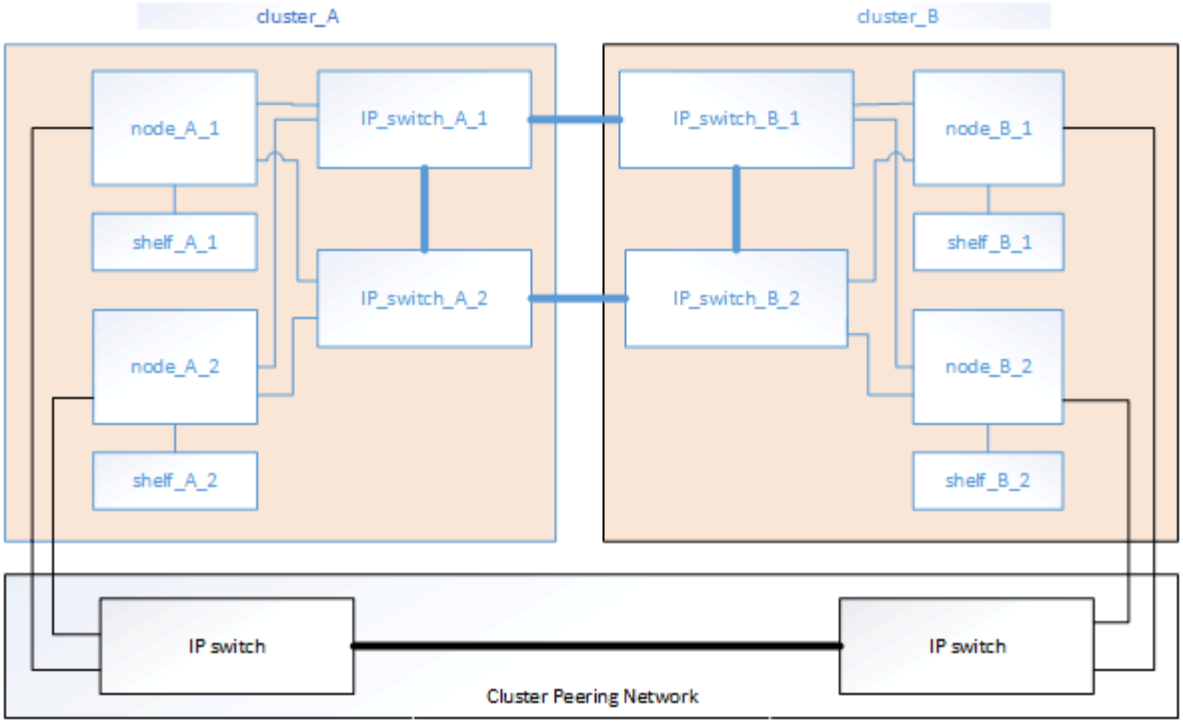
Verwandte Informationen

"Überlegungen für MetroCluster IP-Konfigurationen"

Illustration des Cluster-Peering-Netzwerks

Die beiden Cluster in der MetroCluster Konfiguration werden über ein vom Kunden bereitgestellter Cluster-Peering-Netzwerk Peering Peering durchgeführt. Cluster Peering unterstützt die synchrone Spiegelung von Storage Virtual Machines (SVMs, früher Vserver genannt) zwischen den Standorten.

Intercluster-LIFs müssen auf jedem Node in der MetroCluster-Konfiguration konfiguriert werden, und die Cluster müssen für Peering konfiguriert sein. Die Ports mit den Intercluster-LIFs sind mit dem vom Kunden bereitgestellten Cluster-Peering-Netzwerk verbunden. Die Replizierung der SVM-Konfiguration erfolgt über dieses Netzwerk über den Configuration Replication Service.



Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

"Überlegungen für die Konfiguration von Cluster-Peering"

"Verkabeln der Cluster-Peering-Verbindungen"

"Peering der Cluster"

Erforderliche MetroCluster IP-Konfigurationskomponenten und Namenskonventionen

Wenn Sie Ihre MetroCluster IP-Konfiguration planen, müssen Sie die erforderlichen und unterstützten Hardware- und Softwarekomponenten kennen. Für Einfachheit und Klarheit sollten Sie auch die Namenskonventionen verstehen, die für Komponenten in Beispielen in der gesamten Dokumentation verwendet werden.

Unterstützte Software und Hardware

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

"NetApp Hardware Universe"

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

Anforderungen an Hardwareredundanz in einer MetroCluster IP-Konfiguration

Aufgrund der Hardware-Redundanz in der MetroCluster IP-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.

ONTAP-Cluster-Anforderungen in einer MetroCluster IP-Konfiguration

Für MetroCluster IP-Konfigurationen sind zwei ONTAP Cluster erforderlich, eines an jedem MetroCluster Standort.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
- Standort B: Cluster_B

IP-Switch-Anforderungen in einer MetroCluster IP-Konfiguration

Für MetroCluster IP-Konfigurationen sind vier IP-Switches erforderlich. Die vier Switches bilden zwei Switch-Storage-Fabrics, die in der MetroCluster IP-Konfiguration zwischen jedem der Cluster die ISL bieten.

Zudem sorgen die IP-Switches für eine Intracluster-Kommunikation zwischen den Controller-Modulen in jedem Cluster.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
  - IP_Switch_A_1
  - IP_Switch_A_2
- Standort B: Cluster_B
  - IP_Switch_B_1
  - IP_Switch_B_2

Anforderungen an das Controller-Modul in einer MetroCluster IP-Konfiguration

MetroCluster IP-Konfigurationen erfordern vier oder acht Controller-Module.

Die Controller-Module an jedem Standort bilden ein HA-Paar. Jedes Controller-Modul besitzt einen DR-Partner am anderen Standort.

Jedes Controller-Modul muss die gleiche ONTAP-Version aufweisen. Unterstützte Plattformmodelle sind von der ONTAP Version abhängig:

- Neue MetroCluster IP-Installationen auf FAS Systemen werden in ONTAP 9.4 nicht unterstützt.

  Vorhandene MetroCluster IP Konfigurationen auf FAS Systemen können auf ONTAP 9.4 aktualisiert werden.

- Ab ONTAP 9.5 werden neue MetroCluster IP-Installationen auf FAS Systemen unterstützt.
- Ab ONTAP 9.4 werden für ADP konfigurierte Controller-Module unterstützt.

Beispielnamen

Die folgenden Beispielnamen werden in der Dokumentation verwendet:

- Standort A: Cluster_A
  - Controller_A_1
  - Controller_A_2
- Standort B: Cluster_B
  - Controller_B_1
  - Controller_B_2

Anforderungen für Gigabit-Ethernet-Adapter in einer MetroCluster IP-Konfiguration

Bei den MetroCluster IP-Konfigurationen wird für die IP-Schnittstellen zu den für das MetroCluster IP Fabric verwendeten IP-Switches ein Ethernet-Adapter mit 40/100 Gbit/s oder 10/25 Gbit/s verwendet.

Integrierte Ports sind in die Controller-Hardware (Steckplatz 0) integriert und können nicht ersetzt werden, der erforderliche Steckplatz für den Adapter ist daher nicht verfügbar.

Modell der Plattform	Erforderlicher Gigabit-Ethernet-Adapter	Erforderlicher Steckplatz für Adapter	Ports
AFF A900, ASA A900 und FAS9500	X91146A	Steckplatz 5, Steckplatz 7	E5b, e7b **Hinweis:** Die Ports e5a und e7a können nur für Intercluster-LIFs verwendet werden. Sie können diese Ports nicht für ein Daten-LIF verwenden.
AFF A700 UND FAS9000	X91146A-C	Einschubfach 5	e5a, e5b
AFF A800, AFF C800, ASA A800 und ASA C800	X1146A/Onboard-Ports	Steckplatz 1/gilt nicht für Onboard-Ports	e0b: e1b
FAS8300, AFF A400, ASA A400, ASA C400 und AFF C400	X1146A	Steckplatz 1	e1a, e1b
AFF A300 UND FAS8200	X1116 A	Steckplatz 1	e1a, e1b
FAS2750, AFF A150, ASA A150 und AFF A220	Onboard-Ports	Keine Angabe	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250 und AFF C250	Onboard-Ports	Keine Angabe	e0c, e0d
AFF A320	Onboard-Ports	Keine Angabe	e0g, e0h

AFF A70, FAS70	X50132A	Steckplatz 2	e2a, e2b
AFF A90, AFF A1K, FAS90, AFF C80	X50132A	Steckplatz 2, Steckplatz 3	e2b, e3b **Hinweis:** die Ports e2a und e3a müssen unbenutzt bleiben. Die Verwendung dieser Ports für Front-End-Netzwerke oder Peering wird nicht unterstützt.
AFF A50	X60134A	Steckplatz 2	e2a, e2b
AFF A30, AFF C30, AFF C60, FAS50	X60134A	Steckplatz 2	e2a, e2b
AFF A20	X60132A	Steckplatz 4, Steckplatz 2	e2b, e4b

"Erfahren Sie mehr über die automatische Laufwerkszuordnung und ADP-Systeme in MetroCluster IP-Konfigurationen".

Pool- und Festplattenanforderungen (mindestens unterstützt)

Es werden acht SAS-Platten-Shelves empfohlen (vier Shelfs an jedem Standort), damit sich die Anschaffung von Festplatten pro Shelf zulässt.

MetroCluster IP-Konfigurationen mit vier Nodes erfordern an jedem Standort die Minimalkonfiguration:

- Jeder Node hat mindestens einen lokalen Pool und einen Remote-Pool am Standort.
- Mindestens sieben Laufwerke pro Pool.

  In einer MetroCluster-Konfiguration mit vier Nodes und einem einzelnen gespiegelten Datenaggregat pro Node sind für die Minimalkonfiguration 24 Festplatten am Standort erforderlich.

In einer minimal unterstützten Konfiguration verfügt jeder Pool über das folgende Laufwerkslayout:

- Drei Root-Laufwerke
- Drei Datenlaufwerke
- Ein Ersatzlaufwerk

Bei einer unterstützten Minimalkonfiguration ist pro Standort mindestens ein Shelf erforderlich.

MetroCluster-Konfigurationen unterstützen RAID-DP, RAID4 und RAID-TEC.

> Ab ONTAP 9.4 unterstützen MetroCluster IP-Konfigurationen neue Installationen mithilfe von automatischer Festplattenzuweisung und ADP (Advanced Drive Partitioning). Weitere Informationen finden Sie unter "Überlegungen zur automatischen Laufwerkszuweisung und ADP-Systemen" .

Überlegungen zum Speicherort von Laufwerken für teilweise bestückte Shelfs

Die Laufwerke sollten sich in den Steckplätzen 0-5 und 18-23 befinden, um Laufwerke bei Verwendung von Shelfs, die halb bestückt sind (12 Laufwerke in einem Shelf mit 24 Laufwerken), automatisch zuweisen.

Bei einer Konfiguration mit einem teilweise bestückten Shelf müssen die Laufwerke gleichmäßig in die vier Quadranten des Shelfs verteilt werden.

Überlegungen zum Laufwerkstandort für interne AFF A800 Laufwerke

Für eine korrekte Implementierung der ADP-Funktion müssen die AFF A800 Systemfestplattenschächte in Quartale aufgeteilt und die Laufwerke symmetrisch in den Quartalen angeordnet sein.

Ein AFF A800 System verfügt über 48 Laufwerkschächte. Die Buchten können in Quartiere unterteilt werden:

- Quartal:
  - Einschübe 0 Bis 5
  - Buchten 24 - 29
- Quartal:
  - Buchten 6 - 11
  - Buchten 30 - 35
- Quartal:
  - Buchten 12 - 17
  - Buchten 36 - 41
- Quartal:
  - Buchten 18 - 23
  - Buchten 42 - 47

Wenn dieses System mit 16 Laufwerken bestückt ist, müssen sie symmetrisch auf die vier Quartale verteilt werden:

- Vier Laufwerke im ersten Quartal: 0, 1, 2, 3
- Im zweiten Quartal vier Laufwerke: 6, 7, 8, 9
- Im dritten Quartal vier Laufwerke: 12, 13, 14, 15
- Vier Laufwerke im vierten Quartal: 18, 19, 20, 21

Mischen von IOM12 und IOM 6 Modulen in einem Stack

Ihre Version von ONTAP muss Shelf-Mix unterstützen. Siehe "NetApp Interoperabilitäts-Matrix-Tool (IMT)" Um zu prüfen, ob Ihre Version von ONTAP Shelf-Mischungen unterstützt.

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

Rack der MetroCluster IP-Konfigurationshardwarekomponenten

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

Über diese Aufgabe

Dieser Task muss auf beiden MetroCluster-Sites ausgeführt werden.

Schritte

1. Planen der Positionierung der MetroCluster Komponenten

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

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   Folgen Sie den Schritten zur *Installation der Hardware* unter den *Installations- und Setup-Anweisungen* für Ihr Plattformmodell im"Dokumentation zu ONTAP -Hardwaresystemen" .

4. Installieren Sie die IP-Switches im Rack oder Schrank.
5. 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.
   - Um die Fehlerbehebung zu unterstützen, werden für jedes SAS-Platten-Shelf in jeder MetroCluster DR-Gruppe eindeutige Shelf-IDs empfohlen.

   > Verkabeln Sie zum jetzigen Zeitpunkt keine Festplatten-Shelfs, die nicht gespiegelte Aggregate enthalten sollen. Sie müssen warten, bis die für nicht gespiegelte Aggregate vorgesehenen Shelfs implementiert sind, bevor die MetroCluster-Konfiguration abgeschlossen ist und diese erst nach Verwendung der implementiert werden `metrocluster modify -enable-unmirrored-aggr-deployment true` Befehl.

MetroCluster IP-Switches verkabeln

So verwenden Sie die Porttabellen mit mehreren MetroCluster IP-Konfigurationen

Sie müssen verstehen, wie die Informationen in den Porttabellen verwendet werden, um Ihre RCF-Dateien korrekt zu generieren.

Bevor Sie beginnen

Lesen Sie vor der Verwendung der Tabellen diese Überlegungen durch:

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Verfolgen Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2 usw.). Sie benötigen diese Informationen, wenn Sie das Tool RcfFileGenerator verwenden, wie später in diesem Konfigurationsverfahren beschrieben.
- Sie sollten alle Nodes auf die gleiche Weise verkabeln. Wenn für die Verkabelung der Nodes unterschiedliche Portkombinationsoptionen verfügbar sind, sollten alle Nodes die gleichen Port-Kombinationen verwenden. Beispiel: e1a auf Knoten 1 und e1a auf Knoten 2 sollten an einen Schalter angeschlossen werden. Gleichermaßen sollte der zweite Port beider Nodes an den zweiten Switch angeschlossen werden.

- Der "RCfFileGenerator für MetroCluster-IP" bietet außerdem eine Übersicht über die Verkabelung pro Port für jeden Switch. Verwenden Sie diese Verkabelungsübersicht, um Ihre Verkabelung zu überprüfen.

Verkabelung von zwei MetroCluster-Konfigurationen mit den Switches

Wenn Sie mehrere MetroCluster-Konfigurationen an einen Switch anschließen, verkabeln Sie jeden MetroCluster gemäß der entsprechenden Tabelle. Wenn Sie beispielsweise eine FAS2750 und eine AFF A700 an denselben Switch anschließen, verkabeln Sie die FAS2750 gemäß „MetroCluster 1“ in Tabelle 1 und die AFF A700 gemäß „MetroCluster 2“ oder „MetroCluster 3“ in Tabelle 2. Die FAS2750 und die AFF A700 können nicht physisch als „MetroCluster 1“ verkabelt werden.

Verkabelung von MetroCluster Konfigurationen mit acht Nodes

Bei MetroCluster Konfiguration mit ONTAP 9.8 und früher müssen bei einigen Verfahren für die Transition eines Upgrades eine zweite DR-Gruppe mit vier Nodes zur Konfiguration hinzugefügt werden, um eine temporäre Konfiguration mit acht Nodes zu erstellen. Ab ONTAP 9.9 werden dauerhafte MetroCluster-Konfigurationen mit acht Nodes unterstützt.

Über diese Aufgabe

Für Konfigurationen mit acht Knoten verwenden Sie dieselbe Methode wie oben beschrieben. Anstelle einer zweiten MetroCluster ist eine weitere DR-Gruppe mit vier Nodes verkabelt.

Ihre Konfiguration umfasst beispielsweise Folgendes:

- Cisco Switches 3132Q-V
- MetroCluster 1: FAS2750 Plattformen
- MetroCluster 2: AFF A700 Plattformen (Hinzufügen dieser Plattformen als zweite DR-Gruppe mit vier Nodes)

Schritte

1. Verkabeln Sie bei MetroCluster 1 die Cisco 3132Q-V Switches mithilfe der Tabelle für die FAS2750-Plattform und der Zeilen für MetroCluster 1-Schnittstellen.
2. Verkabeln Sie bei MetroCluster 2 (der zweiten DR-Gruppe) die Cisco 3132Q-V-Switches mithilfe der Tabelle für die AFF A700 Plattform und der Zeilen für MetroCluster 2-Schnittstellen.

Plattform-Portzuweisungen für Cisco 3132Q-V-Switches in einer MetroCluster IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Richtlinien, bevor Sie die Tabellen verwenden:

- Wenn Sie den Switch für MetroCluster FC zu IP-Übergang konfigurieren, können Port 5, Port 6, Port 13 oder Port 14 zum Verbinden der lokalen Clusterschnittstellen des MetroCluster FC-Node verwendet werden. Siehe "RCfFileGenerator" Und die generierten Verkabelungsdateien für weitere Details zur Verkabelung dieser Konfiguration. Für alle anderen Verbindungen können Sie die in den Tabellen aufgeführten Port-Nutzungszuweisungen verwenden.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
FAS2750, AFF A220	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 1)
FAS9000, AFF A700	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 2)
AFF A800, ASA A800	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 3)

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 1)

Plattform-Port-Zuordnungen zum Verkabelung eines FAS2750 oder AFF A220 Systems mit einem Cisco 3132Q-V Switch prüfen:

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 2)

Plattform-Port-Zuweisungen prüfen, um ein FAS9000 oder AFF A700 System mit einem Cisco 3132Q-V Switch zu verkabeln:

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 3)

Plattform-Port-Zuweisungen prüfen, um ein AFF A800 oder ASA A800 System mit einem Cisco 3132Q-V Switch zu verkabeln:

Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port- Cisco 9336C-Switches in einer MetroCluster -IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für Cisco 3232C-Switches oder 36-Port-Cisco 9336C-FX2-Switches, die keinen NS224-Speicher verbinden.

  Wenn Sie einen 12-Port Cisco 9336C-FX2 Switch haben, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für 12-Port Cisco 9336C-FX2-Switches" .

  Wenn Sie einen Cisco 9336C-FX2-Switch mit 36 Ports haben und mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für einen 36-Port Cisco 9336C-FX2-Switch, der NS224-Speicher verbindet" .

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Wenn Sie eine einzelne MetroCluster mit den Switches konfigurieren, verwenden Sie die Portgruppe **MetroCluster 1**.

  Verfolgen Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2, MetroCluster 3 oder MetroCluster 4). Sie benötigen sie, wenn Sie das RcfFileGenerator-Tool verwenden, wie später in diesem Konfigurationsvorgang beschrieben.

- Der RcfFileGenerator für MetroCluster IP bietet auch eine Übersicht über die Verkabelung pro Port für jeden Switch.

  Verwenden Sie diese Verkabelungsübersicht, um Ihre Verkabelung zu überprüfen.

- RCF-Dateiversion Version 2.10 oder höher ist für den 25G-Breakout-Modus für MetroCluster-ISLs erforderlich.
- Für die Verwendung einer anderen Plattform als FAS8200 oder AFF A300 in der Gruppe „MetroCluster 4“ sind ONTAP 9.13.1 oder höher und RCF-Dateiversion 2.00 erforderlich.

> Die Version der RCF-Datei unterscheidet sich von der Version des RCFfilegenerator-Tools, mit dem die Datei generiert wird. Beispielsweise können Sie eine RCF-Datei Version 2.00 mit RCFfilegenerator v1.6c generieren.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750, AFF A220 FAS500f, AFF C250, ASA C250 AFF A250, ASA A250	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 1)
AFF A20	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 2)
AFF A30, AFF C30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 3a - 25G) • Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuweisungen (Gruppe 3b - 100G)
FAS8200, AFF A300	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 4)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 5)

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A50	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 6)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 7)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 8)

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 1)

Prüfen der Plattform-Port-Zuordnungen zur Verkabelung von AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 oder ASA A250 mit einem Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 2)

Überprüfen Sie die Zuweisung der Plattformschnittstelle, um ein AFF A20-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e2a	e4a
5/2-4		disabled	
6/1		e2a	e4a
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e2b	e4b
13/2-4		disabled	
14/1		e2b	e4b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e2b	e4b
25/2-4		disabled	
26/1		e2b	e4b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e2a	e4a
29/2-4		disabled	
30/1		e2a	e4a
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Cisco 3232C oder Cisco 9336C-FX2 – Plattform-Port-Zuordnungen (Gruppe 3a)

Überprüfen Sie die Zuordnungen der Plattformports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System über eine 25-Gbit-Ethernet-Karte mit vier Ports mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln.

> Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5/1	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5/2-4		disabled		disabled		disabled	
6/1		e4a	e4b	e4a	e4b	e4a	e4b
6/2-4		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29/1	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
29/2-4		disabled		disabled		disabled	
30/1		e4a	e4b	e4a	e4b	e4a	e4b
30/2-4		disabled		disabled		disabled	
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Cisco 3232C oder Cisco 9336C-FX2 – Plattform-Port-Zuordnungen (Gruppe 3b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem Cisco 3232C- oder 9336C-FX2-Switch über eine 100-GB-Ethernet-Karte mit zwei Ports zu verkabeln.

> Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
30		e4a	e4b	e4a	e4b	e4a	e4b
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 4)

Überprüfen Sie die Zuordnungen der Plattformports, um ein FAS8200- oder AFF A300-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Wenn Sie ein Upgrade von älteren RCF-Dateien durchführen, verwendet die Verkabelungskonfiguration möglicherweise Ports in der Gruppe „MetroCluster 4“ (Ports 25/26 und 29/30).

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 5)

Prüfen der Port-Zuordnungen der Plattformen zur Verkabelung der AFF A320, FAS8300, AFF C400, ASA C400, FAS8700 AFF A400 oder ASA A400 System auf einen Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Für die Verwendung von Ports in der Gruppe „MetroCluster 4“ ist ONTAP 9.13.1 oder höher erforderlich.

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 6)

Überprüfen Sie die Zuweisung der Plattformschnittstelle, um ein AFF A50-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6		e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b
14		e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25	MetroCluster 4, MetroCluster interface	e2a	e2b
26		e2a	e2b
27 - 28	Unused	disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b
30		e4a	e4b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 7)

Plattform-Port-Zuordnungen zur Verkabelung von FAS9000, AFF A700, AFF C800, ASA C800, AFF A800 prüfen, ASA A800, FAS9500, AFF A900 oder ASA A900 System mit einem Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

> Für die Verwendung von Ports in der Gruppe „MetroCluster 4“ ist ONTAP 9.13.1 oder höher erforderlich.

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 8)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System mit einem Cisco 3232C- oder 9336C-FX2 Switch zu verkabeln:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16									
17									
18									
19									
20									
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4									
23/1-4									
24/1-4									
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
26									
27 - 28	Unused	disabled		disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
30									
31 - 32	Unused	disabled		disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	

Plattform-Portzuweisungen für 12-Port- Cisco 9336C-FX2-Switches in einer MetroCluster -IP -Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für 12-Port-Switches Cisco 9336C-FX2.

  Wenn Sie einen 36-Port Cisco 9336C-FX2 Switch haben, der keine NS224-Shelves verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port-Switches Cisco 9336C-FX2" .

  Wenn Sie einen Cisco 9336C-FX2-Switch mit 36 Ports haben und mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für einen 36-Port Cisco 9336C-FX2-Switch, der NS224-Speicher verbindet" .

> Der 12-Port-Switch Cisco 9336C-FX2 unterstützt nicht den Anschluss von NS224-Shelves an den MetroCluster-Switch.

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Wenn Sie eine einzelne MetroCluster mit den Switches konfigurieren, verwenden Sie die Portgruppe **MetroCluster 1**.

Behalten Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2) im Auge. Sie benötigen sie, wenn Sie das Tool RcfFileGenerator verwenden, wie später in diesem Konfigurationsverfahren beschrieben.

- Der RcfFileGenerator für MetroCluster IP bietet auch eine Übersicht über die Verkabelung pro Port für jeden Switch.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 1)
AFF A20	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 2)
AFF A30, AFF C30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3a – 25G) • Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3b – 100G)
FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 4)
AFF A50	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 5)
AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 7)

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 1)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A150-, ASA A150-, FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1-4	Unused	disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 2)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A20-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3a)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mithilfe einer 25G-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3b)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mithilfe einer 100G-Ethernet-Karte mit zwei Ports an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen.

> Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 4)

Überprüfen Sie die Portzuweisungen der Plattform, um ein FAS8300-, AFF C400-, ASA C400-, FAS8700-, AFF A400- oder ASA A400-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b
2					
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b
10					
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 5)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A50-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 6)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF C800-, ASA C800-, AFF A800-, ASA A800-, FAS9500-, AFF A900- oder ASA A900-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Hinweis 2: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A-Adapter (40 Gbit/s) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 7)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20									
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4									
23-36	Ports disallowed to use	blocked		blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Plattform-Portzuweisungen für einen 36-Port- Cisco 9336C-FX2-Switch, der NS224-Speicher in einer MetroCluster -IP-Konfiguration verbindet

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für Cisco 9336C-FX2-Switches mit 36 Ports, wenn mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet.

  Wenn Sie einen 36-Port Cisco 9336C-FX2 Switch haben, der keinen NS224-Speicher verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port-Switches Cisco 9336C-FX2" .

  Wenn Sie einen 12-Port Cisco 9336C-FX2 Switch haben, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für 12-Port Cisco 9336C-FX2-Switches" .

  > Der 12-Port-Switch Cisco 9336C-FX2 unterstützt nicht den Anschluss von NS224-Shelves an den MetroCluster-Switch.

- Wenn Sie einen Cisco 9336C-FX2-Switch verkabeln und NS224-Speicher anschließen, können Sie maximal zwei MetroCluster-Konfigurationen oder DR-Gruppen verwenden. Mindestens eine MetroCluster-Konfiguration oder DR-Gruppe muss NS224-Shelves mit dem MetroCluster-Switch verbinden. Sie können nur Plattformen verbinden, die keine Switch-angeschlossenen NS224-Shelves als zweite MetroCluster-Konfiguration oder zweite DR-Gruppe verbinden.

  Wenn Ihr zweiter MetroCluster oder Ihre DR-Gruppe keine NS224-Shelves mit dem MetroCluster-Switch verbindet, folgen Sie den Verkabelungstabellen für Controller, die keine über einen Switch angeschlossenen NS224-Regale verbinden .

- Der RcfFileGenerator zeigt nur geeignete Plattformen an, wenn die erste Plattform ausgewählt ist.
- Für das Verbinden von MetroCluster Konfigurationen mit einem oder zwei vier Nodes ist ONTAP 9.14.1 oder höher erforderlich.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Überprüfen Sie die Tabelle mit den korrekten Portzuweisungen für Ihre Konfiguration. In diesem Abschnitt gibt es zwei Sätze von Verkabelungstabellen:

- Verkabelungstabellen für Controller, die NS224-Shelfs mit Switch verbinden
- Verkabelungstabellen für Controller, die keine Switch-verbundenen NS224-Shelfs anschließen

Controller, die Switch-Attached NS224 Shelfs verbinden

Legen Sie fest, welche Portzuweisungstabelle Sie für Controller befolgen sollten, die Switch-verbundene NS224-Shelfs verbinden.

Plattform	Verwenden Sie diese Verkabelungstabelle…
AFF C30, AFF A30 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 1a) oder 100G (Gruppe 1b) Ethernet-Karte verwenden. • Cisco 9336C-FX2-Switch zur Verbindung von Port-Zuordnungen der NS224-Speicherplattform (Gruppe 1a - 25G) • Cisco 9336C-FX2-Switch zur Verbindung von NS224-Storage-Plattform-Port-Zuordnungen (Gruppe 1b - 100G)
AFF A320 AFF C400, ASA C400 AFF A400, ASA A400	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 2)
AFF A50	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 3)
AFF A700 AFF C800, ASA C800, AFF A800 AFF A900, ASA A900	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 4)
AFF A70 AFF C80 AFF A90 AFF A1K	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 5)

Cisco 9336C-FX2-Switch, der NS224-Speicherplattform-Port-Zuweisungen verbindet (Gruppe 1a)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30- oder AFF C60-System zu verkabeln, bei dem Switch-verbundene NSS24-Shelfs über eine 25-Gbit-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch angeschlossen werden.

> Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled	
2/1		e4a	e4b	e4a	e4b
2/2-4		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled	
4/1		e4a	e4b	e4a	e4b
4/2-4		disabled		disabled	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Speicherplattform-Portzuweisungen (Gruppe 1b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30- oder AFF C60-System zu verkabeln, das Switch-angeschlossene NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch über eine 100G-Ethernet-Karte mit zwei Ports verbindet.

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 2)

Plattform-Port-Zuweisungen prüfen, um ein AFF A320-, AFF C400-, ASA C400-, AFF A400- oder ASA A400-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 3)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A50-System zu verkabeln, das Switch-verbundene NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbindet:

Controllers connecting switch-attached shelves			
Switch Port	Port Use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b
18			
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b
20			
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)		
28			
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 4)

Plattform-Port-Zuweisungen prüfen, um ein AFF A700-, AFF C800-, ASA C800-, AFF A800-, AFF A900- oder ASA A900-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
18							
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 5)

Prüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A70-, AFF C80-, AFF A90- oder AFF A1K-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Controller verbinden keine Switch-Attached NS224 Shelfs

Legen Sie fest, welche Portzuweisungstabelle Sie für Controller befolgen sollten, die keine Switch-verbundenen NS224-Shelfs verbinden.

Plattform	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750, AFF A220	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 6)
AFF A20	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 7)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 8)
AFF C30, AFF A30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 9a) oder 100G (Gruppe 9b) Ethernet-Karte verwenden. • Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9a) • Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9b)
FAS8200, AFF A300	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 10)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 11)
AFF A50	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 12)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 13)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 14)

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 6)

Plattform-Port-Zuweisungen prüfen, um ein AFF A150-, ASA A150-, FAS2750- oder AFF A220-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 7)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A20-System zu verkabeln, bei dem keine Switch-angeschlossenen NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 8)

Plattform-Port-Zuweisungen prüfen, um ein FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9a)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs über eine 25-Gbit-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch angeschlossen sind.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9b)

Prüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs über eine 100-GB-Ethernet-Karte mit zwei Ports an einen Cisco 9336C-FX2-Switch angeschlossen sind.

> Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 10)

Plattform-Port-Zuordnungen prüfen, um ein FAS8200- oder AFF A300-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 11)

Plattform-Port-Zuweisungen prüfen, um ein AFF A320-, FAS8300-, AFF C400-, ASA C400-, FAS8700-, AFF A400- oder ASA A400-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 12)

Prüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind.

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 13)

Plattform-Port-Zuordnungen prüfen, um ein FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 oder ASA A900 System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2 Switch verbunden sind:

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 14)

Prüfen Sie die Plattform-Port-Zuweisungen, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2 Switch verbunden sind:

Plattform-Portzuweisungen für von Broadcom unterstützte BES-53248-IP-Switches in einer MetroCluster -IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Sie können die Switches nicht mit Remote-ISL-Ports unterschiedlicher Geschwindigkeit verwenden (z. B. ein 25-Gbit/s-Port, der an einen 10-Gbit/s-ISL-Port angeschlossen ist).
- Wenn Sie den Switch für den Übergang von MetroCluster FC zu IP konfigurieren, werden die folgenden Ports je nach gewählter Zielplattform verwendet:

Zielplattform	Port
FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 oder FAS8700 Plattformen eingesetzt	Ports 1 bis 6, 10 Gbit/s
FAS8200 oder AFF A300 Plattformen	Ports 3 - 4 und 9 - 12, 10 Gbit/s

- Bei AFF A320 Systemen, die mit Broadcom BES-53248-Switches konfiguriert sind, werden möglicherweise nicht alle Funktionen unterstützt.

  Jede Konfiguration oder Funktion, die erfordert, dass die lokalen Cluster-Verbindungen mit einem Switch verbunden sind, wird nicht unterstützt. Beispielsweise werden die folgenden Konfigurationen und Verfahren nicht unterstützt:

  - MetroCluster Konfigurationen mit acht Nodes
  - Der Wechsel von MetroCluster FC- zu MetroCluster IP-Konfigurationen
  - Aktualisieren einer MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher)

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750 AFF A220	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 1)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 2)
AFF A20	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 3)
AFF C30, AFF A30 FAS50 AFF C60	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 4)
FAS8200, AFF A300	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 5)
AFF A320	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 6)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 7)

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 1)

Plattform-Port-Zuordnungen zum Verkabelung eines AFF A150, ASA A150, FAS2750 oder AFF A220 Systems mit einem Broadcom BES-53248 Switch prüfen:

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused	disabled	
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- Wenn beide MetroCluster-Konfigurationen dieselbe Plattform verwenden, empfiehlt NetApp die Auswahl der Gruppe „MetroCluster 3“ für eine Konfiguration und die Gruppe „MetroCluster 4“ für die andere Konfiguration. Wenn die Plattformen unterschiedlich sind, müssen Sie für die erste Konfiguration „MetroCluster 3“ oder „MetroCluster 4“ und für die zweite Konfiguration „MetroCluster 1“ oder „MetroCluster 2“ auswählen.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 2)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- Wenn beide MetroCluster-Konfigurationen dieselbe Plattform verwenden, empfiehlt NetApp die Auswahl der Gruppe „MetroCluster 3“ für eine Konfiguration und die Gruppe „MetroCluster 4“ für die andere Konfiguration. Wenn die Plattformen unterschiedlich sind, müssen Sie für die erste Konfiguration „MetroCluster 3“ oder „MetroCluster 4“ und für die zweite Konfiguration „MetroCluster 1“ oder „MetroCluster 2“ auswählen.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 3)

Überprüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A20-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e2a	e4a
2			
3	MetroCluster 2, Local Cluster interface	e2a	e4a
4			
5	MetroCluster 1, MetroCluster interface	e2b	e4b
6			
7	MetroCluster 2, MetroCluster interface	e2b	e4b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 3, Local Cluster interface (note 1)	e2a	e4a
18			
19	MetroCluster 3, MetroCluster interface (note 1)	e2b	e4b
20			
21	MetroCluster 4, Local Cluster interface (note 1)	e2a	e4a
22			
23	MetroCluster 4, MetroCluster interface (note 1)	e2b	e4b
24			
..	Ports not licensed (25 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 4)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem Broadcom BES-53248-Switch unter Verwendung einer 25-Gbit-Ethernet-Karte mit vier Ports zu verkabeln.

- Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.
- Diese Konfiguration erfordert einen QSFP-zu-SFP+-Adapter in der Karte des Controllers, um eine Netzwerkgeschwindigkeit von 25 Gbit/s zu unterstützen.

Physical Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4							
5	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
6							
7	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9 - 12	Unused	disabled		disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 3, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
18							
19	MetroCluster 3, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
20							
21	MetroCluster 4, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
22							
23	MetroCluster 4, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
24							
..	Ports not licensed (25 - 54)						
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
54							
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
56							

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 5)

Prüfen Sie die Zuordnungen der Plattform-Ports zur Verkabelung eines FAS8200 oder AFF A300 Systems mit einem Broadcom BES-53248-Switch:

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 6)

Überprüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A320-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- **Hinweis 2**: Nur ein MetroCluster mit vier Knoten kann mit AFF A320 Systemen an den Switch angeschlossen werden.

  Funktionen, die einen Switch-Cluster erfordern, werden in dieser Konfiguration nicht unterstützt. Dazu gehören auch die Verfahren zur Umstellung von MetroCluster FC auf IP und zur Technologieaktualisierung.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 7)

Prüfen der Plattform-Port-Zuordnungen für die Verkabelung einer FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 oder FAS8700 System auf einen Broadcom BES-53248 Switch:

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see Note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- **Hinweis 2**: Nur ein MetroCluster mit vier Knoten kann mit AFF A320 Systemen an den Switch angeschlossen werden.

  Funktionen, die einen Switch-Cluster erfordern, werden in dieser Konfiguration nicht unterstützt. Dazu gehören auch die Verfahren zur Umstellung von MetroCluster FC auf IP und zur Technologieaktualisierung.

Plattform-Portzuweisungen für von NVIDIA unterstützte SN2100-IP-Switches in einer MetroCluster IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Zum Verbinden einer MetroCluster-Konfiguration mit acht oder zwei vier Nodes sind ONTAP 9.14.1 oder höher und RCF-Dateiversion 2.00 oder höher erforderlich.

  > Die Version der RCF-Datei unterscheidet sich von der Version des RCFfilegenerator-Tools, mit dem die Datei generiert wird. Beispielsweise können Sie eine RCF-Datei Version 2.00 mit RCFfilegenerator v1.6c generieren.

- Wenn Sie mehrere MetroCluster-Konfigurationen verkabeln, folgen Sie dann der entsprechenden Tabelle. Beispiel:
  - Wenn Sie zwei MetroCluster-Konfigurationen des Typs AFF A700 mit vier Nodes verkabeln, verbinden Sie die erste MetroCluster, die als „MetroCluster 1“ angezeigt wird, und die zweite MetroCluster, die in der AFF A700 Tabelle als „MetroCluster 2“ dargestellt ist.

> Die Ports 13 und 14 können im nativen Geschwindigkeitsmodus mit Unterstützung von 40 Gbit/s und 100 Gbit/s oder im Breakout-Modus zur Unterstützung von 4 × 25 Gbit/s oder 4 × 10 Gbit/s verwendet werden. Wenn sie den einheitlichen Geschwindigkeitsmodus verwenden, werden sie als Ports 13 und 14 dargestellt. Wenn sie den Breakout-Modus verwenden, entweder 4 × 25 Gbit/s oder 4 × 10 Gbit/s, dann werden sie als Ports 13s0-3 und 14s0-3 dargestellt.

In den folgenden Abschnitten wird die Beschreibung der physischen Verkabelung beschrieben. Sie können auch auf die verweisen "RCfFileGenerator" Für detaillierte Informationen zur Verkabelung.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 1)
AFF A20	NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 2)

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF C30, AFF A30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3a -25G) • NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 3b -100G)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700 FAS9000, AFF A700	NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 4)
AFF A50	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 5)
AFF C800, ASA C800 AFF A800, ASA A800 FAS9500 AFF A900, ASA A900	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 7)

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 1)

Überprüfen Sie die Zuordnungen der Plattformports zur Verkabelung von AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 oder ASA A250-System auf einem NVIDIA SN2100-Switch:

Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 2)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A20-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e2a	e4a
s1s1-3		disabled	
2s0		e2a	e4a
2s1-3		disabled	
3s0	MetroCluster 2, Local Cluster interface	e2a	e4a
3s1-3		disabled	
4s0		e2a	e4a
4s1-3		disabled	
5s0	MetroCluster 3, Local Cluster interface	e2a	e4a
5s1-3		disabled	
6s0		e2a	e4a
6s1-3		disabled	
7	MetroCluster 1, MetroCluster interface	e2b	e4b
8			
9	MetroCluster 2, MetroCluster interface	e2b	e4b
10			
11	MetroCluster 3, MetroCluster interface	e2b	e4b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3a)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem NVIDIA SN2100-Switch über eine 25-Gbit-Ethernet-Karte mit vier Ports zu verkabeln:

> Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem NVIDIA SN2100-Switch über eine 100-GbE-Karte mit zwei Ports zu verkabeln:

> Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 4)

Prüfen der Plattform-Port-Zuordnungen für die Verkabelung einer FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 FAS8700, FAS9000 oder AFF A700 System auf einem NVIDIA SN2100 Switch:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
2	Local Cluster interface						Note 1
3	MetroCluster 2,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
4	Local Cluster interface						Note 1
5	MetroCluster 3,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
6	Local Cluster interface						Note 1
7	MetroCluster 1,	e1a	e1b	e1a	e1b	e5a	e5b
8	MetroCluster interface						
9	MetroCluster 2,	e1a	e1b	e1a	e1b	e5a	e5b
10	MetroCluster interface						
11	MetroCluster 3,	e1a	e1b	e1a	e1b	e5a	e5b
12	MetroCluster interface						
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G						
15	ISL, Local Cluster	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16	100G						

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 5)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A50-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1,	e4a	e4b
2	Local Cluster interface		
3	MetroCluster 2,	e4a	e4b
4	Local Cluster interface		
5	MetroCluster 3,	e4a	e4b
6	Local Cluster interface		
7	MetroCluster 1,	e2a	e2b
8	MetroCluster interface		
9	MetroCluster 2,	e2a	e2b
10	MetroCluster interface		
11	MetroCluster 3,	e2a	e2b
12	MetroCluster interface		
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G		
15	ISL, Local Cluster	ISL, Local Cluster	
16	100G		

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 6)

Plattform-Port-Zuordnungen zur Verkabelung von AFF C800, ASA C800, AFF A800, ASA A800, FAS9500 prüfen AFF A900 oder ASA A900 System zu einem NVIDIA SN2100-Switch:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 7)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein FAS70-, AFF A70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
8									
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
12									
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3									
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16									

Verkabeln Sie die ONTAP Controllermodul-Ports in einer MetroCluster IP-Konfiguration

Sie müssen die für Cluster-Peering, Management und Datenkonnektivität verwendeten Controller-Modul-Ports verkabeln.

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.

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"

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

   Befolgen Sie die Installationsanweisungen für Ihre Plattform auf der "Dokumentation zu ONTAP Hardwaresystemen".

   > MetroCluster IP-Systeme verfügen über keine dedizierten HA-Ports (High Availability). Je nach Plattform wird der HA-Datenverkehr über die MetroCluster, den lokalen Cluster oder die Shared Cluster/MetroCluster-Schnittstelle bedient. Wenn Sie zur Installation Ihrer Plattform *ONTAP Hardware Systems Documentation* verwenden, sollten Sie die Anweisungen zum Verkabelung des Clusters und der HA-Ports nicht befolgen.

Konfigurieren Sie die MetroCluster IP-Switches

Wählen Sie das richtige Konfigurationsverfahren für den MetroCluster IP-Switch

Sie müssen die IP-Switches konfigurieren, um eine Back-End-MetroCluster-IP-Konnektivität bereitzustellen. Das von Ihnen zu befolgende Verfahren hängt von Ihrem Switch-Anbieter ab.

- "Konfigurieren Sie Broadcom IP-Switches"
- "Konfigurieren Sie Cisco IP-Switches"
- "Konfigurieren Sie NVIDIA IP-Switches"

Konfigurieren Sie Broadcom IP-Switches für Cluster-Interconnect und Backend- MetroCluster IP-Konnektivität

Sie müssen die Broadcom IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

> Ihre Konfiguration erfordert zusätzliche Lizenzen (6 x 100-GB-Port-Lizenz) in den folgenden Szenarien:

- Die Ports 53 und 54 werden als MetroCluster-ISL mit 40 Gbit/s oder 100 Gbit/s verwendet.
- Sie verwenden eine Plattform, die das lokale Cluster und MetroCluster-Schnittstellen mit den Ports 49 - 52 verbindet.

Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen

Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Broadcom-Switch-Einstellungen löschen und eine grundlegende Konfiguration durchführen.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Wechseln Sie zur erhöhten Eingabeaufforderung (`#`): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Löschen Sie die Startkonfiguration, und entfernen Sie das Banner

   a. Löschen der Startkonfiguration:

   `erase startup-config`

```
(IP_switch_A_1) #erase startup-config

Are you sure you want to clear the configuration? (y/n) y

(IP_switch_A_1) #
```

   Dieser Befehl löscht das Banner nicht.

   b. Entfernen Sie das Banner:

   `no set clibanner`

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Starten Sie den Switch neu:*`(IP_switch_A_1) #reload*`

```
Are you sure you would like to reset the system? (y/n) y
```

   Wenn das System fragt, ob die nicht gespeicherte oder geänderte Konfiguration vor dem erneuten Laden des Switches gespeichert werden soll, wählen Sie **Nein** aus.

4. Warten Sie, bis der Schalter neu geladen wurde, und melden Sie sich dann am Switch an.

   Der Standardbenutzer lautet „`admin`“, und es ist kein Passwort festgelegt. Es wird eine Eingabeaufforderung wie die folgende angezeigt:

```
(Routing)>
```

5. Zur erhöhten Eingabeaufforderung wechseln:

   `enable`

```
Routing)> enable
(Routing) #
```

6. Legen Sie das Service-Port-Protokoll auf fest `none`:

   `serviceport protocol none`

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Weisen Sie die IP-Adresse dem Service-Port zu:

   `serviceport ip` *`ip-address netmask gateway`*

   Das folgende Beispiel zeigt eine dem Service-Port zugewiesene IP-Adresse „10.10.10.10“ mit dem Subnetz „255.255.255.0“ und dem Gateway „10.10.10.1“:

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Überprüfen Sie, ob der Service-Port ordnungsgemäß konfiguriert ist:

   `show serviceport`

   Das folgende Beispiel zeigt, dass der Port als aktiv ist und die richtigen Adressen zugewiesen wurden:

```
(Routing) #show serviceport

Interface Status............................... Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. Konfigurieren Sie den SSH-Server.

> - Die RCF-Datei deaktiviert das Telnet-Protokoll. Wenn Sie den SSH-Server nicht konfigurieren, können Sie nur über die serielle Port-Verbindung auf die Bridge zugreifen.
> - Sie müssen den SSH-Server konfigurieren, um die Protokollsammlung und andere externe Tools verwenden zu können.

a. Generieren von RSA-Schlüsseln.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. DSA-Schlüssel generieren (optional)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Wenn Sie die FIPS-konforme Version von EFOS verwenden, generieren Sie die ECDSA-Schlüssel. Im folgenden Beispiel werden die Schlüssel mit einer Länge von 521 erstellt. Gültige Werte sind 256, 384 oder 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Aktivieren Sie den SSH-Server.

Schließen Sie bei Bedarf den Konfigurationskontext.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

> Wenn Schlüssel bereits vorhanden sind, werden Sie möglicherweise aufgefordert, sie zu überschreiben.

10. Konfigurieren Sie bei Bedarf die Domäne und den Namensserver:

    `configure`

    Das folgende Beispiel zeigt die `ip domain` Und `ip name server` Befehl:

    ```
    (Routing) # configure
    (Routing) (Config)#ip domain name lab.netapp.com
    (Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

11. Konfigurieren Sie auf Wunsch die Zeitzone und die Zeitsynchronisierung (SNTP).

    Das folgende Beispiel zeigt die `sntp` Befehle, die IP-Adresse des SNTP-Servers und der relativen Zeitzone angeben.

    ```
    (Routing) #
    (Routing) (Config)#sntp client mode unicast
    (Routing) (Config)#sntp server 10.99.99.5
    (Routing) (Config)#clock timezone -7
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

    Verwenden Sie für EFOS Version 3.10.0.3 und höher den `ntp` Befehl, wie im folgenden Beispiel dargestellt:

```
> (Config)# ntp ?

authenticate             Enables NTP authentication.
authentication-key       Configure NTP authentication key.
broadcast                Enables NTP broadcast mode.
broadcastdelay           Configure NTP broadcast delay in microseconds.
server                   Configure NTP server.
source-interface         Configure the NTP source-interface.
trusted-key              Configure NTP authentication key number for
trusted time source.
vrf                      Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Konfigurieren Sie den Switch-Namen:

    ```
    hostname IP_switch_A_1
    ```

    In der Switch-Eingabeaufforderung wird der neue Name angezeigt:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Konfiguration speichern:

    ```
    write memory
    ```

    Sie erhalten Eingabeaufforderungen und Ausgabe ähnlich dem folgenden Beispiel:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Broadcom-Switch EFOS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe muss bei jedem Switch in der MetroCluster IP-Konfiguration wiederholt werden.

Beachten Sie Folgendes:

- Beim Upgrade von EFOS 3.4.x.x auf EFOS 3.7.x.x oder höher muss auf dem Switch EFOS 3.4.4.6 (oder höher 3.4.x.x-Version) ausgeführt werden. Wenn Sie vor dieser Version eine Version ausführen, aktualisieren Sie zuerst den Switch auf EFOS 3.4.4.6 (oder höher 3.4.x.x Version), und aktualisieren Sie dann den Switch auf EFOS 3.7.x.x oder höher.
- Die Konfiguration für EFOS 3.4.x.x und 3.7.x.x oder höher ist unterschiedlich. Wenn Sie die EFOS-Version von 3.4.x.x auf 3.7.x.x oder höher ändern oder umgekehrt, müssen Sie den Switch auf die Werkseinstellungen zurücksetzen und die RCF-Dateien für die entsprechende EFOS-Version werden (neu) angewendet. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.
- Ab EFOS Version 3.7.x.x oder höher ist eine FIPS-konforme Version und eine FIPS-konforme Version verfügbar. Verschiedene Schritte gelten für den Wechsel von einem nicht FIPS-konformen auf eine FIPS-konforme Version oder umgekehrt. Wenn EFOS von einer nicht FIPS-konformen Version oder umgekehrt geändert wird, wird der Switch auf die Werkseinstellungen zurückgesetzt. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.

Schritte

1. Laden Sie die Switch-Firmware aus dem herunter"Broadcom Support-Site".
2. Überprüfen Sie, ob Ihre EFOS-Version FIPS-konform oder nicht-FIPS-konform ist, indem Sie die verwenden `show fips status` Befehl. In den folgenden Beispielen: `IP_switch_A_1` Verwendet FIPS-konformes EFOS und `IP_switch_A_2` Verwendet ein nicht FIPS-konformes EFOS.

Beispiel 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Beispiel 2

```
IP_switch_A_2 #show fips status
                     ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

3. Bestimmen Sie anhand der folgenden Tabelle, welche Methode Sie befolgen müssen:

Verfahren	**Aktuelle EFOS-Version**	* Neue EFOS-Version*	**Hohe Stufen**
Schritte zur Aktualisierung von EFOS zwischen zwei (nicht) FIPS-konformen Versionen	3.4.x.x	3.4.x.x	Installieren Sie das neue EFOS-Image mit Methode 1) die Konfigurations- und Lizenzinformationen bleiben erhalten
3.4.4.6 (oder höher 3.4.x.x)	3.7.x.x oder höher ohne FIPS-konform	EFOS mit Methode 1 aktualisieren. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.7.x.x oder höher an	3.7.x.x oder höher ohne FIPS-konform
3.4.4.6 (oder höher 3.4.x.x)	EFOS mit Methode 1 abstufen. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.4.x.x an	3.7.x.x oder höher ohne FIPS-konform	

Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten	3.7.x.x oder höher FIPS-konform	3.7.x.x oder höher FIPS-konform	Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten
Schritte zum Upgrade auf/von einer FIPS-konformen EFOS-Version	Nicht FIPS-konform	FIPS-konform	Installation des EFOS-Images unter Verwendung von Methode 2. Informationen zur Switch-Konfiguration und -Lizenz gehen verloren.

- Methode 1: Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition
- Methode 2: Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition

Die folgenden Schritte können nur ausgeführt werden, wenn beide EFOS-Versionen nicht FIPS-konform sind oder beide EFOS-Versionen FIPS-konform sind.

> Führen Sie diese Schritte nicht aus, wenn eine Version FIPS-konform ist und die andere Version nicht FIPS-konform ist.

Schritte

1. Kopieren Sie die Switch-Software auf den Switch: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   In diesem Beispiel wird die betriebssystemdatei efos-3.4.4.6.stk vom SFTP-Server unter 50.50.50.50 auf die Sicherungspartition kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode........................................ SFTP
Set Server IP................................ 50.50.50.50
Path......................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Legen Sie beim nächsten Neustart des Switches den Switch fest, der von der Backup-Partition aus gestartet werden soll:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Vergewissern Sie sich, dass das neue Startabbild beim nächsten Start aktiv ist:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Konfiguration speichern:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Starten Sie den Switch neu:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Warten Sie, bis der Schalter neu gestartet wurde.

> In seltenen Fällen kann der Switch nicht booten. Folgen Sie den Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation Um das neue Image zu installieren.

7. Wenn Sie den Switch von EFOS 3.4.x.x auf EFOS 3.7.x.x oder umgekehrt umstellen, befolgen Sie die folgenden beiden Verfahren, um die korrekte Konfiguration (RCF) anzuwenden:
   a. Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Herunterladen und Installieren der Broadcom RCF-Dateien
8. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Sie können die folgenden Schritte durchführen, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist. Mit diesen Schritten kann das nicht-FIPS- oder FIPS-konforme EFOS 3.7.x.x-Image von ONIE installiert werden, wenn der Switch nicht startet.

Schritte

1. Starten Sie den Schalter in den ONIE-Installationsmodus.

   Wählen Sie während des Startvorgangs ONIE aus, wenn der folgende Bildschirm angezeigt wird:

```
+-----------------------------------------------------------------------+
|EFOS                                                                   |
|*ONIE                                                                  |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
+-----------------------------------------------------------------------+
```

   Nach der Auswahl von „ONIE“ wird der Schalter geladen und Ihnen folgende Auswahlmöglichkeiten zur Verfügung stehen:

```
 +-----------------------------------------------------------------+
 |*ONIE: Install OS                                                |
 | ONIE: Rescue                                                    |
 | ONIE: Uninstall OS                                              |
 | ONIE: Update ONIE                                               |
 | ONIE: Embed ONIE                                                |
 | DIAG: Diagnostic Mode                                           |
 | DIAG: Burn-In Mode                                              |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 +-----------------------------------------------------------------+
```

Der Schalter startet nun in den ONIE-Installationsmodus.

2. Beenden Sie die ONIE-Erkennung, und konfigurieren Sie die ethernet-Schnittstelle

   Sobald die folgende Meldung angezeigt wird, drücken Sie <ENTER>, um die ONIE-Konsole zu öffnen:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   Die ONIE-Erkennung wird fortgesetzt, und Meldungen werden auf die Konsole gedruckt.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Konfigurieren Sie die ethernet-Schnittstelle und fügen Sie die Route mit hinzu `ifconfig eth0 <ipAddress> netmask <netmask> up` Und `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Stellen Sie sicher, dass der Server, der die ONIE-Installationsdatei hostet, erreichbar ist:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Installieren Sie die neue Switch-Software

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Die Software wird installiert und startet den Switch dann neu. Lassen Sie den Switch normal in die neue EFOS-Version neu starten.

6. Vergewissern Sie sich, dass die neue Switch-Software installiert ist

show bootvar

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Schließen Sie die Installation ab

   Der Switch wird neu gestartet, ohne dass die Konfiguration angewendet wurde, und setzt die Werkseinstellungen zurück. Befolgen Sie die beiden Verfahren, um die Grundeinstellungen des Switches zu konfigurieren und die RCF-Datei anzuwenden, wie in den folgenden beiden Dokumenten beschrieben:

   a. Konfigurieren Sie die Grundeinstellungen des Switches. Befolgen Sie Schritt 4 und höher: Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Erstellen und wenden Sie die RCF-Datei wie in beschrieben an Herunterladen und Installieren der Broadcom RCF-Dateien

Herunterladen und Installieren der Broadcom RCF-Dateien

Sie müssen die Switch-RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Bevor Sie beginnen

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Über diese Aufgabe

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	v1.32_Switch-A1.txt
IP_Switch_A_2	v1.32_Switch-A2.txt
IP_Switch_B_1	v1.32_Switch-B1.txt
IP_Switch_B_2	v1.32_Switch-B2.txt

> Die RCF-Dateien für EFOS Version 3.4.4.6 oder höher 3.4.x.x Version und EFOS Version 3.7.0.4 sind unterschiedlich. Sie müssen sicherstellen, dass Sie die richtigen RCF-Dateien für die EFOS-Version erstellt haben, auf der der Switch ausgeführt wird.

EFOS-Version	RCF-Dateiversion
3.4.x.x	V1.3x, v1.4x
3.7.x.x	v2.x

Schritte

1. Generieren Sie die Broadcom RCF-Dateien für die MetroCluster-IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP"
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch:
   ```
   copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr
   ```

   In diesem Beispiel wird die RCF-Datei „BES-53248_v1.32_Switch-A1.txt“ vom SFTP-Server unter „50.50.50.50“ in den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode............................................ SFTP
Set Server IP................................... 50.50.50.50
Path............................................ /RcfFiles/
Filename........................................ BES-
53248_v1.32_Switch-A1.txt
Data Type....................................... Config Script
Destination Filename........................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"*******************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248



...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Überprüfen Sie, ob die RCF-Datei als Skript gespeichert ist:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr             852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Anwenden des RCF-Skripts:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"*********************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Konfiguration speichern:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Starten Sie den Switch neu:

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

a. Wiederholen Sie die vorherigen Schritte für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Schalter neu laden:

```
reload
```

```
IP_switch_A_1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

> Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

Für Details zum ISL-Port

Führen Sie den Befehl aus `show port all`.

Für Port-Channel-Details

Führen Sie den Befehl aus `show port-channel all`.

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Konfigurieren Sie Cisco IP-Switches

Konfigurieren Sie Cisco IP-Switches für Cluster-Interconnect und Backend- MetroCluster IP-Konnektivität

Sie müssen die Cisco IP Switches für die Verwendung als Cluster Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

Über diese Aufgabe

Einige der Verfahren in diesem Abschnitt sind unabhängige Verfahren, und Sie müssen nur diejenigen ausführen, die Sie an Ihre Aufgabe gerichtet sind oder für Ihre Aufgabe relevant sind.

Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen

Bevor Sie eine RCF-Datei installieren, müssen Sie die Cisco Switch-Konfiguration löschen und die grundlegende Konfiguration durchführen. Dieses Verfahren ist erforderlich, wenn Sie dieselbe RCF-Datei nach einer vorherigen Installation neu installieren möchten oder wenn Sie eine neue Version einer RCF-Datei installieren möchten.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

   a. Löschen Sie die vorhandene Konfiguration:

```
write erase
```

b. Laden Sie die Switch-Software neu:

```
reload
```

Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung „`Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/Nein)[n]`", you should respond `yes` Fortfahren.

c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:

- Admin-Passwort
- Switch-Name
- Out-of-Band-Managementkonfiguration
- Standard-Gateway
- SSH-Service (RSA)

  Nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

Das folgende Beispiel zeigt die Eingabeaufforderungen und Systemantworten bei der Konfiguration des Switches. Die Winkelklammern (`<<<`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Sie geben grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Managementadresse und Gateway, und wählen SSH mit RSA aus.

Dieses Beispiel zeigt die minimalen Informationen, die für die Konfiguration des RCF erforderlich sind. Nach der Anwendung des RCF können weitere Optionen konfiguriert werden. Sie können beispielsweise SNMPv3, NTP oder SCP/SFTP konfigurieren, nachdem Sie den RCF installiert haben.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Reihe von Eingabeaufforderungen vervollständigt die Konfiguration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[##########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch-A-1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch-A-1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco Switch NX-OS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Schritte

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Software-Download"

2. Kopieren Sie die Switch-Software auf den Switch:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   In diesem Beispiel werden die Datei nxos.7.0.3.I4.6.bin und das EPLD-Image vom SFTP-Server 10.10.99.99 in den lokalen Bootflash kopiert:

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                 161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind:

   ```
   dir bootflash:
   ```

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software:

   ```
   install all nxos bootflash:nxos.version-number.bin
   ```

   Der Switch wird automatisch neu geladen (neu gestartet), nachdem die Switch-Software installiert wurde.

   Das folgende Beispiel zeigt die Softwareinstallation auf IP_Switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Überprüfen Sie, ob die Switch-Software installiert wurde:
   `show version`

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

```
IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  ------------------ ------------- ----------- -----------------
     1         SUP         Yes           disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module   Type  Upgrade-Result
-------- ----- --------------
     1   SUP   Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. [[STEP 8]]nach dem Neustart des Switches melden Sie sich erneut an und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

   ```
   show version module 1 epld
   ```

9. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco IP RCF-Dateien

Sie müssen die RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Wenn Sie einen QSFP-zu-SFP+-Adapter verwenden, müssen Sie den ISL-Port möglicherweise im nativen Geschwindigkeitsmodus statt im Breakout-Speed-Modus konfigurieren. Informationen zur Bestimmung des ISL-Port-Geschwindigkeitsmodus finden Sie in der Dokumentation des Switch-Herstellers.

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Schritte

1. Erstellen Sie die Cisco RCF-Dateien für MetroCluster IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP"
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

   Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch:

   ```
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
   bootflash: vrf management
   ```

   In diesem Beispiel wird die RCF-Datei NX3232_v1.80_Switch-A1.txt vom SFTP-Server unter 10.10.99.99 auf den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Wiederholen Sie den vorherigen Unterschritt für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Überprüfen Sie bei jedem Switch, ob die RCF-Datei im Bootflash-Verzeichnis jedes Switches vorhanden ist:

   ```
   dir bootflash:
   ```

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

   ```
   IP_switch_A_1# dir bootflash:
                     .
                     .
                     .
   5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                     .
                     .
                     .

   Usage for bootflash://sup-local
   1779363840 bytes used
   13238841344 bytes free
   15018205184 bytes total
   IP_switch_A_1#
   ```

4. Konfigurieren Sie die TCAM-Regionen auf Cisco Switches 3132Q-V und Cisco 3232C-Switches.

   Überspringen Sie diesen Schritt, wenn Cisco 3132Q-V oder Cisco 32Q-V Switches nicht vorhanden sind.

a. Stellen Sie auf dem Cisco Switch 3132Q-V die folgenden TCAM-Bereiche ein:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. Legen Sie auf dem Cisco 3232C Switch die folgenden TCAM-Regionen fest:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Speichern Sie nach dem Einstellen der TCAM-Bereiche die Konfiguration, und laden Sie den Schalter neu:

```
copy running-config startup-config
reload
```

5. Kopieren Sie die passende RCF-Datei vom lokalen Bootflash auf jeden Switch in die laufende Konfiguration:

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Kopieren Sie die RCF-Dateien von der ausgeführten Konfiguration auf die Startkonfiguration auf jedem Switch:

   `copy running-config startup-config`

   Sie sollten eine Ausgabe wie die folgende sehen:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Schalter neu laden:

   `reload`

```
IP_switch_A_1# reload
```

8. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Einstellen der Vorwärtskorrektur für Systeme mit 25-Gbit/s-Konnektivität

Wenn Ihr System mit 25-Gbit/s-Konnektivität konfiguriert ist, müssen Sie den fec-Parameter (Forward Error Correction) nach Anwendung der RCF-Datei manuell auf OFF setzen. Die RCF-Datei wendet diese Einstellung nicht an.

Über diese Aufgabe

Die 25-Gbps-Ports müssen vor Durchführung dieses Verfahrens verkabelt werden.

"Plattform-Port-Zuweisungen für Cisco 3232C- oder Cisco 9336C-Switches"

Diese Aufgabe gilt nur für Plattformen mit 25-Gbit/s-Konnektivität:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Diese Aufgabe muss an allen vier Switches der MetroCluster IP-Konfiguration ausgeführt werden.

Schritte

1. Stellen Sie den fec-Parameter auf aus für jeden 25-Gbit/s-Port, der mit einem Controller-Modul verbunden ist, und kopieren Sie dann die laufende Konfiguration in die Startkonfiguration:

   a. Konfigurationsmodus aufrufen: `config t`

   b. Geben Sie die zu konfigurierende 25-Gbit/s-Schnittstelle an: `interface interface-ID`

   c. fec auf aus stellen: `fec off`

   d. Wiederholen Sie die vorherigen Schritte für jeden 25-Gbit/s-Port am Switch.

   e. Konfigurationsmodus beenden: `exit`

   Im folgenden Beispiel werden die Befehle für Interface ethernet1/25/1 auf Switch IP_Switch_A_1 angezeigt:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Wiederholen Sie den vorherigen Schritt auf den anderen drei Switches der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle:

   ```
   show interface brief
   ```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

   ```
   SwitchA_1# config t
   Enter configuration commands, one per line. End with CNTL/Z.
   SwitchA_1(config)# int Eth1/14
   SwitchA_1(config-if)# shutdown
   SwitchA_12(config-if)# exit
   SwitchA_1(config-if)# copy running-config startup-config
   [########################################] 100%
   Copy complete, now saving to disk (please wait)...
   Copy complete.
   ```

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches in einem MetroCluster IP-Standort

Die MACsec-Verschlüsselung kann nur auf die WAN-ISL-Ports angewendet werden.

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches

Sie müssen die MACsec-Verschlüsselung nur für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

Lizenzierungsanforderungen für MACsec

MACsec erfordert eine Sicherheitslizenz. Eine vollständige Erläuterung des Cisco NX-OS-Lizenzschemas und der Beschaffung und Anwendung von Lizenzen finden Sie im "Cisco NX-OS Licensing Guide"

Aktivierung von Cisco MACs Encryption WAN-ISLs in MetroCluster IP-Konfigurationen

Sie können die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration aktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   ```
   configure terminal
   ```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Aktivieren Sie MACsec und MKA auf dem Gerät:

   `feature macsec`

   ```
   IP_switch_A_1(config)# feature macsec
   ```

3. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Konfigurieren Sie eine MACsec-Schlüsselkette und -Tasten

Sie können eine MACsec-Schlüsselkette oder Schlüssel für Ihre Konfiguration erstellen.

- Key Lifetime und Hitless Key Rollover*

Eine MACsec-Schlüsselkette kann über mehrere vorinstallierte PSKs (Preshared Keys) verfügen, die jeweils mit einer Schlüssel-ID und einer optionalen Lebensdauer konfiguriert sind. Eine Schlüssellebensdauer legt fest, zu welcher Zeit die Taste aktiviert und abläuft. Wenn keine lebenslange Konfiguration vorhanden ist, ist die Standardlebensdauer unbegrenzt. Wenn eine Lebensdauer konfiguriert ist, rollt MKA nach Ablauf der Lebensdauer zum nächsten konfigurierten vorfreigegebenen Schlüssel in der Schlüsselkette um. Die Zeitzone des Schlüssels kann lokal oder UTC sein. Die Standardzeitzone ist UTC. Ein Schlüssel kann auf einen zweiten Schlüssel innerhalb derselben Schlüsselkette übertragen werden, wenn Sie den zweiten Schlüssel (in der Schlüsselkette) konfigurieren und eine Lebensdauer für den ersten Schlüssel konfigurieren. Wenn die Lebensdauer der ersten Taste abläuft, wird automatisch die nächste Taste in der Liste angezeigt. Wenn dieselbe Taste auf beiden Seiten des Links gleichzeitig konfiguriert ist, ist der Schlüsselüberschlag ohne Unterbrechung des Datenverkehrs aktiviert (d. h. der Schlüssel wird ohne Unterbrechung des Datenverkehrs überrollt).

Schritte

1. Den globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Um den verschlüsselten Schlüsselzeichenkette auszublenden, ersetzen Sie den String in der Ausgabe des durch ein Platzhalterzeichen `show running-config` Und `show startup-config` Befehl:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

> Die Oktett-Zeichenfolge wird ebenfalls ausgeblendet, wenn Sie die Konfiguration in einer Datei speichern.

Standardmäßig werden PSK-Schlüssel im verschlüsselten Format angezeigt und können einfach entschlüsselt werden. Dieser Befehl gilt nur für MACsec-Schlüsselketten.

3. Erstellen Sie eine MACsec-Schlüsselkette, um eine Reihe von MACsec-Schlüsseln zu halten und den MACsec-Konfigurationsmodus für die Schlüsselkette aufzurufen:

   `key chain name macsec`

   ```
   IP_switch_A_1(config)# key chain 1 macsec
   IP_switch_A_1(config-macseckeychain)#
   ```

4. Erstellen Sie eine MACsec-Taste, und rufen Sie den MACsec-Key-Konfigurationsmodus auf:

   `key key-id`

   Der Bereich liegt zwischen 1 und 32 hex-stelligen Schlüsselzeichenfolge und die maximale Größe beträgt 64 Zeichen.

   ```
   IP_switch_A_1 switch(config-macseckeychain)# key 1000
   IP_switch_A_1 (config-macseckeychain-macseckey)#
   ```

5. Konfigurieren Sie die Oktett-Zeichenfolge für den Schlüssel:

   `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
   abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
   cryptographic-algorithm AES_256_CMAC
   ```

   > Das Argument Octet-string kann bis zu 64 hexadezimale Zeichen enthalten. Der Oktett-Schlüssel wird intern kodiert, so dass der Schlüssel im Klartext nicht in der Ausgabe des angezeigt wird `show running-config macsec` Befehl.

6. Konfigurieren einer Sendezeit für die Taste (in Sekunden):

   `send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

Standardmäßig behandelt das Gerät die Startzeit als UTC. Das Argument Start-Time ist die Uhrzeit und das Datum, zu der der Schlüssel aktiv wird. Das Argument „Dauer“ ist die Länge der Lebensdauer in Sekunden. Die maximale Länge beträgt 2147483646 Sekunden (ca. 68 Jahre).

7. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

8. Zeigt die Schlüsselkettenkonfiguration an:

   `show key chain name`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
   ```

Konfigurieren einer MACsec-Richtlinie

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Erstellen einer MACsec-Richtlinie:

   `macsec policy name`

   ```
   IP_switch_A_1(config)# macsec policy abc
   IP_switch_A_1(config-macsec-policy)#
   ```

3. Konfigurieren Sie eine der folgenden Chiffren GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 oder GCM-AES-XPN-256:

   `cipher-suite name`

   ```
   IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
   ```

4. Konfigurieren Sie die zentrale Serverpriorität, um die Verbindung zwischen Peers während eines Schlüsselaustauschs zu unterbrechen:

   `key-server-priority number`

   ```
   switch(config-macsec-policy)# key-server-priority 0
   ```

5. Konfigurieren Sie die Sicherheitsrichtlinie, um den Umgang mit Daten und Kontrollpaketen zu definieren:

   `security-policy security policy`

   Wählen Sie aus den folgenden Optionen eine Sicherheitsrichtlinie aus:

   - Must-Secure — Pakete, die keine MACsec-Header tragen, werden verworfen
   - Sollte-sicher — Pakete, die keine MACsec-Header tragen, sind zulässig (dies ist der Standardwert)

   ```
   IP_switch_A_1(config-macsec-policy)# security-policy should-secure
   ```

6. Konfigurieren Sie das Replay Protection-Fenster, damit die gesicherte Schnittstelle kein Paket akzeptiert, das kleiner als die konfigurierte Fenstergröße ist: `window-size number`

   > Die Größe des Replay Protection Window stellt die maximale Anzahl von Frames dar, die von MACsec akzeptiert und nicht verworfen werden. Der Bereich liegt zwischen 0 und 596000000.

   ```
   IP_switch_A_1(config-macsec-policy)# window-size 512
   ```

7. Konfigurieren Sie die Zeit in Sekunden, um einen SAK-Rekey zu erzwingen:

   `sak-expiry-time time`

   Sie können mit diesem Befehl den Sitzungsschlüssel in ein vorhersehbares Zeitintervall ändern. Der Standardwert ist 0.

   ```
   IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
   ```

8. Konfigurieren Sie einen der folgenden Vertraulichkeitsvereinbarungen im Layer 2-Frame, in dem die Verschlüsselung beginnt:

   `conf-offsetconfidentiality offset`

   Wählen Sie eine der folgenden Optionen:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

> Dieser Befehl kann erforderlich sein, damit zwischen den Zwischenschaltern Paketheader (dmac, smac, etype) wie MPLS-Tags verwendet werden können.

9. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

10. Die MACsec-Richtlinienkonfiguration anzeigen:

    `show macsec policy`

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Aktivieren Sie die Verschlüsselung von Cisco MACsec an den Schnittstellen

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Wählen Sie die Schnittstelle aus, die Sie mit MACsec-Verschlüsselung konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

3. Fügen Sie die Schlüsselanhänger und die Richtlinie, die auf der Schnittstelle konfiguriert werden sollen, hinzu, um die MACsec-Konfiguration hinzuzufügen:

   `macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# macsec keychain 1 policy abc
   ```

4. Wiederholen Sie die Schritte 1 und 2 auf allen Schnittstellen, für die die MACsec-Verschlüsselung

konfiguriert werden soll.

5. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Deaktivieren Sie Cisco MACs Verschlüsselungs-WAN-ISLs in MetroCluster IP-Konfigurationen

Möglicherweise müssen Sie die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration deaktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Deaktivieren Sie die MACsec-Konfiguration auf dem Gerät:

   `macsec shutdown`

   ```
   IP_switch_A_1(config)# macsec shutdown
   ```

   Durch Auswahl der Option „`no`“ wird die MACsec-Funktion wiederhergestellt.

3. Wählen Sie die Schnittstelle aus, die Sie bereits mit MACsec konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Entfernen Sie die auf der Schnittstelle konfigurierte Schlüsselanhänger und Richtlinie, um die MACsec-Konfiguration zu entfernen:

   `no macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
   ```

5. Wiederholen Sie die Schritte 3 und 4 auf allen Schnittstellen, für die MACsec konfiguriert ist.
6. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Überprüfen der MACsec-Konfiguration

Schritte

1. Wiederholen Sie * alle* der vorherigen Vorgänge auf dem zweiten Schalter innerhalb der Konfiguration, um eine MACsec-Sitzung einzurichten.
2. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob beide Switches erfolgreich verschlüsselt sind:

   a. Ausführen: `show macsec mka summary`

   b. Ausführen: `show macsec mka session`

   c. Ausführen: `show macsec mka statistics`

   Sie können die MACsec-Konfiguration mit den folgenden Befehlen überprüfen:

Befehl	Zeigt Informationen über… an.
`show macsec mka session interface typeslot/port number`	Die MKA-Sitzung von MACsec für eine bestimmte Schnittstelle oder für alle Schnittstellen
`show key chain name`	Konfiguration der Schlüsselkette
`show macsec mka summary`	Die MKA-Konfiguration von MACsec
`show macsec policy policy-name`	Die Konfiguration für eine bestimmte MACsec-Richtlinie oder für alle MACsec-Richtlinien

Konfigurieren Sie NVIDIA IP-Switches

Konfigurieren Sie den NVIDIA IP SN2100-Switch für die Clusterverbindung und die Backend- MetroCluster IP-Konnektivität

Sie müssen die NVIDIA SN2100 IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

[[Reset-the-Switch] setzt den NVIDIA IP SN2100-Schalter auf die Werkseinstellungen zurück

Sie können eine der folgenden Methoden auswählen, um einen Schalter auf die werkseitigen Standardeinstellungen zurückzusetzen.

- Setzen Sie den Switch mithilfe der RCF-Dateioption zurück

- Laden Sie die Cumulus-Software herunter und installieren Sie sie

Zurücksetzen des Switches mit der RCF-Dateioption

Bevor Sie eine neue RCF-Konfiguration installieren, müssen Sie die NVIDIA-Switch-Einstellungen zurücksetzen.

Über diese Aufgabe

Um den Switch auf die Standardeinstellungen zurückzusetzen, führen Sie die RCF-Datei mit dem aus `restoreDefaults` Option. Mit dieser Option werden die ursprünglichen gesicherten Dateien an den ursprünglichen Speicherort kopiert und anschließend der Switch neu gestartet. Nach dem Neustart wird der Switch mit der ursprünglichen Konfiguration online geschaltet, die bei der ersten Ausführung der RCF-Datei zum Konfigurieren des Switches existierte.

Die folgenden Konfigurationsdetails werden nicht zurückgesetzt:

- Konfiguration von Benutzern und Anmeldeinformationen
- Konfiguration des Management-Netzwerk-Ports, eth0

> Alle anderen Konfigurationsänderungen, die während der Anwendung der RCF-Datei auftreten, werden auf die ursprüngliche Konfiguration zurückgesetzt.

Bevor Sie beginnen

- Sie müssen den Switch gemäß konfigurieren Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie. Wenn Sie auf diese Weise nicht konfiguriert haben oder vor der Ausführung der RCF-Datei zusätzliche Funktionen konfiguriert haben, können Sie dieses Verfahren nicht verwenden.
- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Überprüfen Sie, ob die RCF-Konfiguration erfolgreich mit derselben oder einer kompatiblen RCF-Dateiversion angewendet wurde und ob die Sicherungsdateien vorhanden sind.

   > Die Ausgabe kann Backup-Dateien, erhaltene Dateien oder beides anzeigen. Wenn Sicherungsdateien oder nicht vorhandene Dateien nicht in der Ausgabe angezeigt werden, können Sie dieses Verfahren nicht verwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Führen Sie die RCF-Datei mit der Option zum Wiederherstellen der Standardeinstellungen aus: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Beantworten Sie die Eingabeaufforderung mit „Ja“. Der Switch wird auf die ursprüngliche Konfiguration zurückgesetzt und startet neu.
4. Warten Sie, bis der Schalter neu gestartet wurde.

   Der Switch wird zurückgesetzt und behält die ursprüngliche Konfiguration wie z. B. die Konfiguration des Managementnetzwerks und die aktuellen Zugangsdaten vor dem Anwenden der RCF-Datei bei. Nach dem Neustart können Sie eine neue Konfiguration anwenden, indem Sie dieselbe oder eine andere Version der RCF-Datei verwenden.

Laden Sie die Cumulus-Software herunter und installieren Sie sie

Über diese Aufgabe

Verwenden Sie diese Schritte, wenn Sie den Schalter vollständig zurücksetzen möchten, indem Sie das Cumulus-Bild anwenden.

Bevor Sie beginnen

- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Das Cumulus Switch-Softwarebild ist über HTTP zugänglich.

> Weitere Informationen zur Installation von Cumulus Linux finden Sie unter "Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches"

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.

Schritte

1. Von der Cumulus-Konsole herunterladen und die Switch-Software-Installation mit dem Befehl in Warteschlange stellen `onie-install -a -i` Anschließend folgt der Dateipfad zur Switch-Software:

   In diesem Beispiel die Firmware-Datei `cumulus-linux-4.4.3-mlx-amd64.bin` Wird vom HTTP-Server '50.50.50.50' auf den lokalen Switch kopiert.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
##################################################################
# 100.0%
```

```
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
```

```
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Antworten `y` Um die Eingabeaufforderung zur Bestätigung der Installation zu bestätigen, wenn das Image heruntergeladen und verifiziert wurde.
3. Starten Sie den Switch neu, um die neue Software zu installieren: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> Der Switch startet neu und wechselt in die Switch-Software-Installation, was einige Zeit in Anspruch nimmt. Nach Abschluss der Installation wird der Switch neu gestartet und bleibt an der Eingabeaufforderung „Login“.

4. Konfigurieren Sie die grundlegenden Switch-Einstellungen
   a. Wenn der Switch gestartet wird und in der Anmeldeaufforderung angezeigt wird, melden Sie sich an, und ändern Sie das Passwort.

   > Der Benutzername ist 'Cumulus' und das Standardpasswort lautet 'Cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Konfigurieren Sie die Managementoberfläche.

   Die von Ihnen verwendeten Befehle hängen von der verwendeten Switch-Firmware-Version ab.

   > Die folgenden Beispielbefehle konfigurieren den Hostnamen als IP_Switch_A_1, die IP-Adresse als 10.10.10.10, die Netzmaske als 255.255.255.0 (24) und die Gateway-Adresse als 10.10.10.1.

Cumulus 4.4.x

Mit den folgenden Beispielbefehlen können Sie den Hostnamen, die IP-Adresse, die Netzmaske und das Gateway auf einem Switch konfigurieren, auf dem Cumulus 4.4.x. ausgeführt wird

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

Cumulus 5.4.x und höher

Mit den folgenden Beispielbefehlen können Sie den Hostnamen, die IP-Adresse, die Netzmaske und das Gateway auf einem Switch konfigurieren, auf dem Cumulus 5.4.x. ausgeführt wird Oder höher.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. Starten Sie den Switch mithilfe des neu `sudo reboot` Befehl.

```
cumulus@cumulus:~$ sudo reboot
```

Wenn der Switch neu startet, können Sie eine neue Konfiguration mit den Schritten unter anwenden Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie.

Laden Sie die NVIDIA RCF-Dateien herunter und installieren Sie sie

Sie müssen die Switch-RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Bevor Sie beginnen

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.
- Die Switch-Software wird installiert und das Managementnetzwerk konfiguriert.
- Sie haben die ersten Schritte zur Installation des Switches mit der Methode 1 oder Methode 2 ausgeführt.
- Nach der Erstinstallation haben Sie keine zusätzliche Konfiguration angewendet.

> Wenn Sie nach dem Zurücksetzen des Switches und vor dem Anwenden der RCF-Datei eine weitere Konfiguration durchführen, können Sie dieses Verfahren nicht verwenden.

Über diese Aufgabe

Sie müssen diese Schritte bei jedem der IP-Schalter in der MetroCluster IP-Konfiguration (neue Installation) oder am Ersatzschalter (Switch-Austausch) wiederholen.

Wenn Sie einen QSFP-zu-SFP+-Adapter verwenden, müssen Sie den ISL-Port möglicherweise im nativen Geschwindigkeitsmodus statt im Breakout-Speed-Modus konfigurieren. Informationen zur Bestimmung des ISL-Port-Geschwindigkeitsmodus finden Sie in der Dokumentation des Switch-Herstellers.

Schritte

1. Generieren Sie die NVIDIA RCF-Dateien für MetroCluster IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP".

b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

c. Navigieren Sie zu Ihrem Home Directory. Wenn Sie als 'cumulus' angemeldet sind, lautet der Dateipfad `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

d. Laden Sie die RCF-Datei in dieses Verzeichnis herunter.
Das folgende Beispiel zeigt, dass Sie die Datei mit SCP herunterladen `SN2100_v2.0.0_IP_switch_A_1.txt` Von Server '50.50.50.50' in Ihr Home-Verzeichnis und speichern Sie es als `SN2100_v2.0.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*******************************************************************
**
Banner of the SCP server
*******************************************************************
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Ausführen der RCF-Datei. Die RCF-Datei erfordert eine Option zum Anwenden eines oder mehrerer Schritte. Führen Sie die RCF-Datei ohne die Befehlszeilenoption aus, sofern Sie nicht vom technischen Support dazu aufgefordert werden. Um den Abschlussstatus der verschiedenen Schritte der RCF-Datei zu überprüfen, verwenden Sie die Option '-1' oder 'all', um alle (ausstehenden) Schritte anzuwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

3. Wenn Ihre Konfiguration DAC-Kabel verwendet, aktivieren Sie die DAC-Option an den Switch-Ports:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

Im folgenden Beispiel wird die DAC-Option für den Port aktiviert `swp7`:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.00
    Running command: Enabling the DacOption for port swp7
    runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. Starten Sie den Switch nach Aktivierung der DAC-Option an den Switch-Ports neu:

```
sudo reboot
```

> Wenn Sie die DAC-Option für mehrere Switch-Ports festlegen, müssen Sie den Switch nur einmal neu starten.

Legen Sie die Fehlerkorrektur für Systeme mit 25-Gbit/s-Konnektivität vor

Wenn Ihr System über eine 25-Gbit/s-Konnektivität konfiguriert ist, stellen Sie den Parameter Vorwärtskorrektur (fec) nach Anwendung des RCF manuell auf aus. Die RCF wendet diese Einstellung nicht an.

Über diese Aufgabe

- Diese Aufgabe gilt nur für Plattformen mit 25-Gbit/s-Konnektivität. Siehe "Plattform-Port-Zuweisungen für von NVIDIA unterstützte SN2100 IP-Switches".
- Diese Aufgabe muss an allen vier Switches der MetroCluster IP-Konfiguration ausgeführt werden.
- Sie müssen jeden Switch-Port einzeln aktualisieren. Sie können im Befehl nicht mehrere Ports oder Portbereiche angeben.

Schritte

1. Stellen Sie den `fec` Parameter für den ersten Switch-Port, der eine 25-Gbit/s-Konnektivität verwendet, auf aus:

   ```
   sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
   ```

2. Wiederholen Sie den Schritt für jeden 25-Gbit/s-Switch-Port, der mit einem Controller-Modul verbunden ist.

Stellen Sie die Switch-Port-Geschwindigkeit für die MetroCluster IP-Schnittstellen ein

Über diese Aufgabe

- Gehen Sie folgendermaßen vor, um die Switch-Port-Geschwindigkeit für die folgenden Systeme auf 100 G einzustellen:
  - AFF A70, AFF A90, AFF A1K, AFF C80
  - AFF A30, AFF C30, AFF A50, AFF C60
  - FAS50, FAS70 UND FAS90
- Sie müssen jeden Switch-Port einzeln aktualisieren. Sie können im Befehl nicht mehrere Ports oder Portbereiche angeben.

Schritt

1. Verwenden Sie die RCF-Datei mit der `runCmd` Option, um die Geschwindigkeit einzustellen. Dies wendet die Einstellung an und speichert die Konfiguration.

   Die folgenden Befehle legen die Geschwindigkeit für die MetroCluster-Schnittstellen `swp7` und `swp8`fest:

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
   ```

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
   ```

   Beispiel

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.20
    Running command: Setting switchport swp7 to 100G speed
    runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
    runCmd: 'nv set interface swp7 link speed 100G', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden. Sie müssen jeden Port oder Port-Kanal einzeln deaktivieren. Im Befehl können Sie nicht mehrere Ports oder Port-Bereiche angeben.

Schritte

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

> Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

```
net show interface
```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe der RCF-Datei.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

Mit dem folgenden Beispielbefehl wird der Port „swp14“ deaktiviert:

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Wiederholen Sie diesen Schritt für jeden identifizierten nicht verwendeten Port oder Port-Kanal.

Installieren Sie die Konfigurationsdatei des Ethernet Switch Health Monitors für einen NVIDIA SN2100 MetroCluster IP-Switch

Um die Integritätsüberwachung von Ethernet-Switches auf NVIDIA-Ethernet-Switches zu konfigurieren, befolgen Sie dieses Verfahren.

Diese Anweisungen gelten, wenn NVIDIA X190006-PE und X190006-PI Switches nicht richtig erkannt werden.

Dies kann durch Ausführen von `system switch ethernet show` und prüfen Sie, ob **OTHER** für Ihr Modell angezeigt wird. Um Ihr NVIDIA-Switch-Modell zu identifizieren, suchen Sie die Teilenummer mit dem Befehl `nv show platform hardware` für NVIDIA CL 5.8 und früher oder `nv show platform` für spätere Versionen.

> Diese Schritte werden auch empfohlen, wenn Sie möchten, dass die Integritätsüberwachung und Protokollerfassung bei Verwendung von NVIDIA CL 5.11.x mit den folgenden ONTAP-Versionen wie vorgesehen funktioniert. Auch ohne diese Schritte funktionieren Integritätsüberwachung und Protokollerfassung möglicherweise weiterhin, aber durch deren Befolgung wird sichergestellt, dass alles ordnungsgemäß funktioniert.
>
> - 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 und spätere Patch-Versionen

Bevor Sie beginnen

- Stellen Sie sicher, dass das ONTAP Cluster betriebsbereit ist und ausgeführt wird.
- Aktivieren Sie SSH auf dem Switch, um alle in CSHM verfügbaren Funktionen zu nutzen.
- Löschen Sie das `/mroot/etc/cshm_nod/nod_sign/` Verzeichnis auf allen Knoten:

  a. Betreten Sie die Nodeshell:

  ```
  system node run -node <name>
  ```

  b. Zu erweiterten Berechtigungen wechseln:

  ```
  priv set advanced
  ```

  c. Listen Sie die Konfigurationsdateien im `/etc/cshm_nod/nod_sign` Verzeichnis auf. Wenn das Verzeichnis existiert und Konfigurationsdateien enthält, werden die Dateinamen aufgelistet.

  ```
  ls /etc/cshm_nod/nod_sign
  ```

  d. Löschen Sie alle Konfigurationsdateien, die Ihren angeschlossenen Switch-Modellen entsprechen.

  Wenn Sie sich nicht sicher sind, entfernen Sie alle Konfigurationsdateien für die oben aufgeführten unterstützten Modelle, laden Sie die neuesten Konfigurationsdateien für dieselben Modelle herunter, und installieren Sie sie.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

  a. Vergewissern Sie sich, dass die gelöschten Konfigurationsdateien nicht mehr im Verzeichnis sind:

  ```
  ls /etc/cshm_nod/nod_sign
  ```

Schritte

1. Laden Sie die ZIP-Datei für die Konfiguration der Ethernet-Switch-Systemzustandsüberwachung basierend auf der entsprechenden ONTAP-Version herunter. Diese Datei ist auf der Seite verfügbar "NVIDIA Ethernet-Switches" .

   a. Wählen Sie auf der Download-Seite der NVIDIA SN2100-Software **Nvidia CSHM-Datei** aus.

   b. Aktivieren Sie auf der Seite Achtung/muss gelesen werden das Kontrollkästchen, um zuzustimmen.

   c. Aktivieren Sie auf der Seite Endbenutzer-Lizenzvereinbarung das Kontrollkästchen, um zuzustimmen, und klicken Sie auf **Akzeptieren und Fortfahren**.

d. Wählen Sie auf der Seite Nvidia CSHM File - Download die entsprechende Konfigurationsdatei aus. Folgende Dateien sind verfügbar:

ONTAP 9.15.1 und höher

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 bis 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Laden Sie die entsprechende ZIP-Datei auf Ihren internen Webserver hoch.
2. Greifen Sie von einem der ONTAP-Systeme im Cluster aus auf den erweiterten Modus zu.

   ```
   set -privilege advanced
   ```

3. Führen Sie den Befehl Switch Health Monitor configure aus.

   ```
   cluster1::> system switch ethernet
   ```

4. Überprüfen Sie, ob die Befehlsausgabe mit dem folgenden Text für Ihre ONTAP-Version endet:

ONTAP 9.15.1 und höher

Die Konfigurationsdatei wurde von der Statusüberwachung des Ethernet-Switches installiert.

ONTAP 9.11.1 bis 9.14.1

SHM hat die Konfigurationsdatei installiert.

ONTAP 9.10.1

Das heruntergeladene CSHM-Paket wurde erfolgreich verarbeitet.

Sollte ein Fehler auftreten, wenden Sie sich an den NetApp Support.

1. Warten Sie bis zu zweimal das Abfrageintervall der Ethernet-Switch-Integritätsüberwachung, das durch Ausführen gefunden `system switch ethernet polling-interval show`wird, bevor Sie den nächsten Schritt abschließen.
2. Führen Sie den Befehl auf dem ONTAP-System aus `system switch ethernet show` , und stellen Sie sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **true** und das Seriennummernfeld nicht **Unknown** anzeigt.

```
cluster1::> system switch ethernet show
```

Wenn Ihr Modell nach der Anwendung der Konfigurationsdatei immer noch **ANDERE** anzeigt, wenden Sie sich an den NetApp-Support.

Siehe die "System-Switch-Ethernet-Konfigurations-Health-Monitor" Befehl für weitere Details.

Was kommt als Nächstes?

"Konfigurieren Sie die Überwachung des Switch-Systemzustands".

Überwachen der Integrität des MetroCluster-IP-Switches

Erfahren Sie mehr über die Switch-Integritätsüberwachung in einer MetroCluster-IP-Konfiguration

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich.

Wichtige Hinweise zur Konfiguration von CSHM in einer MetroCluster-IP-Konfiguration

Dieser Abschnitt enthält die allgemeinen Schritte zur Konfiguration von SNMPv3 und zur Protokollerfassung auf Cisco-, Broadcom- und NVIDIA SN2100-Switches. Sie müssen die Schritte für eine Switch-Firmware-Version befolgen, die in einer MetroCluster-IP-Konfiguration unterstützt wird. Weitere Informationen finden Sie im "Hardware Universe" um die unterstützten Firmware-Versionen zu überprüfen.

In einer MetroCluster-Konfiguration konfigurieren Sie die Integritätsüberwachung nur auf den lokalen Cluster-Switches.

Für die Protokollerfassung mit Broadcom- und Cisco-Switches muss für jeden Cluster mit aktivierter Protokollerfassung ein neuer Benutzer auf dem Switch erstellt werden. In einer MetroCluster-Konfiguration bedeutet dies, dass für MetroCluster 1, MetroCluster 2, MetroCluster 3 und MetroCluster 4 jeweils ein separater Benutzer auf den Switches konfiguriert werden muss. Diese Switches unterstützen nicht mehrere SSH-Schlüssel für denselben Benutzer. Bei jeder weiteren Einrichtung der Protokollerfassung werden alle bereits vorhandenen SSH-Schlüssel für den Benutzer überschrieben.

Bevor Sie CSHM konfigurieren, sollten Sie nicht verwendete ISLs deaktivieren, um unnötige ISL-Warnmeldungen zu vermeiden.

Konfigurieren Sie SNMPv3, um den Zustand von MetroCluster IP-Switches zu überwachen

In MetroCluster IP-Konfigurationen können Sie SNMPv3 zur Überwachung des Funktionszustands von IP-Switches konfigurieren.

Dieses Verfahren zeigt die allgemeinen Schritte zum Konfigurieren von SNMPv3 auf einem Switch. Einige der aufgeführten Switch-Firmware-Versionen werden in einer MetroCluster-IP-Konfiguration möglicherweise nicht unterstützt.

Sie müssen die Schritte für eine Switch-Firmware-Version befolgen, die in einer MetroCluster-IP-Konfiguration unterstützt wird. Weitere Informationen finden Sie im "Hardware Universe" um die unterstützten Firmware-Versionen zu überprüfen.

- SNMPv3 wird nur auf ONTAP 9.12.1 und höher unterstützt.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 und spätere Versionen beheben diese beiden Probleme:
  - "Bei der ONTAP-Integritätsüberwachung von Cisco-Switches kann der SNMPv2-Verkehr nach der Umstellung auf SNMPv3 zur Überwachung weiterhin sichtbar sein."
  - "Falsch-positive Switch-Lüfter- und Stromwarnungen bei SNMP-Fehlern"

Über diese Aufgabe

Die folgenden Befehle werden verwendet, um einen SNMPv3-Benutzernamen auf den Switches **Broadcom**, **Cisco** und **NVIDIA** zu konfigurieren:

Broadcom-Switches

Konfigurieren Sie einen NETZWERKBETREIBER für SNMPv3-Benutzernamen auf Broadcom BES-53248-Switches.

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-
md5|auth-sha] [priv-aes128|priv-des]
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version
SNMPv3 -community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp status
```

```
(sw1)(Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1)(Config)# show snmp user snmp

     Name            Group Name      Auth Priv
                                     Meth Meth    Remote Engine ID
---------------- ------------------ ---- ------
-------------------------
<username>        network-admin      MD5  AES128
8000113d03d8c497710bee
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

                                   Device Name: sw1
                                    IP Address: 10.228.136.24
                                  SNMP Version: SNMPv2c
                                 Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                  Model Number: BES-53248
                                 Switch Network: cluster-network
                               Software Version: 3.9.0.2
                     Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                 Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Überprüfen Sie nach dem Abwarten der CSHM-Abfrageperiode, ob die Seriennummer für den Ethernet-Switch eingetragen ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: <username>
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                     Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                               Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA
```

Cisco Switches

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf Cisco 9336C-FX2-Switches:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```

- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt  auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

```
(sw1)(Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1)(Config)# show snmp user

-----------------------------------------------------------------
---------
                              SNMP USERS
-----------------------------------------------------------------
---------

User              Auth            Priv(enforce)   Groups
acl_filter
----------------- --------------- --------------- ---------------
-----------
admin             md5             des(no)         network-admin
SNMPv3User        md5             aes-128(no)     network-operator

-----------------------------------------------------------------
---------
     NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
-----------------------------------------------------------------
---------

User              Auth                Priv
----------------- ------------------ ------------

(sw1)(Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                   Device Name: sw1
                                    IP Address: 10.231.80.212
                                  SNMP Version: SNMPv2c
                                 Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: cshm1!
                                  Model Number: N9K-C9336C-FX2
                                Switch Network: cluster-network
                             Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                     Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                     Device Name: sw1
                                      IP Address: 10.231.80.212
                                    SNMP Version: SNMPv3
                                   Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: SNMPv3User
                                    Model Number: N9K-C9336C-FX2
                                  Switch Network: cluster-network
                               Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                       Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                     RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
```

NVIDIA – CL 5.4.0

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.4.0:

- Für **keine Authentifizierung**:

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Für * MD5/SHA-Authentifizierung*:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     4318
Version 1 and 2c Community String  Configured
Version 3 Usernames                Not Configured
---------------------------------  ----------------
cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf        2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf   2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
 # Auto-generated config file: do not edit. #
 agentaddress udp:@mgmt:161
 agentxperms 777 777 snmp snmp
 agentxsocket /var/agentx/master
 createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
 ifmib_max_num_ifaces 500
 iquerysecname _snmptrapusernameX
 master agentx
 monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
```

```
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
 pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
 pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! default


net add/del commands since the last "net commit"

User        Timestamp                   Command
----------  --------------------------
-----------------------------------------------------------------------
-----
SNMPv3User  2020-08-11 00:13:51.826987  net add snmp-server username
SNMPv3User auth-md5 <password> encrypt-aes <password>

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     24253
Version 1 and 2c Community String  Configured
Version 3 Usernames                Configured     <---- Configured
here
---------------------------------  ----------------
cumulus@sw1:~$
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                     Device Name: sw1
(b8:59:9f:09:7c:22)
                                      IP Address: 10.231.80.212
                                    SNMP Version: SNMPv2c
                                   Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                    Model Number: MSN2100-CB2FC
                                  Switch Network: cluster-network
                               Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                      Reason For Not Monitoring: None
                       Source Of Switch Version: LLDP
                                  Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                     RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                  RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

NVIDIA – CL 5.11.0

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.11.0:

- Für **keine Authentifizierung**:

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Für * MD5/SHA-Authentifizierung*:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

   ```
   nv show system snmp-server
   ```

   ```
   cumulus@sw1:~$ nv show system snmp-server
                         applied
   --------------------  ----------------------------------------
   [username]            SNMPv3_USER
   [username]            limiteduser1
   [username]            testuserauth
   [username]            testuserauthaes
   [username]            testusernoauth
   trap-link-up
     check-frequency     60
   trap-link-down
     check-frequency     60
   [listening-address]   all
   [readonly-community]  $nvsec$94d69b56e921aec1790844eb53e772bf
   state                 enabled
   cumulus@sw1:~$
   ```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

   ```
   security login create -user-or-group-name SNMPv3User -application
   snmp -authentication-method usm -remote-switch-ipaddress
   10.231.80.212
   ```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                     Device Name: sw1
(b8:59:9f:09:7c:22)
                                      IP Address: 10.231.80.212
                                    SNMP Version: SNMPv2c
                                   Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                    Model Number: MSN2100-CB2FC
                                  Switch Network: cluster-network
                                Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                      Reason For Not Monitoring: None
                       Source Of Switch Version: LLDP
                                  Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                     RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                               Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                  RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Konfigurieren der Protokollsammlung auf einem MetroCluster-IP-Switch

In einer MetroCluster-IP-Konfiguration können Sie die Protokollsammlung so konfigurieren, dass Switch-Protokolle zu Debugzwecken gesammelt werden.

> Auf Broadcom- und Cisco-Switches ist für jeden Cluster mit Protokollsammlung ein neuer Benutzer erforderlich. Beispielsweise erfordern MetroCluster 1, MetroCluster 2, MetroCluster 3 und MetroCluster 4 die Konfiguration eines separaten Benutzers auf den Switches. Mehrere SSH-Schlüssel für denselben Benutzer werden nicht unterstützt.

Über diese Aufgabe

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung der Erfassung, der Anforderung detaillierter **Support** Protokolle und der Aktivierung einer stündlichen Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

HINWEIS: Wenn Sie den FIPS-Modus aktivieren, müssen Sie Folgendes ausführen:

1. Generieren Sie SSH-Schlüssel auf dem Switch mithilfe der Herstelleranweisungen neu.
2. Regenerieren Sie SSH-Schlüssel in ONTAP mit `debug system regenerate-systemshell-key-pair`
3. Führen Sie die Setup-Routine für die Protokollsammlung mit dem `system switch ethernet log setup-password` Befehl erneut aus

Bevor Sie beginnen

- Der Benutzer muss Zugriff auf die Switch-Befehle haben `show` . Wenn diese nicht verfügbar sind, erstellen Sie einen neuen Benutzer und erteilen Sie dem Benutzer die erforderlichen Berechtigungen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass `Is Monitored:` Feld ist in der Ausgabe des `system switch ethernet show` Befehl.
- Für die Protokollerfassung mit Broadcom- und Cisco-Switches:
  - Der lokale Benutzer muss über Netzwerkadministratorrechte verfügen.
  - Für jedes Cluster-Setup sollte auf dem Switch ein neuer Benutzer erstellt werden, bei dem die Protokollerfassung aktiviert ist. Diese Switches unterstützen nicht mehrere SSH-Schlüssel für denselben Benutzer. Bei jeder weiteren Einrichtung der Protokollerfassung werden alle bereits vorhandenen SSH-Schlüssel für den Benutzer überschrieben.
- Für die Unterstützung der Log-Erfassung mit NVIDIA-Switches muss der *user* für die Log-Sammlung berechtigt sein `cl-support`, den Befehl auszuführen, ohne ein Passwort angeben zu müssen. Führen Sie den folgenden Befehl aus, um diese Verwendung zuzulassen:

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee
-a' visudo -f /etc/sudoers.d/cumulus
```

Schritte

ONTAP 9.15.1 und höher

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie bei der Benutzerspezifikationsabfrage mit **y** antworten, stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, wie in Bevor Sie beginnen .

   ```
   system switch ethernet log setup-password
   ```

   ```
   cluster1::*> system switch ethernet log setup-password
   Enter the switch name: <return>
   The switch name entered is not recognized.
   Choose from the following list:
   cs1
   cs2

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs1
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs2

   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>
   ```

   Erstellen Sie für CL 5.11.1 den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie für die Protokollerfassung einen anderen Benutzer als den Administrator angeben? {y|n}: **y**

1. [[Schritt 2]]Aktivieren Sie die regelmäßige Protokollerfassung:

```
system switch ethernet log modify -device <switch-name> -periodic
-enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs1: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs2: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       true        scheduled
never-run
cs2                                       true        scheduled
never-run
2 entries were displayed.
```

2. Support-Protokoll anfordern:

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1

cs1: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> system switch ethernet log collect-support-log -device
cs2

cs2: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> *system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       false       halted
initiated
cs2                                       true        scheduled
initiated
2 entries were displayed.
```

3. Um alle Details der Protokollsammlung anzuzeigen, einschließlich der Aktivierung, Statusmeldung, des vorherigen Zeitstempels und des Dateinamens der periodischen Erfassung, des Anforderungsstatus, der Statusmeldung und des vorherigen Zeitstempels und des Dateinamens der Support-Sammlung, verwenden Sie Folgendes:

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

                    Switch Name: cs1
           Periodic Log Enabled: true
            Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
    Last Periodic Log Timestamp: 3/11/2024 11:02:59
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:14:20
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

                    Switch Name: cs2
           Periodic Log Enabled: false
            Periodic Log Status: Periodic collection has been
halted.
    Last Periodic Log Timestamp: 3/11/2024 11:05:18
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:18:54
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

ONTAP 9.14.1 und frühere Versionen

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie auf die Eingabeaufforderung der Benutzerspezifikation antworten `y`, stellen Sie sicher, dass der Benutzer die erforderlichen Berechtigungen hatBevor Sie beginnen, wie in beschrieben.

   ```
   system switch ethernet log setup-password
   ```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

> Erstellen Sie für CL 5.11.1 den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie für die Protokollerfassung einen anderen Benutzer als den Administrator angeben? {y|n}: **y**

1. [[Schritt 2]] Um die Erfassung des Support-Protokolls anzufordern und die regelmäßige Erfassung zu aktivieren, führen Sie den folgenden Befehl aus. Damit werden beide Arten der Protokollerfassung gestartet: Die detaillierten `Support` Protokolle und eine stündliche Datenerfassung `Periodic` .

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Wenn Fehlerzustände durch die Log-Collection-Funktion (sichtbar in der Ausgabe von) gemeldet werden `system switch ethernet log show`, siehe "Fehlerbehebung bei der Protokollerfassung" für weitere Details.

Verwalten Sie die Überwachung von Ethernet-Switches in einer MetroCluster-IP-Konfiguration

In den meisten Fällen werden Ethernet-Switches automatisch von ONTAP erkannt und von CSHM überwacht. Die auf den Switch angewendete Referenzkonfigurationsdatei (RCF) aktiviert unter anderem das Cisco Discovery Protocol (CDP) und/oder das Link Layer Discovery Protocol (LLDP). Möglicherweise müssen Sie jedoch manuell einen Switch hinzufügen, der nicht erkannt wird, oder einen Switch entfernen, der nicht mehr verwendet wird. Sie können die aktive Überwachung auch beenden, während Sie den Switch in der Konfiguration beibehalten, z. B. während der Wartung.

Erstellen Sie einen Switch-Eintrag, damit ONTAP ihn überwachen kann

Über diese Aufgabe

Verwenden Sie den `system switch ethernet create` Befehl, um die Überwachung für einen bestimmten Ethernet-Switch manuell zu konfigurieren und zu aktivieren. Dies ist hilfreich, wenn ONTAP den Switch nicht automatisch hinzufügt, oder wenn Sie den Switch zuvor entfernt haben und ihn erneut hinzufügen möchten.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type
cluster-network
```

Ein typisches Beispiel ist das Hinzufügen eines Switches namens [DeviceName] mit der IP-Adresse 1.2.3.4 und SNMPv2c-Anmeldeinformationen auf **cshm1!**. Verwenden Sie `-type storage-network` statt `-type cluster-network`, wenn Sie einen Speicherschalter konfigurieren.

Deaktivieren Sie die Überwachung, ohne den Switch zu löschen

Wenn Sie die Überwachung für einen bestimmten Switch anhalten oder beenden möchten, ihn aber für eine zukünftige Überwachung beibehalten möchten, ändern Sie dessen Parameter, `is-monitoring-enabled-admim` anstatt ihn zu löschen.

Beispiel:

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Auf diese Weise können Sie die Switch-Details und -Konfiguration beibehalten, ohne neue Warnmeldungen oder erneute Ermittlungen zu erzeugen.

Entfernen Sie einen Schalter, den Sie nicht mehr benötigen

Verwenden Sie diese Option `system switch ethernet delete`, um einen Switch zu löschen, der getrennt wurde oder nicht mehr benötigt wird:

```
system switch ethernet delete -device DeviceName
```

Standardmäßig ist dieser Befehl nur erfolgreich, wenn ONTAP den Switch derzeit nicht über CDP oder LLDP erkennt. Um einen erkannten Switch zu entfernen, verwenden Sie den `-force` Parameter:

```
system switch ethernet delete -device DeviceName -force
```

Wenn `-force` verwendet wird, wird der Switch möglicherweise automatisch wieder hinzugefügt, wenn ONTAP ihn erneut erkennt.

Überprüfen der Ethernet-Switch-Überwachung in einer MetroCluster-IP-Konfiguration

Die Ethernet-Switch-Systemzustandsüberwachung (CSHM) versucht automatisch, die erkannten Switches zu überwachen. Wenn die Switches jedoch nicht richtig konfiguriert sind, erfolgt die Überwachung möglicherweise nicht automatisch. Sie sollten überprüfen, ob die Systemzustandsüberwachung ordnungsgemäß für das Monitoring Ihrer Switches konfiguriert ist.

Überwachung der angeschlossenen Ethernet-Switches bestätigen

Über diese Aufgabe

Um zu überprüfen, ob die angeschlossenen Ethernet-Switches überwacht werden, führen Sie Folgendes aus:

```
system switch ethernet show
```

Wenn in der `Model` Spalte **OTHER** angezeigt wird oder im `IS Monitored` Feld **false** angezeigt wird, kann ONTAP den Switch nicht überwachen. Ein Wert von **ANDERE** zeigt in der Regel an, dass ONTAP diesen Switch für die Integritätsüberwachung nicht unterstützt.

Das `IS Monitored` Feld wird aus dem im Feld angegebenen Grund auf **false** gesetzt `Reason`.

> Wenn ein Switch in der Befehlsausgabe nicht aufgeführt ist, hat ONTAP ihn wahrscheinlich nicht erkannt. Vergewissern Sie sich, dass der Switch ordnungsgemäß verkabelt ist. Bei Bedarf können Sie den Schalter manuell hinzufügen. Weitere Informationen finden Sie unter "Verwalten Sie die Überwachung von Ethernet-Switches" .

Vergewissern Sie sich, dass die Firmware- und RCF-Versionen auf dem neuesten Stand sind

Stellen Sie sicher, dass auf dem Switch die neueste unterstützte Firmware ausgeführt wird und dass eine kompatible Referenzkonfigurationsdatei (RCF) angewendet wurde. Weitere Informationen finden Sie auf der "NetApp Support Downloads Seite".

Standardmäßig verwendet der Gesundheitsmonitor SNMPv2c mit der Community-Zeichenfolge **cshm1!** für die Überwachung, aber SNMPv3 kann auch konfiguriert werden.

Wenn Sie die Standard-SNMPv2c-Community-Zeichenfolge ändern müssen, stellen Sie sicher, dass die gewünschte SNMPv2c-Community-Zeichenfolge auf dem Switch konfiguriert wurde.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c
-community-or-username newCommunity!
```

> Weitere Informationen zur Konfiguration von SNMPv3 für die Verwendung finden Sie unter"Optional: SNMPv3 konfigurieren".

Bestätigen Sie die Verbindung zum Managementnetzwerk

Vergewissern Sie sich, dass der Managementport des Switch mit dem Managementnetzwerk verbunden ist.

Für die Ausführung von SNMP-Abfragen und Protokollerfassung ist eine korrekte Management-Port-Verbindung für ONTAP erforderlich.

Verwandte Informationen

- "Fehlerbehebung bei Warnmeldungen"

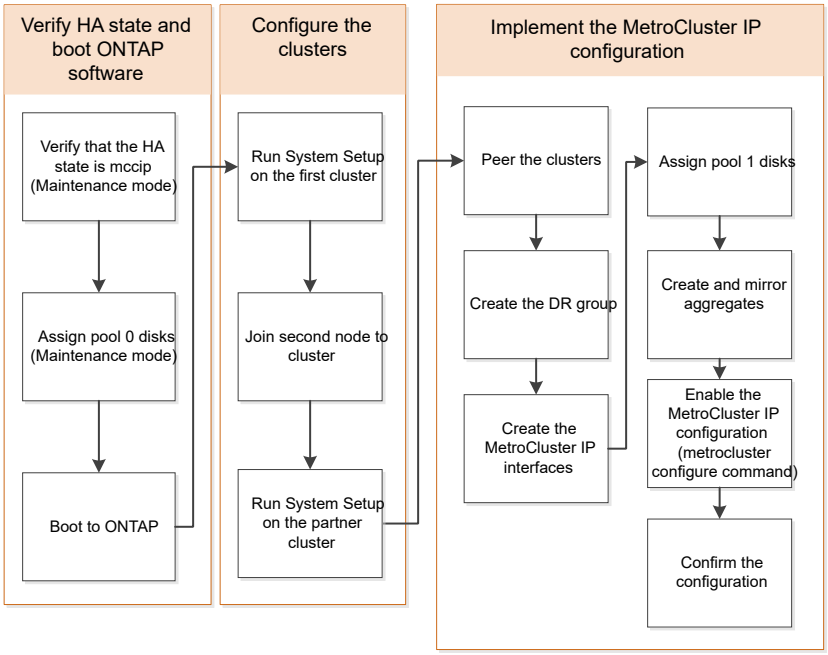
Konfigurieren Sie die MetroCluster Software in ONTAP

Konfigurieren Sie die MetroCluster-Software mithilfe der CLI

Einrichten der ONTAP Knoten und -Cluster in der MetroCluster -IP-Konfiguration

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.

Wenn ein Controller-Modul während der Konfiguration ausfällt, lesen Sie "Ausfallszenarien für Controller-Module während der MetroCluster-Installation".



Konfigurieren Sie MetroCluster IP-Konfigurationen mit acht Knoten

Eine MetroCluster Konfiguration mit acht Nodes besteht aus zwei DR-Gruppen. Um die erste DR-Gruppe zu konfigurieren, führen Sie die Aufgaben in diesem Abschnitt aus. Nachdem Sie die erste DR-Gruppe konfiguriert haben, können Sie die folgenden Schritte ausführen: "Erweitern Sie eine MetroCluster IP-Konfiguration mit vier Knoten auf eine Konfiguration mit acht Knoten" .

Sammeln Sie die erforderlichen Informationen für Ihre MetroCluster -IP-Konfiguration

Sie müssen die erforderlichen IP-Adressen für die Controller-Module erfassen, bevor Sie mit dem Konfigurationsprozess beginnen.

Über diese Links können Sie CSV-Dateien herunterladen und die Tabellen mit Ihren standortspezifischen Informationen ausfüllen.

"MetroCluster IP-Setup-Arbeitsblatt, Site_A"

"MetroCluster IP-Setup-Arbeitsblatt, Site_B"

Vergleichen Sie ONTAP Standardcluster- 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	Nicht zutreffend	Erforderlich

Überprüfen Sie den HA-Konfigurationsstatus Ihrer Controller- und Chassis-Komponenten in einer MetroCluster -IP-Konfiguration

In einer MetroCluster IP-Konfiguration müssen Sie überprüfen, ob der ha-Konfigurationsstatus der Controller- und Chassis-Komponenten auf „`mccip`“ eingestellt ist, damit sie ordnungsgemäß booten. Obwohl dieser Wert auf werkseitig empfangene Systeme vorkonfiguriert sein sollte, sollten Sie die Einstellung dennoch überprüfen, bevor Sie fortfahren.

Wenn der HA-Status des Controller-Moduls und des Chassis falsch ist, können Sie die MetroCluster nicht konfigurieren, ohne den Node neu zu initialisieren. Sie müssen die Einstellung mit diesem Verfahren korrigieren und dann das System mit einem der folgenden Verfahren initialisieren:

- Führen Sie in einer MetroCluster IP-Konfiguration die Schritte in "Systemstandardwerte auf einem Controller-Modul wiederherstellen"aus.
- Führen Sie in einer MetroCluster FC-Konfiguration die Schritte in "Stellen Sie die Systemstandardeinstellungen wieder her und konfigurieren Sie den HBA-Typ auf einem Controller-Modul"aus.

Bevor Sie beginnen

Vergewissern Sie sich, dass sich das System im Wartungsmodus befindet.

Schritte

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

   ```
   ha-config show
   ```

   Der richtige HA-Status hängt von Ihrer MetroCluster-Konfiguration ab.

MetroCluster-Konfigurationstyp	HA-Status für alle Komponenten…
MetroCluster FC-Konfiguration mit acht oder vier Nodes	mcc
MetroCluster FC-Konfiguration mit zwei Nodes	mcc-2n
MetroCluster IP-Konfiguration mit acht oder vier Nodes	Mccip

2. Wenn der angezeigte Systemstatus des Controllers nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Controller-Modul fest:

MetroCluster-Konfigurationstyp	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify controller mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mccip`

3. Wenn der angezeigte Systemstatus des Chassis nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Chassis fest:

MetroCluster-Konfigurationstyp	Befehl

MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify chassis mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mccip`

4. Booten des Node zu ONTAP:

   ```
   boot_ontap
   ```

5. Wiederholen Sie dieses gesamte Verfahren, um den HA-Status auf jedem Node in der MetroCluster-Konfiguration zu überprüfen.

Stellen Sie die Systemstandards auf einem Controllermodul wieder her, bevor Sie eine MetroCluster IP-Konfiguration einrichten

Setzen Sie die Standardeinstellungen der Controller-Module zurück und stellen Sie sie wieder her.

1. Geben Sie an der LOADER-Eingabeaufforderung Umgebungsvariablen auf ihre Standardeinstellung zurück: `set-defaults`
2. Starten Sie den Knoten im Startmenü: `boot_ontap menu`

   Warten Sie, bis das Startmenü angezeigt wird, nachdem Sie diesen Befehl ausgeführt haben.

3. Löschen Sie die Node-Konfiguration:

   - Wenn Sie Systeme verwenden, die für ADP konfiguriert sind, wählen Sie Option `9a` Über das Startmenü und antworten `no` Wenn Sie dazu aufgefordert werden.

     Dieser Prozess ist störend.

     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.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a
...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

- Wenn Ihr System nicht für ADP konfiguriert ist, geben Sie ein `wipeconfig` Drücken Sie an der Eingabeaufforderung des Startmenüs die Eingabetaste.

  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.
```

Manuelles Zuweisen von Laufwerken zu Pool 0 in einer MetroCluster -IP-Konfiguration

Wenn Sie die werkseitig konfigurierten Systeme nicht empfangen haben, müssen Sie die Pool-0-Laufwerke möglicherweise manuell zuweisen. Je nach Plattformmodell und ob das System ADP nutzt, müssen Sie für jeden Knoten der MetroCluster-IP-Konfiguration Laufwerke manuell dem Pool 0 zuweisen. Das von Ihnen verwendete Verfahren hängt von der Version von ONTAP ab.

Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.4 und höher)

Wenn das System werkseitig nicht konfiguriert wurde und die Anforderungen für die automatische Laufwerkszuweisung nicht erfüllt, müssen Sie die Pool-0-Laufwerke manuell zuweisen.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.4 oder höher.

Um festzustellen, ob Ihr System eine manuelle Festplattenzuweisung benötigt, sollten Sie prüfen "Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher".

Sie führen diese Schritte im Wartungsmodus aus. Der Vorgang muss an jedem Knoten der Konfiguration durchgeführt werden.

Die Beispiele in diesem Abschnitt basieren auf folgenden Annahmen:

- Node_A_1 und Node_A_2 eigene Laufwerke auf:
  - Standort_A-Shelf_1 (lokal)
  - Standort_B-Shelf_2 (Remote)
- Eigene Laufwerke Node_B_1 und Node_B_2 auf:

- Standort_B-Shelf_1 (lokal)
- Standort_A-Shelf_2 (Remote)

Schritte

1. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

2. Wählen Sie Option 9a, und antworten `no` Wenn Sie dazu aufgefordert werden.

   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.
   (10) Set Onboard Key Manager recovery secrets.
   (11) Configure node for external key management.
   Selection (1-11)? 9a

   ...

   ########## WARNING: AGGREGATES WILL BE DESTROYED ##########
   This is a disruptive operation that applies to all the disks
   that are attached and visible to this node.

   Before proceeding further, make sure that:

   The aggregates visible from this node do not contain
   data that needs to be preserved.
   This option (9a) has been executed or will be executed
   on the HA partner node (and DR/DR-AUX partner nodes if
   applicable), prior to reinitializing any system in the
   HA-pair or MetroCluster configuration.
   The HA partner node (and DR/DR-AUX partner nodes if
   applicable) is currently waiting at the boot menu.
   Do you want to abort this operation (yes/no)? no
   ```

3. Wenn der Knoten neu gestartet wird, drücken Sie bei Aufforderung Strg-C, um das Startmenü anzuzeigen, und wählen Sie dann die Option für **Wartungsmodus Boot** aus.

4. Weisen Sie im Wartungsmodus den lokalen Aggregaten auf dem Node manuell Laufwerke zu:

   ```
   disk assign disk-id -p 0 -s local-node-sysid
   ```

   Die Laufwerke sollten symmetrisch zugeordnet werden, sodass jeder Knoten eine gleiche Anzahl von Laufwerken hat. Nachfolgend finden Sie eine Konfiguration mit zwei Storage-Shelfs an jedem Standort.

   a. Bei der Konfiguration von Node_A_1 weisen Sie Laufwerke von Steckplatz 0 bis 11 manuell dem Pool0 des Node A1 von Site_A-Shelf_1 zu.
   b. Bei der Konfiguration von Node_A_2 weisen Sie die Laufwerke von Steckplatz 12 bis 23 manuell dem Pool0 des Node A2 von Site_A-Shelf_1 zu.
   c. Beim Konfigurieren von Node_B_1 weisen Sie Laufwerke von Steckplatz 0 bis 11 manuell dem Pool0 des Node B1 von Site_B-Shelf_1 zu.
   d. Beim Konfigurieren von Node_B_2 weisen Sie Laufwerke manuell zwischen Steckplatz 12 und 23 dem Pool0 des Node B2 von Site_B-Shelf_1 zu.
5. Beenden des Wartungsmodus:

   ```
   halt
   ```

6. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

7. Wiederholen Sie diese Schritte auf den anderen Knoten der MetroCluster IP-Konfiguration.
8. Wählen Sie Option **4** aus dem Startmenü auf beiden Knoten und lassen Sie das System booten.
9. Fahren Sie mit fort "Einrichtung von ONTAP".

Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.3)

Wenn für jeden Node mindestens zwei Festplatten-Shelfs vorhanden sind, können Sie die automatische Zuweisung von ONTAP nutzen, um die lokalen (Pool 0) Festplatten automatisch zuzuweisen.

Über diese Aufgabe

Im Wartungsmodus des Node müssen Sie zunächst eine einzelne Festplatte in den entsprechenden Shelfs Pool 0 zuweisen. ONTAP weist dann automatisch den Rest der Festplatten im Shelf demselben Pool zu. Diese Aufgabe ist nicht erforderlich für Systeme, die vom Werk empfangen werden, die über Pool 0 verfügen, um das vorkonfigurierte Root-Aggregat zu enthalten.

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.3.

Dieser Vorgang ist nicht erforderlich, wenn Sie Ihre MetroCluster-Konfiguration vom Werk erhalten haben. Die Nodes aus dem Werk werden mit Pool 0-Festplatten und Root-Aggregaten konfiguriert.

Dieses Verfahren kann nur angewandt werden, wenn mindestens zwei Festplatten-Shelfs für jeden Node vorhanden sind, sodass die automatische Zuweisung von Festplatten auf Shelf-Ebene möglich ist. Wenn Sie die automatische Zuweisung auf Shelf-Ebene nicht verwenden können, müssen Sie die lokalen Festplatten manuell zuweisen, damit jeder Node über einen lokalen Festplatten-Pool (Pool 0) verfügt.

Diese Schritte müssen im Wartungsmodus ausgeführt werden.

Beispiele in diesem Abschnitt setzen die folgenden Platten-Shelves voraus:

- Node_A_1 besitzt Festplatten auf:
  - Standort_A-Shelf_1 (lokal)
  - Standort_B-Shelf_2 (Remote)
- Node_A_2 ist verbunden mit:
  - Standort_A-Shelf_3 (lokal)
  - Standort_B-Shelf_4 (Remote)
- Node_B_1 ist verbunden mit:
  - Standort_B-Shelf_1 (lokal)
  - Standort_A-Shelf_2 (Remote)
- Node_B_2 ist verbunden mit:
  - Standort_B-Shelf_3 (lokal)
  - Standort_A-Shelf_4 (Remote)

Schritte

1. Weisen Sie auf jedem Knoten manuell eine einzelne Festplatte für das Root-Aggregat zu:

   `disk assign disk-id -p 0 -s local-node-sysid`

   Durch die manuelle Zuweisung dieser Festplatten kann die Funktion für die automatische Zuweisung von ONTAP den Rest der Festplatten auf jedem Shelf zuweisen.

   a. Weisen Sie auf Node_A_1 manuell einer Festplatte aus dem lokalen Standort_A-Shelf_1 dem Pool 0 zu.
   b. Weisen Sie auf Node_A_2 manuell einer Festplatte aus dem lokalen Site_A-Shelf_3 dem Pool 0 zu.
   c. Weisen Sie auf Node_B_1 manuell eine Festplatte vom lokalen Standort_B-Shelf_1 dem Pool 0 zu.
   d. Weisen Sie auf Node_B_2 dem Pool 0 manuell eine Festplatte von Local Site_B-Shelf_3 zu.
2. Starten Sie jeden Knoten an Standort A mit Option 4 im Startmenü:

   Sie sollten diesen Schritt auf einem Node abschließen, bevor Sie mit dem nächsten Node fortfahren.

   a. Beenden des Wartungsmodus:

      ```
      halt
      ```

   b. Anzeigen des Startmenüs:

      ```
      boot_ontap menu
      ```

   c. Wählen Sie im Startmenü Option 4, und fahren Sie fort.
3. Starten Sie jeden Knoten an Standort B mit Option 4 im Startmenü:

   Sie sollten diesen Schritt auf einem Node abschließen, bevor Sie mit dem nächsten Node fortfahren.

   a. Beenden des Wartungsmodus:

      ```
      halt
      ```

b. Anzeigen des Startmenüs:

```
boot_ontap menu
```

c. Wählen Sie im Startmenü Option 4, und fahren Sie fort.

Einrichten von ONTAP -Knoten in einer MetroCluster -IP-Konfiguration

Nachdem Sie jeden Node gebootet haben, werden Sie aufgefordert, eine grundlegende Node- und Cluster-Konfiguration durchzuführen. Nach dem Konfigurieren des Clusters kehren Sie zur ONTAP-CLI zurück, um Aggregate zu erstellen und die MetroCluster-Konfiguration zu erstellen.

Bevor Sie beginnen

- Sie müssen die MetroCluster-Konfiguration verkabelt haben.

Wenn Sie die neuen Controller mit einem Netboot booten müssen, siehe "Booten Sie die neuen Controller-Module ein".

Über diese Aufgabe

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

Schritte

1. Schalten Sie jeden Node am lokalen Standort ein, wenn dies noch nicht geschehen ist, und lassen Sie ihn alle vollständig booten.

   Wenn sich das System im Wartungsmodus befindet, müssen Sie den Stopp-Befehl eingeben, um den Wartungsmodus zu beenden, und geben Sie dann den aus `boot_ontap` Befehl zum Booten des Systems und Abrufen des Cluster-Setups.

2. Fahren Sie auf dem ersten Node in jedem Cluster mit den Aufforderungen zum Konfigurieren des Clusters fort.

   a. Aktivieren Sie das AutoSupport-Tool, indem Sie den vom System bereitgestellten Anweisungen folgen.

      Die Ausgabe sollte wie folgt aussehen:

```
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
.
.
.
```

b. Konfigurieren Sie die Node-Managementoberfläche, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Erstellen Sie das Cluster, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

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


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

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Fügen Sie Lizenzen hinzu, richten Sie eine SVM für die Cluster-Administration ein, und geben Sie DNS-Informationen ein, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Aktivieren Sie das Speicherausfallschutz, und richten Sie den Knoten ein, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Die Konfiguration des Node abschließen, jedoch keine Datenaggregate erstellen.

   Sie können ONTAP System Manager verwenden und im Webbrowser die Cluster-Management-IP-Adresse (https://172.17.12.153).) aufrufen

   "Cluster-Management mithilfe von System Manager (ONTAP 9.7 und früher)"

   "ONTAP System Manager (Version 9.7 und höher)"

g. Konfigurieren Sie den Service-Prozessor (SP):

   "Konfigurieren Sie das SP/BMC-Netzwerk"

"Verwenden Sie einen Service Processor mit System Manager - ONTAP 9.7 und früher"

3. Booten Sie den nächsten Controller, und verbinden Sie ihn mit den Aufforderungen zum Cluster.
4. Sicherstellen, dass die Nodes im Hochverfügbarkeits-Modus konfiguriert sind:

   ```
   storage failover show -fields mode
   ```

   Wenn dies nicht der Fall ist, müssen Sie auf jedem Node den HA-Modus konfigurieren und dann die Nodes neu booten:

   ```
   storage failover modify -mode ha -node localhost
   ```

   Der erwartete Konfigurationsstatus von HA und Storage-Failover lautet wie folgt:

   - DER HA-Modus ist konfiguriert, ein Storage-Failover ist jedoch nicht aktiviert.
   - DIE HA-Übernahmemfunktion ist deaktiviert.
   - HA-Schnittstellen sind offline.
   - SPÄTER werden HA-Modus, Storage Failover und Schnittstellen konfiguriert.

5. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

   ```
   network port show
   ```

Die MetroCluster-IP-Schnittstellen sind derzeit nicht konfiguriert und werden nicht in der Befehlsausgabe angezeigt.

Im folgenden Beispiel werden zwei Cluster-Ports auf Node_A_1 angezeigt:

```
cluster_A::*> network port show -role cluster



Node: node_A_1


Ignore

                                                     Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                     Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false
```

```
e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Wiederholen Sie diese Schritte auf dem Partner-Cluster.

Nächste Schritte

Kehren Sie zur ONTAP-Befehlszeilenschnittstelle zurück und führen Sie die MetroCluster-Konfiguration durch. Führen Sie dazu die folgenden Aufgaben aus.

Konfigurieren Sie ONTAP -Cluster in einer MetroCluster -IP-Konfiguration

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

Über diese Aufgabe

Bevor Sie ausführen `metrocluster configure`, HA-Modus und DR-Spiegelung sind nicht aktiviert und Sie können eine Fehlermeldung in Bezug auf dieses erwartete Verhalten sehen. Sie aktivieren später den HA-Modus und die DR-Spiegelung, wenn Sie den Befehl ausführen `metrocluster configure` Um die Konfiguration zu implementieren.

Deaktivieren der automatischen Laufwerkszuweisung (bei manueller Zuweisung in ONTAP 9.4)

Wenn in ONTAP 9.4 Ihre MetroCluster IP-Konfiguration weniger als vier externe Storage-Shelfs pro Standort umfasst, müssen Sie die automatische Laufwerkszuweisung auf allen Nodes deaktivieren und Laufwerke manuell zuweisen.

Über diese Aufgabe

In ONTAP 9.5 und höher ist diese Aufgabe nicht erforderlich.

Diese Aufgabe gilt nicht für ein AFF A800 System mit einem internen Shelf und ohne externen Shelfs.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Automatische Laufwerkszuweisung deaktivieren:

   ```
   storage disk option modify -node <node_name> -autoassign off
   ```

2. Sie müssen diesen Befehl für alle Knoten in der MetroCluster IP Konfiguration ausgeben.

Überprüfen der Laufwerkszuweisung von Pool 0-Laufwerken

Sie müssen überprüfen, ob die Remote-Laufwerke für die Knoten sichtbar sind und ordnungsgemäß zugewiesen wurden.

Über diese Aufgabe

Die automatische Zuweisung ist abhängig vom Plattformmodell für Storage-Systeme und der Anordnung der

Festplatten-Shelfs.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Vergewissern Sie sich, dass Pool-0-Laufwerke automatisch zugewiesen werden:

   ```
   disk show
   ```

   Das folgende Beispiel zeigt die Ausgabe „Cluster_A“ für ein AFF A800 System ohne externe Shelfs.

   Ein Viertel (8 Laufwerke) wurde automatisch „Node_A_1“ zugewiesen und ein Quartal wurde automatisch „Node_A_2“ zugewiesen. Die übrigen Laufwerke sind Remote-Laufwerke (Pool 1) für „Node_B_1“ und „Node_B_2“.

   ```
   cluster_A::*> disk show
                   Usable     Disk      Container           Container
   Disk            Size       Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
   ```

```
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Im folgenden Beispiel wird die Ausgabe „Cluster_B“ angezeigt:

```
cluster_B::> disk show
                 Usable     Disk              Container   Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
```

```
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_B_2
node_B_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_B_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_B_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_B_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_B_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_B_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_B_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_B_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_B_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_B_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_B_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_B_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_B_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_B_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_B_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_B_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.

cluster_B::>
```

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 für Cluster-Peering

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.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01-01_clus1   e0a       e0a
   Cluster cluster01-01_clus2   e0b       e0b
   Cluster cluster01-02_clus1   e0a       e0a
   Cluster cluster01-02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

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

   ```
   network interface failover-groups create -vserver <system_svm> -failover-group
   <failover_group> -targets <physical_or_logical_ports>
   ```

   Im folgenden Beispiel werden die Ports „e0e“ und „e0f“ der Failover-Gruppe „intercluster01“ auf dem System „SVMcluster01“ 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.

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic02“ in 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:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
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:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster -failover
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“, und „cluster01_ic.02“ auf dem „SVMe0e“ Port an den „e0f“-Port scheitern.

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

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:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask>
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask>
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic.02“ 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:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
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:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show –service-policy default-intercluster -failover
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01: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

Mit dem Befehl Cluster Peer create können Sie eine Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster erstellen. Nachdem die Peer-Beziehung erstellt wurde, können Sie Cluster Peer Creation im Remote-Cluster ausführen, um sie für den lokalen Cluster zu authentifizieren.

Über diese Aufgabe

- 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_ip_addresses> -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 im Quellcluster beim Ziel-Cluster:

   ```
   cluster peer create -peer-addrs <peer_lif_ip_addresses> -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
```

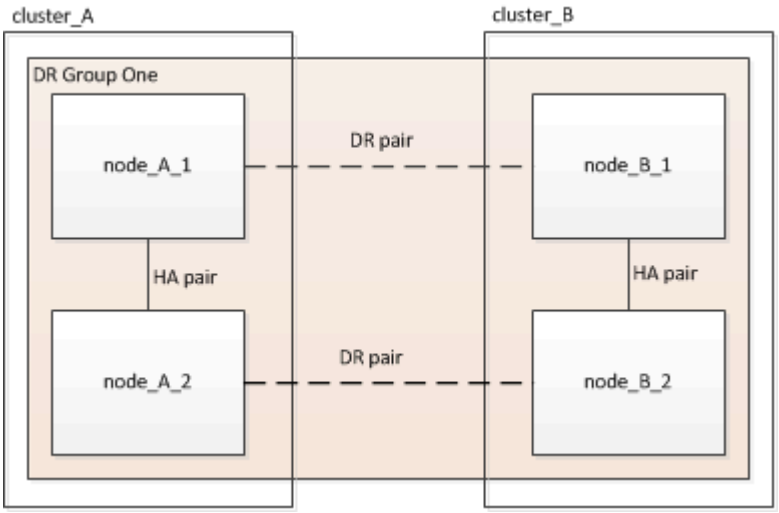
Erstellen der DR-Gruppe

Sie müssen die Disaster-Recovery-Gruppenbeziehungen (DR) zwischen den Clustern erstellen.

Über diese Aufgabe

Sie führen dieses Verfahren auf einem der Cluster in der MetroCluster-Konfiguration durch, um die DR-Beziehungen zwischen den Nodes in beiden Clustern zu erstellen.

> Die DR-Beziehungen können nach Erstellung der DR-Gruppen nicht mehr geändert werden.



Schritte

1. Überprüfen Sie, ob die Nodes bereit für die Erstellung der DR-Gruppe sind, indem Sie auf jedem Node den folgenden Befehl eingeben:

   ```
   metrocluster configuration-settings show-status
   ```

   Die Befehlsausgabe sollte zeigen, dass die Nodes bereit sind:

   ```
   cluster_A::> metrocluster configuration-settings show-status
   Cluster                    Node          Configuration Settings Status
   -------------------------- -------------
   --------------------------------
   cluster_A                  node_A_1      ready for DR group create
                              node_A_2      ready for DR group create
   2 entries were displayed.
   ```

   ```
   cluster_B::> metrocluster configuration-settings show-status
   Cluster                    Node          Configuration Settings Status
   -------------------------- -------------
   --------------------------------
   cluster_B                  node_B_1      ready for DR group create
                              node_B_2      ready for DR group create
   2 entries were displayed.
   ```

2. Erstellen der DR-Gruppe:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

```
<partner_cluster_name> -local-node <local_node_name> -remote-node
<remote_node_name>
```

Dieser Befehl wird nur einmal ausgegeben. Es muss nicht auf dem Partner-Cluster wiederholt werden. Sie geben im Befehl den Namen des Remote-Clusters und den Namen eines lokalen Node und eines Node im Partner-Cluster an.

Die beiden Nodes, die Sie angeben, sind als DR-Partner konfiguriert, und die anderen beiden Nodes (die im Befehl nicht angegeben sind) werden als das zweite DR-Paar in der DR-Gruppe konfiguriert. Diese Beziehungen können nicht geändert werden, wenn Sie diesen Befehl eingeben.

Mit dem folgenden Befehl werden diese DR-Paare erstellt:

- Node_A_1 und Node_B_1
- Node_A_2 und Node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Konfigurieren und Anschließen der MetroCluster IP-Schnittstellen

Sie müssen die MetroCluster IP-Schnittstellen konfigurieren, die zur Replizierung von Storage und nicht-flüchtigem Cache jedes Nodes verwendet werden. Anschließend stellen Sie die Verbindungen mithilfe der MetroCluster-IP-Schnittstellen bereit. Dadurch werden iSCSI-Verbindungen für die Speicherreplikation erstellt.

> Die MetroCluster-IP-Adresse und die verbundenen Switch-Ports werden erst online geschaltet, nachdem Sie die MetroCluster-IP-Schnittstellen erstellt haben.

Über diese Aufgabe

- Sie müssen für jeden Node zwei Schnittstellen erstellen. Die Schnittstellen müssen mit den in der MetroCluster RCF-Datei definierten VLANs verknüpft sein.
- Sie müssen alle MetroCluster IP Schnittstelle „A“-Ports in demselben VLAN und alle MetroCluster IP Schnittstelle „B“-Ports in dem anderen VLAN erstellen. Siehe "Überlegungen zur MetroCluster IP-Konfiguration".
- Ab ONTAP 9.9 müssen Sie auch die angeben, wenn Sie eine Layer 3-Konfiguration verwenden `-gateway` Parameter beim Erstellen von MetroCluster-IP-Schnittstellen. Siehe "Überlegungen für Layer 3-Weitbereichs-Netzwerke".

  Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

  Falls unterstützt, können Sie auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben. Verwenden Sie dazu den `-vlan-id` Parameter im `metrocluster configuration-settings interface create` Befehl.

  Die folgenden Plattformen unterstützen **Not** den `-vlan-id` Parameter:

  - FAS8200 UND AFF A300
  - AFF A320

- FAS9000 und AFF A700
- AFF C800, ASA C800, AFF A800 und ASA A800

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

  Die Standard- und gültigen VLAN-Zuweisungen hängen davon ab, ob die Plattform den folgenden Parameter unterstützt `-vlan-id`:

Plattformen, die <code>-vlan-</code> unterstützen

Standard-VLAN:

- Wenn der `-vlan-id` Parameter nicht angegeben wird, werden die Schnittstellen mit VLAN 10 für die „A“-Ports und VLAN 20 für die „B“-Ports erstellt.
- Das angegebene VLAN muss mit dem im RCF ausgewählten VLAN übereinstimmen.

Gültige VLAN-Bereiche:

- Standard-VLAN 10 und 20
- VLANs 101 und höher (zwischen 101 und 4095)

Plattformen, die <code>-vlan-</code> nicht unterstützen

Standard-VLAN:

- Keine Angabe. Für die Schnittstelle muss kein VLAN auf der MetroCluster-Schnittstelle angegeben werden. Der Switch-Port definiert das verwendete VLAN.

Gültige VLAN-Bereiche:

- Alle VLANs werden beim Generieren der RCF nicht explizit ausgeschlossen. Die RCF warnt Sie, wenn das VLAN ungültig ist.

- Die von den MetroCluster IP-Schnittstellen verwendeten physischen Ports hängen vom Plattformmodell ab. Informationen zur Verwendung des Ports für Ihr System finden Sie unter "MetroCluster IP-Switches verkabeln" .
- Die folgenden IP-Adressen und Subnetze werden in den Beispielen verwendet:

Knoten	Schnittstelle	IP-Adresse	Subnetz
Node_A_1	MetroCluster IP-Schnittstelle 1	10.1.1.1	10.1.1/24
MetroCluster IP-Schnittstelle 2	10.1.2.1	10.1.2/24	Node_A_2
MetroCluster IP-Schnittstelle 1	10.1.1.2	10.1.1/24	MetroCluster IP-Schnittstelle 2

10.1.2.2	10.1.2/24	Knoten_B_1	MetroCluster IP-Schnittstelle 1
10.1.1.3	10.1.1/24	MetroCluster IP-Schnittstelle 2	10.1.2.3
10.1.2/24	Knoten_B_2	MetroCluster IP-Schnittstelle 1	10.1.1.4
10.1.1/24	MetroCluster IP-Schnittstelle 2	10.1.2.4	10.1.2/24

- Bei diesem Verfahren werden folgende Beispiele verwendet:

  Die Ports für ein AFF A700 oder ein FAS9000 System (e5a und e5b).

  Die Ports für ein AFF A220-System, um zu zeigen, wie der Parameter auf einer unterstützten Plattform verwendet `-vlan-id` wird.

  Konfigurieren Sie die Schnittstellen an den richtigen Ports für Ihr Plattformmodell.

Schritte

1. Vergewissern Sie sich, dass die automatische Festplattenzuordnung für jeden Node aktiviert ist:

   ```
   storage disk option show
   ```

   Bei der automatischen Festplattenzuweisung werden Pool 0- und Pool 1-Festplatten auf Shelf-Basis zugewiesen.

   In der Spalte Automatische Zuweisung wird angegeben, ob die automatische Zuweisung der Festplatte aktiviert ist.

   ```
   Node         BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

2. Vergewissern Sie sich, dass Sie auf den Nodes MetroCluster IP-Schnittstellen erstellen können:

   ```
   metrocluster configuration-settings show-status
   ```

   Alle Nodes sollten bereit sein:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for interface create
              node_A_2     ready for interface create
cluster_B
              node_B_1     ready for interface create
              node_B_2     ready for interface create
4 entries were displayed.
```

3. Erstellen Sie die Schnittstellen auf Node_A_1.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_A_1“:

   > Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_A_1" mit IP-Adresse "10.1.1.1":

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
   10.1.1.1 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

   Bei Plattformmodellen, die VLANs für die MetroCluster IP Schnittstelle unterstützen, können Sie die einschließen `-vlan-id` Parameter, wenn Sie die Standard-VLAN-IDs nicht verwenden möchten. Das folgende Beispiel zeigt den Befehl für ein AFF A220 System mit einer VLAN-ID von 120:

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
   10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_A_1“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
   ```

```
-netmask <netmask>
```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle am Port „e5b“ auf „Node_A_1“ mit der IP-Adresse „10.1.2.1“:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

> Sie können überprüfen, ob diese Schnittstellen mit vorhanden sind `metrocluster configuration-settings interface show` Befehl.

4. Erstellen Sie die Schnittstellen auf Node_A_2.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_A_2“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_A_2" mit IP-Adresse "10.1.1.2":

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
   10.1.1.2 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_A_2“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf dem Port „e5b“ auf „Node_A_2“ mit der IP-Adresse „10.1.2.2“:

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
   10.1.2.2 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

Bei Plattformmodellen, die VLANs für die MetroCluster IP Schnittstelle unterstützen, können Sie die einschließen `-vlan-id` Parameter, wenn Sie die Standard-VLAN-IDs nicht verwenden möchten. Das folgende Beispiel zeigt den Befehl für ein AFF A220 System mit einer VLAN-ID von 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Erstellen Sie die Schnittstellen auf „Node_B_1“.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_B_1“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_B_1" mit IP-Adresse "10.1.1.3":

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_B -home-node node_B_1 -home-port e5a -address
   10.1.1.3 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.cluster_B::>
   ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_B_1“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle am Port „e5b“ auf „Node_B_1“ mit der IP-Adresse „10.1.2.3“:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Erstellen Sie die Schnittstellen auf „Node_B_2“.

   a. Konfigurieren Sie die Schnittstelle am Port e5a auf Node_B_2:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
   -netmask <netmask>
   ```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_B_2" mit IP-Adresse "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_B_2“:

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf dem Port „e5b“ auf „Node_B_2“ mit der IP-Adresse „10.1.2.4“:

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Vergewissern Sie sich, dass die Schnittstellen konfiguriert sind:

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

Das folgende Beispiel zeigt, dass der Konfigurationsstatus für jede Schnittstelle abgeschlossen ist.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- ---------
----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Vergewissern Sie sich, dass die Nodes bereit sind, die MetroCluster-Schnittstellen zu verbinden:

   `metrocluster configuration-settings show-status`

   Im folgenden Beispiel werden alle Knoten im Status „bereit für die Verbindung“ angezeigt:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Stellen Sie die Verbindungen her:
   `metrocluster configuration-settings connection connect`

   Wenn Sie eine Version vor ONTAP 9.10.1 ausführen, können die IP-Adressen nach dem Ausführen dieses Befehls nicht geändert werden.

   Im folgenden Beispiel wird gezeigt, dass Cluster_A erfolgreich verbunden ist:

   ```
   cluster_A::> metrocluster configuration-settings connection connect
   [Job 53] Job succeeded: Connect is successful.
   cluster_A::>
   ```

10. Stellen Sie sicher, dass die Verbindungen hergestellt wurden:

    `metrocluster configuration-settings show-status`

    Der Status der Konfigurationseinstellungen für alle Knoten sollte abgeschlossen sein:

    ```
    Cluster       Node         Configuration Settings Status
    ----------    -----------  ---------------------------------
    cluster_A
                  node_A_1     completed
                  node_A_2     completed
    cluster_B
                  node_B_1     completed
                  node_B_2     completed
    4 entries were displayed.
    ```

11. Vergewissern Sie sich, dass die iSCSI-Verbindungen hergestellt sind:

    a. Ändern Sie die erweiterte Berechtigungsebene:

       `set -privilege advanced`

       Sie müssen mit reagieren `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus angezeigt (`*>`).

    b. Anzeigen der Verbindungen:

       `storage iscsi-initiator show`

       Auf Systemen mit ONTAP 9.5 gibt es für jedes Cluster acht MetroCluster-IP-Initiatoren, die in der Ausgabe angezeigt werden sollten.

       Auf Systemen mit ONTAP 9.4 und früheren Versionen gibt es für jedes Cluster vier MetroCluster IP-Initiatoren, die in der Ausgabe angezeigt werden sollten.

       Im folgenden Beispiel werden die acht MetroCluster-IP-Initiatoren auf einem Cluster mit ONTAP 9.5 angezeigt:

```
cluster_A::*> storage iscsi-initiator show
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
-------------------------------- --------

cluster_A-01
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-aux-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-aux-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-aux-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-pri-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-aux-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-b-initiator2
```

```
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
     dr_partner
              mccip-pri-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-pri-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-pri-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-pri-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

a. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

12. Vergewissern Sie sich, dass die Knoten bereit sind für die abschließende Implementierung der MetroCluster Konfiguration:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_A
              node_A_1           ready to configure -     -
              node_A_2           ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_B
              node_B_1          ready to configure -     -
              node_B_2          ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Überprüfen oder manuelles Durchführen der Zuweisung von Pool-1-Laufwerken

Je nach Storage-Konfiguration müssen Sie für jeden Node der MetroCluster IP-Konfiguration entweder die Laufwerkszuweisung Pool 1 überprüfen oder Laufwerken manuell Pool 1 zuweisen. Das von Ihnen verwendete Verfahren hängt von der Version von ONTAP ab.

Konfigurationstyp	Verfahren
Die Systeme erfüllen die Anforderungen für die automatische Laufwerkszuweisung oder wurden bei Verwendung von ONTAP 9.3 vom Werk empfangen.	Überprüfen der Festplattenzuordnung für Pool 1-Festplatten
Die Konfiguration umfasst drei oder, wenn sie mehr als vier Shelfs enthält, besteht aus einem ungleichen Vielfaches von vier Shelfs (z. B. sieben Shelfs) und läuft mit ONTAP 9.5.	Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)
Die Konfiguration umfasst nicht vier Storage Shelfs pro Standort und läuft mit ONTAP 9.4	Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)
Die Systeme wurden nicht ab Werk empfangen und führen ONTAP 9.3Systeme aus, die von der Fabrik empfangen wurden, sind mit zugewiesenen Laufwerken vorkonfiguriert.	Manuelles Zuweisen von Disketten für Pool 1 (ONTAP 9.3)

Überprüfen der Festplattenzuordnung für Pool 1-Festplatten

Sie müssen überprüfen, ob die Remote-Festplatten für die Knoten sichtbar sind und ordnungsgemäß zugewiesen wurden.

Bevor Sie beginnen

Sie müssen mindestens zehn Minuten warten, bis die automatische Zuweisung von Laufwerken abgeschlossen ist, nachdem die MetroCluster-IP-Schnittstellen und -Verbindungen mit dem erstellt wurden `metrocluster configuration-settings connection connect` Befehl.

Befehlsausgabe zeigt Festplattennamen in Form an: Node-Name:0m.i1.0L1

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Vergewissern Sie sich, dass Pool 1-Festplatten automatisch zugewiesen sind:

   ```
   disk show
   ```

   Die folgende Ausgabe zeigt die Ausgabe eines AFF A800 Systems ohne externe Shelfs.

   Die automatische Laufwerkszuweisung hat einem Viertel (8 Laufwerke) zu „Node_A_1“ und einem Viertel zu „Node_A_2“ zugewiesen. Die übrigen Laufwerke sind Remote-Festplatten (Pool 1) für „Node_B_1“ und „Node_B_2“.

   ```
   cluster_B::> disk show -host-adapter 0m -owner node_B_2
                       Usable     Disk              Container   Container
   Disk                Size       Shelf Bay Type    Type        Name
   Owner
   ----------------    ---------- ----- --- ------- ----------- ---------
   --------
   node_B_2:0m.i0.2L4  894.0GB    0     29  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L3  894.0GB    0     28  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L9  894.0GB    0     24  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
   node_B_2
   8 entries were displayed.

   cluster_B::> disk show -host-adapter 0m -owner node_B_1
                       Usable     Disk              Container   Container
   Disk                Size       Shelf Bay Type    Type        Name
   Owner
   ----------------    ---------- ----- --- ------- ----------- ---------
   --------
   node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
   node_B_1
   node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
   node_B_1
   node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
   node_B_1
   ```

```
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
```

```
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
```

```
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
```

```
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)

Wenn das System werkseitig nicht vorkonfiguriert war und die Anforderungen für die automatische Laufwerkszuweisung nicht erfüllt, müssen Sie die Remote Pool 1-Laufwerke manuell zuweisen.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.4 oder höher.

Weitere Informationen zur Bestimmung, ob Ihr System eine manuelle Festplattenzuordnung erfordert, finden Sie in "Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher".

Wenn die Konfiguration nur zwei externe Shelfs pro Standort umfasst, sollten 1 Laufwerke für jeden Standort aus demselben Shelf gemeinsam genutzt werden, wie in den folgenden Beispielen dargestellt:

- Node_A_1 wird Laufwerken in Einschüben 0-11 an Standort_B-Shelf_2 (Remote) zugewiesen
- Node_A_2 wird Laufwerken in Einschüben 12-23 an Standort_B-Shelf_2 (Remote) zugewiesen

Schritte

1. Weisen Sie auf jedem Knoten in der MetroCluster IP-Konfiguration Remote-Laufwerke Pool 1 zu.

    a. Zeigt die Liste der nicht zugewiesenen Laufwerke an:

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Weisen Sie dem Pool 1 des ersten Knotens (z. B. Node_A_1) die Eigentümerschaft von Remote-Laufwerken (0m) zu:

   ```
   disk assign -disk <disk-id> -pool 1 -owner <owner_node_name>
   ```

   `disk-id` Muss ein Laufwerk auf einem Remote-Shelf von identifizieren `owner_node_name`.

c. Vergewissern Sie sich, dass die Laufwerke Pool 1 zugewiesen wurden:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   > Die iSCSI-Verbindung, die zum Zugriff auf die Remote-Laufwerke verwendet wird, wird als Gerät 0 m angezeigt.

   Die folgende Ausgabe zeigt, dass die Laufwerke in Shelf 23 zugewiesen wurden, da sie in der Liste der nicht zugewiesenen Laufwerke nicht mehr angezeigt werden:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Wiederholen Sie diese Schritte, um dem zweiten Node an Standort A Pool 1-Laufwerke zuzuweisen (z. B. „Node_A_2“).
b. Wiederholen Sie diese Schritte vor Ort B.

Manuelles Zuweisen von Disketten für Pool 1 (ONTAP 9.3)

Wenn Sie für jeden Node mindestens zwei Festplatten-Shelfs haben, können Sie die Remote-Festplatten (Pool1) über die automatische Zuweisungsfunktion von ONTAP automatisch zuweisen.

Bevor Sie beginnen

Sie müssen zuerst eine Festplatte im Shelf Pool 1 zuweisen. ONTAP weist dann automatisch den Rest der Festplatten im Shelf demselben Pool zu.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.3.

Diese Vorgehensweise kann nur verwendet werden, wenn mindestens zwei Festplatten-Shelfs für jeden Node vorhanden sind, wodurch die automatische Zuweisung von Festplatten auf Shelf-Ebene ermöglicht wird.

Wenn Sie die automatische Zuweisung auf Shelf-Ebene nicht verwenden können, müssen Sie die Remote-Festplatten manuell zuweisen, damit jeder Node über einen Remote-Pool von Festplatten (Pool 1) verfügt.

Die Funktion für die automatische Festplattenzuweisung von ONTAP weist die Festplatten für das Shelf zu. Beispiel:

- Alle Festplatten auf Site_B-Shelf_2 werden dem Pool1 von Node_A_1 automatisch zugewiesen
- Alle Festplatten auf Site_B-Shelf_4 werden dem Pool1 der Node_A_2 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_2 werden dem Pool1 der Node_B_1 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_4 werden dem Pool1 der Node_B_2 automatisch zugewiesen

Sie müssen die automatische Zuweisung durch Angabe einer einzelnen Festplatte für jedes Shelf „Seeding“:

Schritte

1. Weisen Sie von jedem Knoten in der MetroCluster IP-Konfiguration einem Pool 1 eine Remote-Festplatte zu.

   a. Zeigen Sie die Liste der nicht zugewiesenen Festplatten an:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   ```
   cluster_A::> disk show -host-adapter 0m -container-type unassigned
                        Usable           Disk    Container   Container
   Disk                   Size Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   6.23.0                    -    23   0 SSD     unassigned  -         -
   6.23.1                    -    23   1 SSD     unassigned  -         -
   .
   .
   .
   node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
   node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
   .
   .
   .
   48 entries were displayed.

   cluster_A::>
   ```

   b. Wählen Sie ein Remote-Laufwerk (0m) aus, und weisen Sie dem Pool 1 des ersten Knotens (z. B. „Node_A_1“) den Besitz der Festplatte zu:

   ```
   disk assign -disk <disk_id> -pool 1 -owner <owner_node_name>
   ```

   Das `disk-id` muss eine Festplatte in einem Remote-Shelf von identifizieren `owner_node_name`.

   Die automatische Zuweisung von ONTAP-Festplatten weist alle Festplatten im Remote-Shelf zu, das die angegebene Festplatte enthält.

   c. Nachdem Sie mindestens 60 Sekunden gewartet haben, bis die automatische Zuweisung der Festplatte erfolgt ist, vergewissern Sie sich, dass die Remote-Festplatten auf dem Shelf Pool 1 automatisch zugewiesen wurden:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   > Die iSCSI-Verbindung, die zum Zugriff auf die Remote-Festplatten verwendet wird, wird als Gerät 0 m angezeigt.

   Die folgende Ausgabe zeigt, dass die Festplatten in Shelf 23 nun zugewiesen sind und nicht mehr angezeigt werden:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                      Usable           Disk    Container   Container
Disk                    Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Wiederholen Sie diese Schritte, um Pool 1-Festplatten dem zweiten Knoten an Standort A zuzuweisen (z. B. „Node_A_2“).

b. Wiederholen Sie diese Schritte vor Ort B.

Aktivieren der automatischen Laufwerkszuweisung in ONTAP 9.4

Über diese Aufgabe

Wenn Sie in ONTAP 9.4 die automatische Laufwerkszuweisung wie zuvor in diesem Verfahren beschrieben deaktiviert haben, müssen Sie sie auf allen Knoten erneut aktivieren.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Automatische Laufwerkszuweisung aktivieren:

   ```
   storage disk option modify -node <node_name> -autoassign on
   ```

   Sie müssen diesen Befehl für alle Nodes in der MetroCluster IP-Konfiguration ausgeben.

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>
   ```

   Der folgende Befehl spiegelt das Root-Aggregat für „Controller_A_1“:

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

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

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

Verwandte Informationen

"Logisches Storage-Management"

Erstellung eines gespiegelten Datenaggregats auf jedem Node

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

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke

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

   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Unabhängig davon, ob Laufwerke mit unterschiedlichen RPM zugelassen sind, finden Sie auf der man Page zum Erstellen von Storage-Aggregaten.

     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>`

Implementieren der MetroCluster-Konfiguration

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

Über diese Aufgabe

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

  Sie können dies mit dem überprüfen `storage aggregate show` Befehl.

  > Wenn Sie ein einzelnes gespiegeltes Datenaggregat verwenden möchten, finden Sie weitere Informationen unter Schritt 1 Weitere Anweisungen.

- Der HA-Konfigurationsstatus der Controller und des Chassis muss „mccip“ sein.

Sie stellen das aus `metrocluster configure` Aktivieren Sie einmal den Befehl auf einem der Nodes, um die MetroCluster-Konfiguration zu aktivieren. 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.

Der `metrocluster configure` Befehl koppelt die beiden Nodes automatisch mit den niedrigsten System-IDs in jedem der beiden Cluster als Disaster Recovery (DR) Partner. In einer MetroCluster Konfiguration mit vier Nodes gibt es zwei DR-Partnerpaare. Das zweite DR-Paar wird aus den beiden Knoten mit höheren System-IDs erstellt.

> Sie müssen vor Ausführung des Befehls * Onboard Key Manager (OKM) oder externe Schlüsselverwaltung nicht konfigurieren `metrocluster configure`.

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 reagieren `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus (*>) angezeigt.
	
	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 Administratorberechtigungsebene:
	
	`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 Knoten 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 in einer MetroCluster Konfiguration mit vier Nodes 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
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

   a. Überprüfen Sie die Konfiguration von Standort A:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show

   Configuration: IP fabric

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

   b. Überprüfen Sie die Konfiguration von Standort B:

   ```
   metrocluster show
   ```

```
cluster_B::> metrocluster show

Configuration: IP fabric

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

4. Um mögliche Probleme bei der nicht-flüchtigen Speicherspiegelung zu vermeiden, müssen Sie jeden der vier Nodes neu booten:

   ```
   node reboot -node <node_name> -inhibit-takeover true
   ```

5. Stellen Sie das aus `metrocluster show` Befehl auf beiden Clustern, um die Konfiguration erneut zu überprüfen.

Konfigurieren der zweiten DR-Gruppe in einer Konfiguration mit acht Nodes

Wiederholen Sie die vorherigen Aufgaben, um die Nodes in der zweiten DR-Gruppe zu konfigurieren.

Erstellen von nicht gespiegelten Datenaggregaten

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

Über diese Aufgabe

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

> In MetroCluster IP-Konfigurationen können Remote-Aggregate nach einem Switchover nicht zugänglich gemacht werden

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

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

Schritte

1. Implementierung von nicht gespiegelten Aggregaten:

```
metrocluster modify -enable-unmirrored-aggr-deployment
true
```

2. Vergewissern Sie sich, dass die automatische Festplattenzuordnung deaktiviert ist:

   ```
   disk option show
   ```

3. Installieren und verkabeln Sie die Festplatten-Shelfs, die die nicht gespiegelten Aggregate enthalten.

   Sie können die Verfahren in der Dokumentation Installation und Setup für Ihre Plattform und Platten-Shelfs verwenden.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Weisen Sie alle Festplatten auf dem neuen Shelf dem entsprechenden Node manuell zu:

   ```
   disk assign -disk <disk_id> -owner <owner_node_name>
   ```

5. 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 den Parameter -Node verwenden oder Laufwerke angeben, die Eigentum dieses Node sind.

   Darüber hinaus müssen Sie sicherstellen, dass Sie nur Laufwerke in das nicht gespiegelte Shelf zum Aggregat aufnehmen.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie auf der „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
```

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

   ```
   storage aggregate show-status -aggregate <aggregate_name>
   ```

7. Deaktivieren der Implementierung nicht gespiegelter Aggregate

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

8. Vergewissern Sie sich, dass die automatische Festplattenzuordnung aktiviert ist:

   ```
   disk option show
   ```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Überprüfen der MetroCluster-Konfiguration

Sie können überprüfen, ob die Komponenten und Beziehungen in der MetroCluster Konfiguration ordnungsgemäß funktionieren.

Über diese Aufgabe

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.

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

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

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

```
cluster_A::> metrocluster check show

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

2. Zeigen Sie detailliertere Ergebnisse des letzten MetroCluster-Prüfbefehls an:

   `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
```

```
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.
```

Im folgenden Beispiel wird die Ausgabe des Befehls „MetroCluster Check Cluster show“ für eine gesunde MetroCluster Konfiguration mit vier Nodes angezeigt. Sie zeigt an, dass die Cluster bei Bedarf bereit sind, eine ausgehandelte Umschaltung durchzuführen.

```
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"

ONTAP-Konfiguration abschließen

Nach dem Konfigurieren, Aktivieren und Prüfen der MetroCluster Konfiguration können Sie die Cluster-Konfiguration fortsetzen, indem Sie nach Bedarf weitere SVMs, Netzwerkschnittstellen und andere ONTAP Funktionen hinzufügen.

Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration

Ab ONTAP 9.15.1 können Sie auf unterstützten Systemen eine End-to-End-Verschlüsselung konfigurieren, um Back-End-Verkehr, wie z. B. NVlog- und Speicherreplikationsdaten, zwischen den Standorten in einer MetroCluster -IP -Konfiguration zu verschlüsseln.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Bevor Sie die End-to-End-Verschlüsselung konfigurieren können, müssen Sie dies tun "Externes Verschlüsselungsmanagement konfigurieren".

- Prüfen Sie die unterstützten Systeme und die Mindestversion von ONTAP, die erforderlich sind, um die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration zu konfigurieren:

Minimale ONTAP-Version	Unterstützte Systeme
ONTAP 9.17.1	• AFF A800, AFF C800 • AFF A20, AFF A30, AFF C30, AFF A50, AFF C60 • AFF A70, AFF A90, AFF A1K, AFF C80 • FAS50, FAS70 UND FAS90
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700

End-to-End-Verschlüsselung

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu aktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

   b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

   ```
   metrocluster check show
   ```

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

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

3. End-to-End-Verschlüsselung für jede DR-Gruppe aktivieren:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung aktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

End-to-End-Verschlüsselung deaktivieren

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu deaktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

   b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

   ```
   metrocluster check show
   ```

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

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

3. Deaktivieren Sie die End-to-End-Verschlüsselung für jede DR-Gruppe:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung deaktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Einrichten von MetroCluster Tiebreaker oder ONTAP Mediator für eine MetroCluster -IP-Konfiguration

Sie können entweder die MetroCluster Tiebreaker Software auf einem dritten Standort herunterladen und installieren oder, beginnend mit ONTAP 9.7, dem ONTAP Mediator.

Bevor Sie beginnen

Der verfügbare Linux-Host mit Netzwerkkonnektivität zu beiden Clustern in der MetroCluster-Konfiguration muss über einen Linux-Host verfügen. Die spezifischen Anforderungen sind in der Dokumentation MetroCluster Tiebreaker oder ONTAP Mediator enthalten.

Wenn Sie eine Verbindung zu einer vorhandenen Tiebreaker- oder ONTAP Mediator-Instanz herstellen, benötigen Sie den Benutzernamen, das Kennwort und die IP-Adresse des Tiebreakers oder Mediators.

Wenn Sie eine neue Instanz des ONTAP Mediators installieren müssen, befolgen Sie die Anweisungen, um die Software zu installieren und zu konfigurieren.

"Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung"

Wenn Sie eine neue Instanz der Tiebreaker Software installieren müssen, befolgen Sie die "Anweisungen zur Installation und Konfiguration der Software".

Über diese Aufgabe

Sie können die MetroCluster Tiebreaker Software und den ONTAP Mediator nicht mit derselben MetroCluster Konfiguration verwenden.

"Überlegungen zur Verwendung von ONTAP Mediator oder MetroCluster Tiebreaker"

Schritt

1. Konfigurieren Sie ONTAP Mediator oder die Tiebreaker-Software:
    - Wenn Sie eine vorhandene Instanz des ONTAP Mediators verwenden, fügen Sie ONTAP Mediator zu ONTAP hinzu:

```
metrocluster configuration-settings mediator add -mediator-address ip-
address-of-mediator-host
```

- Wenn Sie die Tiebreaker Software verwenden, lesen Sie die "Tiebreaker Dokumentation".

Sichern Sie Cluster-Konfigurationsdateien in einer MetroCluster -IP-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.

Schritt

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*.

Konfigurieren Sie die MetroCluster Software mit System Manager

Richten Sie eine MetroCluster IP-Site mit ONTAP System Manager ein

Ab ONTAP 9.8 können Sie mit System Manager einen MetroCluster IP-Standort einrichten.

Ein MetroCluster-Standort besteht aus zwei Clustern. In der Regel befinden sich die Cluster an verschiedenen geografischen Standorten.

Bevor Sie beginnen

- Das System sollte bereits gemäß dem installiert und verkabelt sein "Installations- und Setup-Anleitung", der mit dem System geliefert wurde.
- Clusternetzwerkschnittstellen sollten auf jedem Knoten eines jeden Clusters für die Kommunikation innerhalb des Clusters konfiguriert werden.

Weisen Sie eine Node-Management-IP-Adresse zu

Windows System

Sie sollten Ihren Windows-Computer mit dem Subnetz verbinden, mit dem die Controller verbunden sind. Dadurch wird Ihrem System automatisch eine Node-Management-IP-Adresse zugewiesen.

Schritte

1. Öffnen Sie vom Windows-System aus das Laufwerk **Network**, um die Knoten zu erkennen.
2. Doppelklicken Sie auf den Node, um den Cluster-Setup-Assistenten zu starten.

Andere Systeme

Sie sollten die Node-Management-IP-Adresse für einen der Nodes im Cluster konfigurieren. Sie können diese Node-Management-IP-Adresse verwenden, um den Setup-Assistenten für das Cluster zu starten.

"Erstellen des Clusters auf dem ersten Node"Informationen zum Zuweisen einer Node-Management-IP-Adresse finden Sie unter.

Initialisieren und konfigurieren Sie den Cluster

Sie initialisieren den Cluster, indem Sie ein Administratorpasswort für das Cluster festlegen und die Cluster-Management- und Node-Managementnetzwerke einrichten. Sie können auch Dienste wie einen DNS (Domain Name Server) konfigurieren, um Hostnamen aufzulösen, und einen NTP-Server zur Synchronisierung der Zeit.

Schritte

1. Geben Sie in einem Webbrowser die konfigurierte Node-Management-IP-Adresse ein: "https://node-management-IP"

   System Manager erkennt die im Cluster verbliebenen Nodes automatisch.

2. Führen Sie im Fenster **Storage System initialisieren** folgende Schritte durch:
   a. Geben Sie die Netzwerkkonfigurationsdaten des Cluster-Managements ein.
   b. Geben Sie die Node-Management-IP-Adressen für alle Nodes ein.
   c. Geben Sie DNS-Details an.
   d. Aktivieren Sie im Abschnitt **andere** das Kontrollkästchen **Zeitdienst verwenden (NTP)**, um die Zeitserver hinzuzufügen.

Wenn Sie auf **Absenden** klicken, warten Sie, bis der Cluster erstellt und konfiguriert wurde. Anschließend erfolgt ein Validierungsprozess.

Nächste Schritte

Führen Sie nach dem Einrichten, Initialisieren und Konfigurieren beider Cluster das Verfahren durch"MetroCluster IP-Peering einrichten".

Konfigurieren Sie ONTAP auf einem neuen Cluster-Video

Richten Sie MetroCluster IP-Peering mit ONTAP System Manager ein

Ab ONTAP 9.8 können Sie MetroCluster IP-Konfigurationsvorgänge mit System Manager managen. Nachdem Sie zwei Cluster eingerichtet haben, richten Sie Peering zwischen ihnen ein.

Bevor Sie beginnen

Richten Sie zwei Cluster ein. Siehe "Richten Sie einen MetroCluster IP-Standort ein"Verfahren.

Bestimmte Schritte dieses Prozesses werden von verschiedenen Systemadministratoren an den geografischen Standorten des jeweiligen Clusters ausgeführt. Zur Erläuterung dieses Verfahrens werden die Cluster „Standort A Cluster“ und „Standort B Cluster“ genannt.

Führen Sie den Peering-Prozess von Standort A aus

Dieser Prozess wird von einem Systemadministrator an Standort A durchgeführt

Schritte

1. Melden Sie sich bei Site A Cluster an.
2. Wählen Sie in System Manager in der linken Navigationsleiste **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Im Dashboard werden die Details zu diesem Cluster angezeigt (Standort A). Im Abschnitt **MetroCluster** wird Standort A Cluster auf der linken Seite angezeigt.

3. Klicken Sie Auf **Partner-Cluster Anhängen**.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten in Standort-A-Cluster ermöglichen, mit den Knoten im Standort-B-Cluster zu kommunizieren.

5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner Cluster anhängen Ich habe keine Passphrase**. Auf diese Weise können Sie eine Passphrase generieren.
7. Kopieren Sie die generierte Passphrase, und teilen Sie sie mit dem Systemadministrator an Standort B
8. Wählen Sie **Schließen**.

Peering-Prozess von Standort B durchführen

Dieser Prozess wird von einem Systemadministrator an Standort B durchgeführt

Schritte

1. Melden Sie sich bei Standort B-Cluster an.
2. Wählen Sie in System Manager **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Das Dashboard zeigt die Details zu diesem Cluster an (Standort B). Im Abschnitt MetroCluster wird links Standort-B-Cluster angezeigt.

3. Klicken Sie auf **Attach Partner Cluster**, um den Peering-Prozess zu starten.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten im Cluster Standort B ermöglichen, mit den Knoten in Standort A zu kommunizieren.
5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner Cluster anhängen Ich habe eine Passphrase**. Auf diese Weise können Sie die Passphrase eingeben, die Sie vom Systemadministrator an Standort A erhalten haben
7. Wählen Sie **Peer**, um den Peering-Prozess abzuschließen.

Was kommt als Nächstes?

Nachdem der Peering-Prozess erfolgreich abgeschlossen wurde, konfigurieren Sie die Cluster. Siehe "Konfigurieren Sie einen MetroCluster IP-Standort".

Konfigurieren Sie eine MetroCluster IP-Site mit ONTAP System Manager

Ab ONTAP 9.8 können Sie MetroCluster IP-Konfigurationsvorgänge mit System Manager managen. Dazu müssen zwei Cluster eingerichtet, Cluster-Peering durchgeführt und die Cluster konfiguriert werden.

Bevor Sie beginnen

Gehen Sie wie folgt vor:

- "Richten Sie einen MetroCluster IP-Standort ein"
- "MetroCluster IP-Peering einrichten"

Konfigurieren Sie die Verbindung zwischen Clustern

Schritte

1. Melden Sie sich an einem der Standorte bei System Manager an, und wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** zeigt die Grafik die beiden Cluster, die Sie für die MetroCluster-Sites eingerichtet und angepasst haben. Das Cluster, von dem Sie arbeiten (lokales Cluster), wird auf der linken Seite angezeigt.

2. Klicken Sie auf **MetroCluster konfigurieren**. Führen Sie in diesem Fenster die folgenden Schritte aus:
   a. Es werden die Nodes für jedes Cluster in der MetroCluster-Konfiguration dargestellt. Wählen Sie in den Dropdown-Listen die Knoten im lokalen Cluster aus, die Disaster-Recovery-Partner für die Knoten im Remote-Cluster sind.
   b. Aktivieren Sie das Kontrollkästchen, wenn Sie ONTAP Mediator konfigurieren möchten. Siehe "ONTAP Mediator konfigurieren".
   c. Wenn beide Cluster über eine Lizenz zur Aktivierung der Verschlüsselung verfügen, wird der Abschnitt **Verschlüsselung** angezeigt.

      Geben Sie zum Aktivieren der Verschlüsselung eine Passphrase ein.

   d. Aktivieren Sie das Kontrollkästchen, wenn Sie MetroCluster mit einem freigegebenen Layer-3-Netzwerk konfigurieren möchten.

      > Die HA-Partner-Nodes und die mit den Nodes verbundenen Netzwerk-Switches müssen über eine passende Konfiguration verfügen.

3. Klicken Sie auf **Speichern**, um die MetroCluster-Sites zu konfigurieren.

   Auf dem **Dashboard** im Abschnitt **MetroCluster** zeigt die Grafik ein Häkchen auf der Verbindung zwischen den beiden Clustern an, was auf eine gesunde Verbindung hinweist.

Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung

Vorbereitung der Installation von ONTAP Mediator in einer MetroCluster -IP -Konfiguration

Ihre Umgebung muss bestimmte Anforderungen erfüllen.

Die folgenden Anforderungen gelten für eine Disaster Recovery-Gruppe (DR-Gruppe). Weitere Informationen zu "DR-Gruppen".

- Wenn Sie Ihre Linux-Version aktualisieren möchten, tun Sie dies, bevor Sie die aktuellste Version von ONTAP Mediator installieren.
- Die ONTAP Mediator- und MetroCluster Tiebreaker-Software sollten nicht beide mit derselben MetroCluster-Konfiguration verwendet werden.
- ONTAP Mediator muss auf einem Linux-Host an einem anderen Standort als den MetroCluster-Sites installiert werden.

  Die Konnektivität zwischen dem ONTAP Mediator und jedem Standort muss aus zwei separaten Ausfall-Domains bestehen.

- ONTAP Mediator kann bis zu fünf MetroCluster-Konfigurationen gleichzeitig unterstützen.
- Die automatische ungeplante Umschaltung wird in ONTAP 9.7 und höher unterstützt.
- IPv6 wird mit ONTAP Mediator nicht unterstützt.

Netzwerkanforderungen für die Verwendung von ONTAP Mediator in einer MetroCluster-Konfiguration

Um ONTAP Mediator in einer MetroCluster-Konfiguration zu installieren, müssen Sie sicherstellen, dass die Konfiguration mehrere Netzwerkanforderungen erfüllt.

- Latenz

  Maximale Latenz von weniger als 75 ms (RTT).

  Jitter darf nicht mehr als 5 ms betragen.

- MTU

  Die MTU-Größe muss mindestens 1400 betragen.

- Paketverlust

  Sowohl für das Internet Control Message Protocol (ICMP) als auch für TCP-Datenverkehr muss der Paketverlust unter 0.01 % liegen.

- Bandbreite

  Die Verbindung zwischen ONTAP Mediator und einer DR-Gruppe muss über eine Bandbreite von mindestens 20 Mbit/s verfügen.

- Unabhängige Konnektivität

  Es ist eine unabhängige Verbindung zwischen jedem Standort und dem ONTAP Mediator erforderlich. Ein Ausfall an einem Standort darf die IP-Verbindung zwischen den anderen beiden nicht betroffenen Standorten nicht unterbrechen.

Hostanforderungen für ONTAP Mediator in einer MetroCluster-Konfiguration

Sie müssen sicherstellen, dass die Konfiguration mehrere Host-Anforderungen erfüllt.

- ONTAP Mediator muss an einem externen Standort installiert sein, der physisch von den beiden ONTAP Clustern getrennt ist.
- ONTAP Mediator unterstützt maximal fünf MetroCluster-Konfigurationen.
- ONTAP Mediator benötigt nicht mehr als die Mindestanforderungen des Host-Betriebssystems an CPU und Arbeitsspeicher (RAM).
- Zusätzlich zu den Mindestanforderungen des Host-Betriebssystems muss mindestens 30 GB zusätzlicher nutzbarer Festplattenspeicher zur Verfügung stehen.
  - Jede DR-Gruppe benötigt bis zu 200 MB Festplattenspeicher.

Firewall-Anforderungen für ONTAP Mediator

ONTAP Mediator verwendet eine Reihe von Ports für die Kommunikation mit bestimmten Diensten.

Wenn Sie eine Firewall eines Drittanbieters verwenden:

- HTTPS-Zugriff muss aktiviert sein.
- Er muss so konfiguriert sein, dass der Zugriff auf die Ports 31784 und 3260 möglich ist.

Bei Verwendung der standardmäßigen Red hat oder CentOS Firewall wird die Firewall während der Mediator-Installation automatisch konfiguriert.

In der folgenden Tabelle sind die Ports aufgeführt, die Sie in Ihrer Firewall zulassen müssen:

- Der iSCSI-Port ist nur in einer MetroCluster-IP-Konfiguration erforderlich.
- Der 22/tcp-Port ist für den normalen Betrieb nicht erforderlich, Sie können ihn jedoch vorübergehend für Wartungsarbeiten aktivieren und deaktivieren, wenn die Wartungssitzung beendet ist.

Port/Services	Quelle	Richtung	Ziel	Zweck
22/tcp	Management-Host	Eingehend	ONTAP Mediator	SSH / ONTAP Mediatormanagement
31784/tcp	Cluster-MGM- und Node-MGM-LIFs	Eingehend	Web-Server ONTAP Mediator	REST-API (HTTPS)
3260/tcp	Knotenverwaltungs-LIFs	Bidirektional	ONTAP Mediator iSCSI-Ziele	ISCSI-Datenverbindung für Mailboxen

Richtlinien zum Upgrade von ONTAP Mediator in einer MetroCluster-Konfiguration

Wenn Sie ONTAP Mediator aktualisieren, müssen Sie die Linux-Versionsanforderungen erfüllen und die Richtlinien für die Aktualisierung befolgen.

- ONTAP Mediator kann von einer unmittelbar vorhergehenden Version auf die aktuelle Version aktualisiert werden.
- Alle Mediator-Versionen werden von MetroCluster IP-Konfigurationen mit ONTAP 9.7 oder höher unterstützt.

"Installieren oder aktualisieren Sie ONTAP Mediator"

Nach dem Upgrade

Nachdem die Aktualisierung von Mediator und Betriebssystem abgeschlossen ist, sollten Sie den ausgeben `storage iscsi-initiator show` Befehl, um zu bestätigen, dass die Mediator-Verbindungen aktiv sind.

Einrichten des ONTAP Mediators für eine MetroCluster -IP-Konfiguration

ONTAP Mediator muss auf dem ONTAP-Knoten für die Verwendung in einer MetroCluster-IP-Konfiguration konfiguriert werden.

Bevor Sie beginnen

- ONTAP Mediator muss erfolgreich an einem Netzwerkstandort installiert worden sein, der von beiden MetroCluster-Standorten aus erreichbar ist.

  "Installieren oder aktualisieren Sie ONTAP Mediator"

- Sie müssen über die IP-Adresse des Hosts verfügen, auf dem ONTAP Mediator ausgeführt wird.
- Sie müssen über den Benutzernamen und das Passwort für ONTAP Mediator verfügen.
- Alle Nodes der MetroCluster IP-Konfiguration müssen online sein.

> Ab ONTAP 9.12.1 kann die Funktion zur automatischen erzwungenen Umschaltung von MetroCluster in einer MetroCluster IP Konfiguration aktiviert werden. Diese Funktion ist eine Erweiterung der mediatorgestützten ungeplanten Umschaltung. Bevor Sie diese Funktion aktivieren, überprüfen Sie die "Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung".

Über diese Aufgabe

- Diese Aufgabe ermöglicht standardmäßig automatische ungeplante Umschaltung.
- Diese Aufgabe kann auf der ONTAP-Schnittstelle eines beliebigen Knotens der MetroCluster IP-Konfiguration ausgeführt werden.
- Eine einzelne Installation von ONTAP Mediator kann mit bis zu fünf MetroCluster-IP-Konfigurationen konfiguriert werden.

Schritte

1. Fügen Sie ONTAP Mediator zu ONTAP hinzu:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

   > Sie werden aufgefordert, den Benutzernamen und das Kennwort für das Mediator Admin-Benutzerkonto einzugeben.

2. Stellen Sie sicher, dass die automatische Umschaltfunktion aktiviert ist:

   ```
   metrocluster show
   ```

3. Überprüfen Sie, ob der Mediator jetzt ausgeführt wird.

   a. Zeigen Sie die virtuellen Mediator-Laufwerke an:

      ```
      storage disk show -container-type mediator
      ```

```
 cluster_A::> storage disk show -container-type mediator
                        Usable           Disk    Container
Container
 Disk                   Size Shelf Bay Type    Type        Name
Owner
 ---------------- ---------- ----- --- ------- ----------- ---------
--------
 NET-1.5                   -     -   - VMDISK  mediator    -
node_A_2
 NET-1.6                   -     -   - VMDISK  mediator    -
node_B_1
 NET-1.7                   -     -   - VMDISK  mediator    -
node_B_2
 NET-1.8                   -     -   - VMDISK  mediator    -
node_A_1
```

b. Legen Sie den Berechtigungsmodus auf erweitert fest:

```
set advanced
```

```
 cluster_A::> set advanced
```

c. Anzeigen der Initiatoren, die als Mediator bezeichnet werden:

```
storage iscsi-initiator show -label mediator
```

```
 cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
-------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

d. Überprüfen Sie den Status der AUSO-Fehlerdomäne (Automatic Unplanmäßigen Switchover):

```
metrocluster show
```

> Die folgende Beispielausgabe gilt für ONTAP 9.13.1 und höher. Bei ONTAP 9.12.1 und älteren Versionen sollte der Status der AUSO-Fehlerdomäne sein `auso-on-cluster-disaster`.

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

4. Optional können Sie die automatische erzwungene Umschaltung von MetroCluster konfigurieren.

   Sie können den folgenden Befehl nur auf der erweiterten Berechtigungsebene verwenden.

> Bevor Sie diesen Befehl verwenden, überprüfen Sie die "Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung".

```
metrocluster modify -allow-auto-forced-switchover true
```

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

Entfernen Sie den ONTAP Mediator aus einer MetroCluster -IP-Konfiguration

Sie können ONTAP Mediator aus der MetroCluster-IP-Konfiguration dekonfigurieren.

Bevor Sie beginnen

Sie müssen ONTAP Mediator erfolgreich an einem Netzwerkstandort installiert und konfiguriert haben, der von beiden MetroCluster-Sites aus erreichbar ist.

Schritte

1. Dekonfigurieren Sie ONTAP Mediator mit dem folgenden Befehl:

   `metrocluster configuration-settings mediator remove`

   Sie werden aufgefordert, den Benutzernamen und das Passwort für das Administratorkonto des ONTAP Mediators einzugeben.

   > Wenn der ONTAP Mediator ausfällt, `metrocluster configuration-settings mediator remove` Der Befehl fordert Sie weiterhin auf, den Benutzernamen und das Kennwort für das ONTAP Mediator-Administratorbenutzerkonto einzugeben, und entfernt ONTAP Mediator aus der MetroCluster-Konfiguration.

   a. Überprüfen Sie mit dem folgenden Befehl, ob beschädigte Festplatten vorhanden sind:

      `disk show -broken`

      Beispiel

```
There are no entries matching your query.
```

2. Bestätigen Sie, dass ONTAP Mediator aus der MetroCluster-Konfiguration entfernt wurde, indem Sie die folgenden Befehle auf beiden Clustern ausführen:

   a. `metrocluster configuration-settings mediator show`

      Beispiel

```
This table is currently empty.
```

   b. `storage iscsi-initiator show -label mediator`

      Beispiel

```
There are no entries matching your query.
```

Verbinden Sie eine MetroCluster IP-Konfiguration mit einer anderen ONTAP Mediator-Instanz

Wenn Sie die MetroCluster-Knoten mit einer anderen ONTAP-Mediator-Instanz verbinden möchten, müssen Sie die Konfiguration aufheben und dann die Mediatorverbindung in der ONTAP-Software neu konfigurieren.

Bevor Sie beginnen

Sie benötigen den Benutzernamen, das Passwort und die IP-Adresse der neuen ONTAP Mediator-Instanz.

Über diese Aufgabe

Diese Befehle können von jedem Node in der MetroCluster Konfiguration ausgegeben werden.

Schritte

1. Entfernen Sie den aktuellen ONTAP Mediator aus der MetroCluster-Konfiguration:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Stellen Sie die neue ONTAP Mediator-Verbindung zur MetroCluster-Konfiguration her:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

Wie der ONTAP Mediator automatische ungeplante Switchover in MetroCluster -IP -Konfigurationen unterstützt

ONTAP Mediator stellt Postfach-LUNs zur Speicherung von Statusinformationen zu den MetroCluster-IP-Knoten bereit. Diese LUNs befinden sich am selben Standort wie ONTAP Mediator, der auf einem Linux-Host ausgeführt wird, der physisch von den MetroCluster-Standorten getrennt ist. Die MetroCluster IP-Knoten können die Mailbox-Informationen nutzen, um den Status ihrer Disaster Recovery (DR)-Partner zu überwachen und im Notfall eine Mediator-gestützte ungeplante Umschaltung (MAUSO) zu implementieren.

> MAUSO wird in MetroCluster FC-Konfigurationen nicht unterstützt.

Wenn ein Node einen Standortausfall erkennt, der ein Switchover erfordert, so wird nur schrittweise bestätigt, dass die Umschaltung angemessen ist und falls ja, auch die Umschaltung durchgeführt wird. Standardmäßig wird ein MAUSO für die folgenden Szenarien initiiert:

- Zum Zeitpunkt des Ausfalls werden sowohl SyncMirror-Spiegelung als auch DR-Spiegelung des nichtflüchtigen Cache jedes Node ausgeführt. Die Caches und Spiegelungen werden synchronisiert.
- Keiner der Knoten am noch verbleibenden Standort befindet sich im Übernahmemodus.
- Bei einem Standortausfall. Ein Standortausfall ist ein Ausfall von *all* Nodes am selben Standort.

Ein MAUSO wird in den folgenden Shutdown-Szenarien *Not* initiiert:

- Sie initiieren ein Herunterfahren. Beispiel, wenn Sie:
  - Halten Sie die Nodes an

- Booten Sie die Nodes neu

Erfahren Sie mehr über die MAUSO-Funktionen, die mit jeder Version von ONTAP 9 verfügbar sind.

Beginnt mit…	Beschreibung
ONTAP 9.13.1	• Ein MAUSO wird initiiert, wenn ein Standardszenario Tritt auf, und ein Lüfter- oder Hardwareausfall initiiert ein Herunterfahren der Umgebung. Beispiele für Hardwareausfälle sind eine hohe oder niedrige Temperatur, ein Netzteil, eine NVRAM-Batterie oder ein Heartbeat-Fehler des Service-Prozessors. • Der Standardwert für die Fehlerdomäne ist in einer MetroCluster IP-Konfiguration auf „aus-on-dr-Group“ gesetzt. Bei ONTAP 9.12.1 und älteren Versionen ist der Standardwert auf „auso-on-Cluster-Disaster“ eingestellt. In einer MetroCluster IP Konfiguration mit acht Nodes löst „auso-on-dr-Gruppe“ einen MAUSO aus, entweder beim Ausfall des Clusters oder bei einem HA-Paar in einer DR-Gruppe. Bei einem HA-Paar müssen beide Nodes gleichzeitig ausfallen. Optional können Sie die Einstellung der Fehlerdomäne in die Domäne „auso-on-Cluster-Disaster“ mit ändern `metrocluster modify -auto-switchover -failure-domain auso-on-cluster-disaster` Befehl zum Auslösen eines MAUSO nur, wenn in beiden DR-Gruppen ein HA-Node-Paar-Fehler vorhanden ist. • Sie können das Verhalten so ändern, dass ein MAUSO erzwungen wird, auch wenn der NVRAM zum Zeitpunkt des Fehlers nicht synchron ist.
ONTAP 9.12.1	Sie können die automatische erzwungene Umschaltung von MetroCluster in einer MetroCluster IP-Konfiguration mithilfe von aktivieren `metrocluster modify -allow -auto-forced-switchover true` Befehl. Umschaltung bei Erkennung eines Standortausfalls erfolgt automatisch, wenn die MetroCluster Funktion zur automatischen erzwungenen Umschaltung aktiviert wird. Diese Funktion ergänzt die MetroCluster IP Funktion zur automatischen Umschaltung. **Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung** Wenn Sie zulassen, dass eine MetroCluster-IP-Konfiguration im automatischen Umschaltmodus betrieben wird, kann das folgende bekannte Problem zu Datenverlust führen: • Der nicht-flüchtige Speicher in den Storage Controllern wird nicht zum Remote-DR-Partner am Partnerstandort gespiegelt. **Achtung**: Es können Szenarien auftreten, die nicht erwähnt werden. NetApp ist nicht verantwortlich für Datenkorruption, Datenverlust oder andere Schäden, die durch die Aktivierung der automatischen erzwungenen MetroCluster Switchover-Funktion entstehen können. Verwenden Sie die Funktion zur automatischen erzwungenen Umschaltung nicht von MetroCluster, wenn das Risiko und die Einschränkungen für Sie nicht akzeptabel sind.

Verwalten Sie den ONTAP Mediator mit System Manager in MetroCluster -IP -Konfigurationen

Mit System Manager können Sie Aufgaben zum Verwalten von ONTAP Mediator ausführen.

Über diese Aufgaben

Ab ONTAP 9.8 können Sie System Manager als vereinfachte Schnittstelle zur Verwaltung einer MetroCluster IP-Konfiguration mit vier Knoten verwenden. Zu dieser Konfiguration kann auch ein ONTAP Mediator an einem dritten Standort gehören.

Ab ONTAP 9.14.1 können Sie die folgenden Vorgänge auch für einen MetroCluster IP-Standort mit acht Nodes ausführen. Sie können ein System mit acht Nodes nicht mit System Manager einrichten oder erweitern, aber wenn Sie bereits ein MetroCluster IP-System mit acht Nodes eingerichtet haben, können Sie diese Vorgänge trotzdem ausführen.

Führen Sie die folgenden Aufgaben aus, um ONTAP Mediator zu verwalten.

Aufgabe durchführen…	Ergreifen Sie diese Maßnahmen…
ONTAP Mediator konfigurieren	Beide Cluster an den MetroCluster Standorten sollten up und Peering durchgeführt werden. **Schritte** 1. Wählen Sie unter System Manager in ONTAP 9.8 die Option **Cluster > Einstellungen** aus. 2. Klicken Sie im Abschnitt **Mediator** auf ⚙. 3. Klicken Sie im Fenster **Mediator konfigurieren** auf **Hinzufügen+**. 4. Geben Sie die Konfigurationsdetails für ONTAP Mediator ein. Sie können die folgenden Details eingeben, während Sie ONTAP Mediator mit System Manager konfigurieren. ◦ Die IP-Adresse des ONTAP Mediators. ◦ Der Benutzername. ◦ Das Passwort.

Aktivieren oder Deaktivieren der Mediator-gestützten automatischen Umschaltung (MAUSO)	**Schritte** 1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie neben dem Namen der MetroCluster-Site auf ⋮ . 4. Wählen Sie **Enable** oder **Disable**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **enable** oder **Disable**. ⓘ Sie können ONTAP Mediator aktivieren oder deaktivieren, wenn er erreichbar ist und sich beide Standorte im „Normal“-Modus befinden. ONTAP Mediator ist weiterhin erreichbar, wenn MAUSO aktiviert oder deaktiviert ist und das MetroCluster-System fehlerfrei ist.
Entfernen Sie ONTAP Mediator aus der MetroCluster-Konfiguration	**Schritte** 1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie neben dem Namen der MetroCluster-Site auf ⋮ . 4. Wählen Sie **Mediator Entfernen**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **Entfernen**.
Überprüfen Sie den Zustand von ONTAP Mediator	Führen Sie die spezifischen Schritte des System Managers in "Überprüfen Sie den Funktionszustand einer MetroCluster-Konfiguration"aus.
Durchführen einer Umschaltung und eines Switchback	Führen Sie die Schritte in "Verwenden Sie System Manager für Umschaltung und Switchback (nur MetroCluster IP-Konfigurationen)."aus.

Testen Sie die ONTAP -Knotenumschaltung für Ihre MetroCluster IP-Konfiguration

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

Überprüfung der ausgehandelten Umschaltung

Sie können die ausgehandelte (geplante) Umschaltung testen, um die unterbrechungsfreie Datenverfügbarkeit zu bestätigen.

Über diese Aufgabe

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.

Über diese Aufgabe

Dieser Test dauert etwa 30 Minuten.

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

Die Heilungsschritte sind auf Systemen mit ONTAP 9.5 oder höher nicht erforderlich, auf denen nach einer ausgehandelten Umschaltung automatisch eine Heilung durchgeführt wird. Auf Systemen mit ONTAP 9.6 und höher wird die Reparatur auch nach nicht ungeplanter Umschaltung automatisch durchgeführt.

Schritte

1. Wenn ONTAP 9.4 oder eine frühere Version des Systems ausgeführt wird, kann das Datenaggregat repariert werden:

```
metrocluster heal aggregates
```

Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

```
cluster_A::> metrocluster heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. Wenn das System ONTAP 9.4 oder älter ausführt, können Sie das Root-Aggregat heilen:

   `metrocluster heal root-aggregates`

   Dieser Schritt ist für folgende Konfigurationen erforderlich:

   - MetroCluster FC-Konfigurationen
   - MetroCluster IP-Konfigurationen mit ONTAP 9.4 oder einer früheren Version Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. 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
```

   Wenn der automatische Heilvorgang aus irgendeinem Grund fehlschlägt, müssen Sie den ausgeben `metrocluster heal` Befehle, die manuell wie in ONTAP-Versionen vor ONTAP 9.5 ausgeführt werden. Sie können das verwenden `metrocluster operation show` Und `metrocluster operation history show -instance` Befehle, um den Status der Reparatur zu überwachen und die Ursache eines Fehlers zu bestimmen.

4. Überprüfen der Spiegelung aller Aggregate:

   `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   -
```

5. 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.
```

6. Führen Sie den Wechsel zurück:

```
metrocluster switchback
```

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

7. 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.
```

8. Status des MetroCluster-Vorgangs bestätigen:

```
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: -
```

Überprüfung des Betriebs nach Stromunterbrechung

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

Über diese Aufgabe

Als Best Practice empfiehlt es sich, jede Netzteileinheit (PSU) einer Komponente mit separaten Netzteilen zu verbinden. Wenn beide Netzteile mit derselben Stromverteilereinheit (Power Distribution Unit, PDU) verbunden sind und eine elektrische Störung auftritt, kann der Standort ausfallen oder ein komplettes Shelf 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:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

   ```
   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.

Über diese Aufgabe

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
                                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. Identifizieren 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 die Shelf-ID „31“ ausgewählt, um den Fehler zu verhindern.

```
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 show

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

   Das Aggregat mit Laufwerken auf dem ausgeschalteten Shelf sollte einen „degradierten“ RAID-Status haben, und Laufwerke auf dem betroffenen Plex sollten den Status „Fehlgeschlagen“ 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 den RAID-Status „Resynchronisierung“ aufweisen, 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 von „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
```

MetroCluster-Konfigurationen entfernen

Wenden Sie sich an den technischen Support, wenn Sie die MetroCluster Konfiguration entfernen müssen.

Kontaktieren Sie den technischen Support von NetApp und lesen Sie das entsprechende Handbuch für Ihre

Konfiguration von "Entfernen von Knoten aus einer MetroCluster Konfiguration - Auflösungsleitfaden."

> Die Konfiguration von MetroCluster kann nicht rückgängig gemacht werden. Dieses Verfahren sollte nur mit Unterstützung durch den technischen Support erfolgen. Nach dem Entfernen der MetroCluster-Konfiguration sollten alle Festplatten-Konnektivität und Interconnects auf einen unterstützten Zustand eingestellt werden.

Anforderungen und Überlegungen für ONTAP -Operationen mit MetroCluster -IP-Konfigurationen

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.

Die ONTAP Konfiguration der beiden Cluster einschließlich Netzwerk sollte identisch sein, da die MetroCluster Funktion darauf setzt, dass ein Cluster bei einem Switchover Daten nahtlos für seinen Partner bereitstellen kann.

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.

MetroCluster-Vorgänge in ONTAP System Manager

Je nach ONTAP Version können einige MetroCluster spezifische Vorgänge mit ONTAP System Manager ausgeführt werden.

Weitere Informationen finden Sie im "Managen Sie MetroCluster Standorte mit System Manager" Dokumentation.

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 vserver Peer Repeer Befehl arbeiten kann.

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

Für FlexCache-Beziehungen zu einem Cluster außerhalb der MetroCluster-Konfiguration muss nach einem Switchover das Peering 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 wenn Site_A und site_C nicht verbunden sind, müssen Sie die SVMs On site_B (das Switchover-Cluster) und site_C nach der Umschaltung manuell mit dem vserver Peer-Repeer-Befehl aufheben.

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

Verwandte Informationen

"Management von FlexCache Volumes mit der CLI"

FabricPool-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.7 unterstützen MetroCluster Konfigurationen FabricPool Storage Tiers.

Allgemeine Informationen zur Verwendung von FabricPool finden Sie unter "Festplatten- und Tier-Management (Aggregat)".

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 zum externen Objektspeicher gelangen kann.
- FabricPool unterstützt die SVM-Migration nicht, wenn die Quelle oder das Ziel ein MetroCluster-Cluster ist.

  "Erfahren Sie mehr über SVM-Datenmobilität".

Konfigurieren eines Aggregats zur Verwendung in einer gespiegelten FabricPool

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

Schritte

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 in 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 ist physisch weiter entfernt zum Cluster 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

"Netzwerk- und LIF-Management"

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

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

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

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.

Verwandte Informationen

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

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

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
- Sie sollten ein Subnetz-Objekt erstellen, bevor Sie eine LIF erstellen. Mithilfe eines Subnetzobjekts kann ONTAP Failover-Ziele auf dem Zielcluster ermitteln, da ihm eine Broadcast-Domäne zugeordnet ist.

Überprüfen Sie die LIF-Erstellung

Sie können die erfolgreiche Erstellung einer logischen Schnittstelle in einer MetroCluster-Konfiguration bestätigen, indem Sie den MetroCluster Check lif show-Befehl ausführen. Falls beim Erstellen des LIF Probleme auftreten, können Sie den Befehl MetroCluster Check lif Repair-Placement zum Beheben von Problemen verwenden.

Verwandte Informationen

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

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

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 sich im DR-Cluster keine Ports im gleichen IPspace befinden, 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 wird dadurch bestimmt, dass die Konnektivität der Quell-Fabric-WWN auf den Ports im DR-Cluster geprüft wird.Wenn dieselbe Fabric nicht am DR-Standort vorhanden ist, wird die LIF auf einen zufälligen Port am DR-Partner platziert.	Die Erreichbarkeit wird durch die Reaktion auf ein ARP-Protokoll (Address Resolution Protocol) bestimmt, das von jedem zuvor identifizierten Port des DR-Clusters auf die Quell-IP-Adresse der zu platzierten LIF gesendet wird.um die Erreichbarkeit erfolgreich zu prüfen, müssen ARP-Übertragungen 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 die LIF auf einem zufällig verbundenen Port des DR-Partners platziert.	Von den Ports, die während der Prüfung der Erreichbarkeit als erreichbar markiert sind, ONTAP bevorzugt Ports, die in der Broadcast-Domäne vorhanden sind, die mit dem Subnetz der logischen Schnittstelle verknüpft sind.Wenn im DR-Cluster keine Netzwerk-Ports verfügbar sind, die sich in der Broadcast-Domäne befinden, die mit dem Subnetz der logischen Schnittstelle verknüpft ist, Dann wählt ONTAP Ports aus, die eine Erreichbarkeit der Quell-LIF haben. 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.

Verwandte Informationen

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

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

Volume-Erstellung auf einem Root-Aggregat

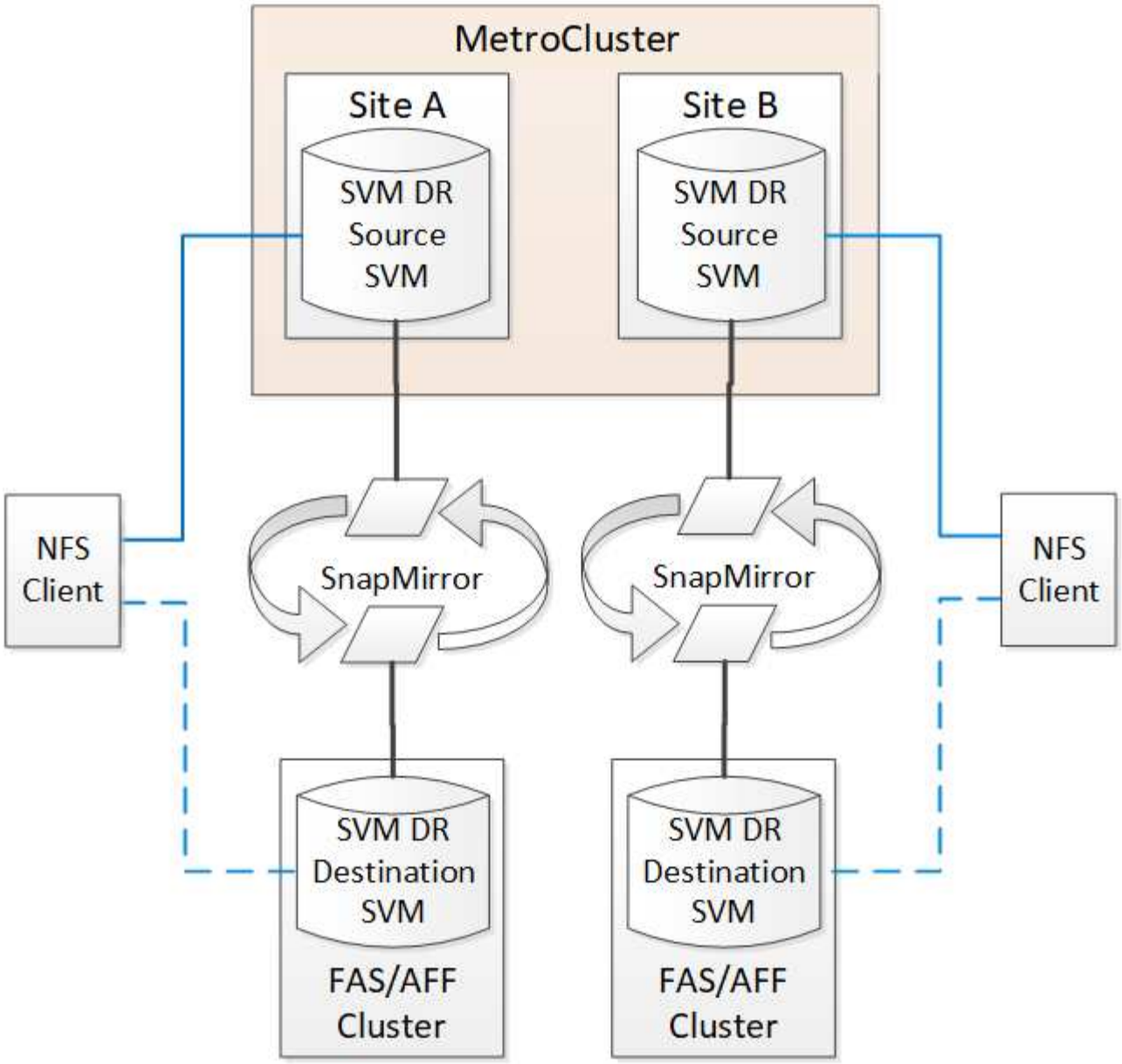
Das System lässt nicht die Erstellung neuer Volumes im Root-Aggregat (ein Aggregat mit einer HA-Richtlinie von CFO) eines Knotens in einer MetroCluster-Konfiguration zu.

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.

Ab ONTAP 9.11.1 können beide Standorte innerhalb einer MetroCluster-Konfiguration die Quelle für eine SVM-DR-Beziehung mit einem FAS oder einem AFF-Ziel-Cluster sein, wie im folgenden Image dargestellt.



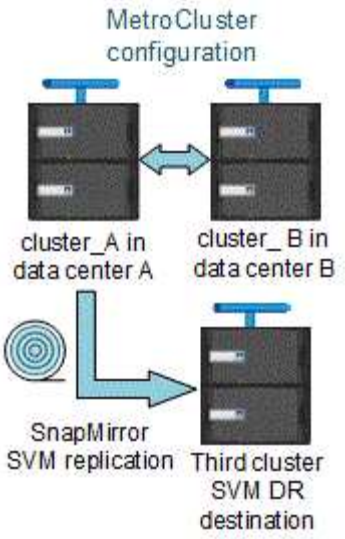
Bei der Verwendung von SVMs mit SnapMirror Disaster Recovery sollten Sie die folgenden Anforderungen und Einschränkungen beachten:

- 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.

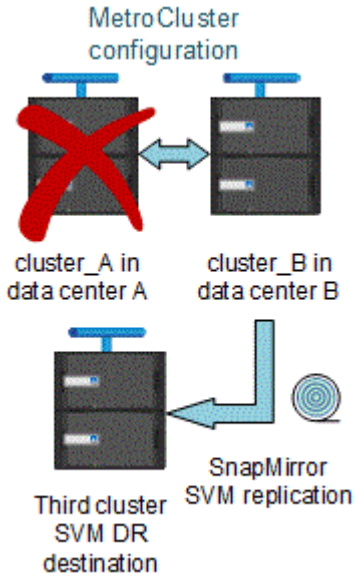
- Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind.

  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.

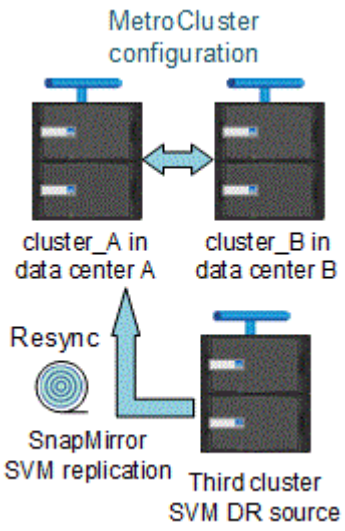
  Nach Abschluss des Switchover- oder Switch-Prozesses werden jedoch die nächsten geplanten SVM-DR-Updates erfolgreich durchgeführt.

Weitere Informationen finden Sie unter „`Replizieren der SVM-Konfiguration`“ in "Datensicherung" 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.

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

Wenn Sie den Befehl Storage Aggregate Plex show nach einer MetroCluster-Umschaltung ausführen, ist der Status von Plex0 des über das Root-Aggregat umgeschaltet unbestimmt und wird als fehlgeschlagen angezeigt. 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.

Schritt

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

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

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

Verwenden Sie den Active IQ Unified Manager und den ONTAP System Manager für die weitere Konfiguration und Überwachung in einer MetroCluster -IP -Konfiguration

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-Dokumentation"

Synchronisieren Sie die Systemzeit mit NTP in einer MetroCluster -IP-Konfiguration

Jedes Cluster benötigt einen eigenen NTP-Server (Network Time Protocol), um die Zeit zwischen den Nodes und ihren Clients zu synchronisieren.

Über diese Aufgabe

- Nach dem Takeover können Sie die Zeitzoneneinstellungen für einen ausgefallenen Node oder den Partner-Node nicht ändern.
- Jedes Cluster in der MetroCluster IP-Konfiguration sollte über einen eigenen NTP-Server oder eigene Server verfügen, die von den Nodes und IP-Switches am MetroCluster-Standort verwendet werden.
- Wenn Sie den MetroCluster Tiebreak oder ONTAP Mediator verwenden, sollte es auch einen eigenen separaten NTP-Server haben.
- Dieses Verfahren zeigt, wie Sie NTP konfigurieren, nachdem Sie die MetroCluster IP-Cluster bereits eingerichtet haben. Wenn Sie die Cluster mit System Manager konfiguriert haben, sollten Sie die NTP-Server bereits im Rahmen des Cluster-Setups konfiguriert haben. Weitere Informationen finden Sie unter "Richten Sie einen MetroCluster IP-Standort ein" .

Abhängig von Ihrer ONTAP-Version können Sie den NTP über die Registerkarte **Cluster** oder **Insights** in der Benutzeroberfläche des Systemmanagers konfigurieren.

Cluster

In System Manager können Sie den NTP auf der Registerkarte **Cluster** mit zwei verschiedenen Optionen konfigurieren, je nach ONTAP-Version:

ONTAP 9.8 oder höher:

Führen Sie die folgenden Schritte aus, um das NTP von der Registerkarte **Cluster** in ONTAP 9.8 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Wählen Sie dann die Option und dann

Bearbeiten.
3. Wählen Sie im Fenster **Cluster-Details bearbeiten** die Option **+Hinzufügen** unter NTP-Servern aus.
4. Fügen Sie den Namen und den Speicherort hinzu, und geben Sie die IP-Adresse des Zeitservers an.
5. Wählen Sie dann **Speichern**.
6. Wiederholen Sie die Schritte für weitere Zeitserver.

ONTAP 9.11.1 oder höher:

Führen Sie die folgenden Schritte aus, um den NTP vom Fenster **Insights** auf der Registerkarte **Cluster** in ONTAP 9.11.1 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Scrollen Sie auf der Seite nach unten zum Fenster **Insights**, suchen Sie **zu wenige NTP-Server sind konfiguriert**, und wählen Sie dann **Fix IT**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Einblick

In ONTAP 9.11.1 oder höher können Sie NTP auch über die Registerkarte **Insights** in System Manager konfigurieren:

Schritte

1. Wechseln Sie in der System Manager-Benutzeroberfläche zur Registerkarte **Insights**.
2. Scrollen Sie nach unten zu **zu wenige NTP-Server sind konfiguriert** und wählen Sie **Fix it**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Wo Sie weitere Informationen zu MetroCluster IP finden

Weitere Informationen zur MetroCluster Konfiguration.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff

"Architektur und Design der MetroCluster IP-Lösung, TR-4689"	• Eine technische Übersicht über die Konfiguration und den Betrieb der MetroCluster IP-Adresse. • Best Practices für eine MetroCluster-IP-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
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln
"Disaster Recovery"	• Disaster Recovery • Erzwungene Umschaltung • Recovery nach einem Multi-Controller- oder Storage-Ausfall

"MetroCluster-Wartung"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes
"MetroCluster Upgrade und Erweiterung"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"MetroCluster Transition"	• Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration
"MetroCluster: Upgrade, Transition und Erweiterung"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Dokumentation zu ONTAP Hardwaresystemen" **Hinweis:** die standardmäßigen Speicherregal-Wartungsverfahren können mit MetroCluster IP-Konfigurationen verwendet werden.	• Hot-Adding eines Festplatten-Shelfs • Hot-entfernen eines Festplatten-Shelfs
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate

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[1]	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 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.

Hinweise

1. Lesen Sie die folgenden Überlegungen für MetroCluster IP-Konfigurationen mit acht Nodes:
    - 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.

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 das richtige Installationsverfahren basierend darauf auswählen, wie die Speichercontroller mit den Speicherregalen verbunden werden.

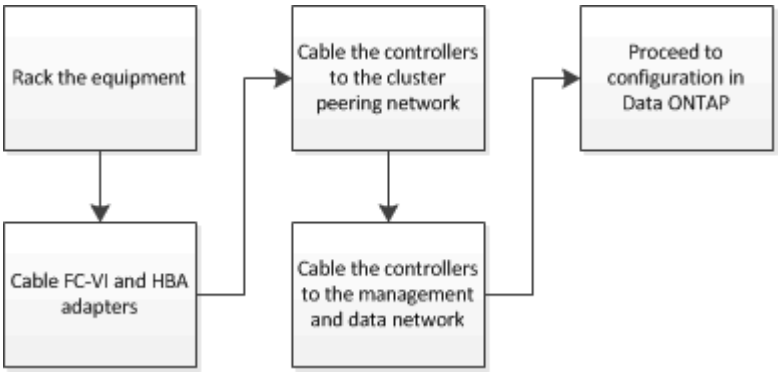
Für diesen Installationstyp…	Verwenden Sie diese Verfahren…

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"

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.



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.

"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. "IMT"

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.

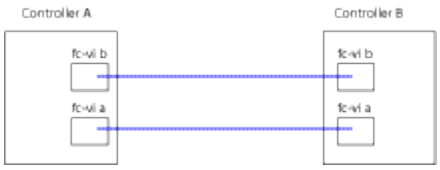
Verkabelung der Controller untereinander und den Storage Shelfs

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.

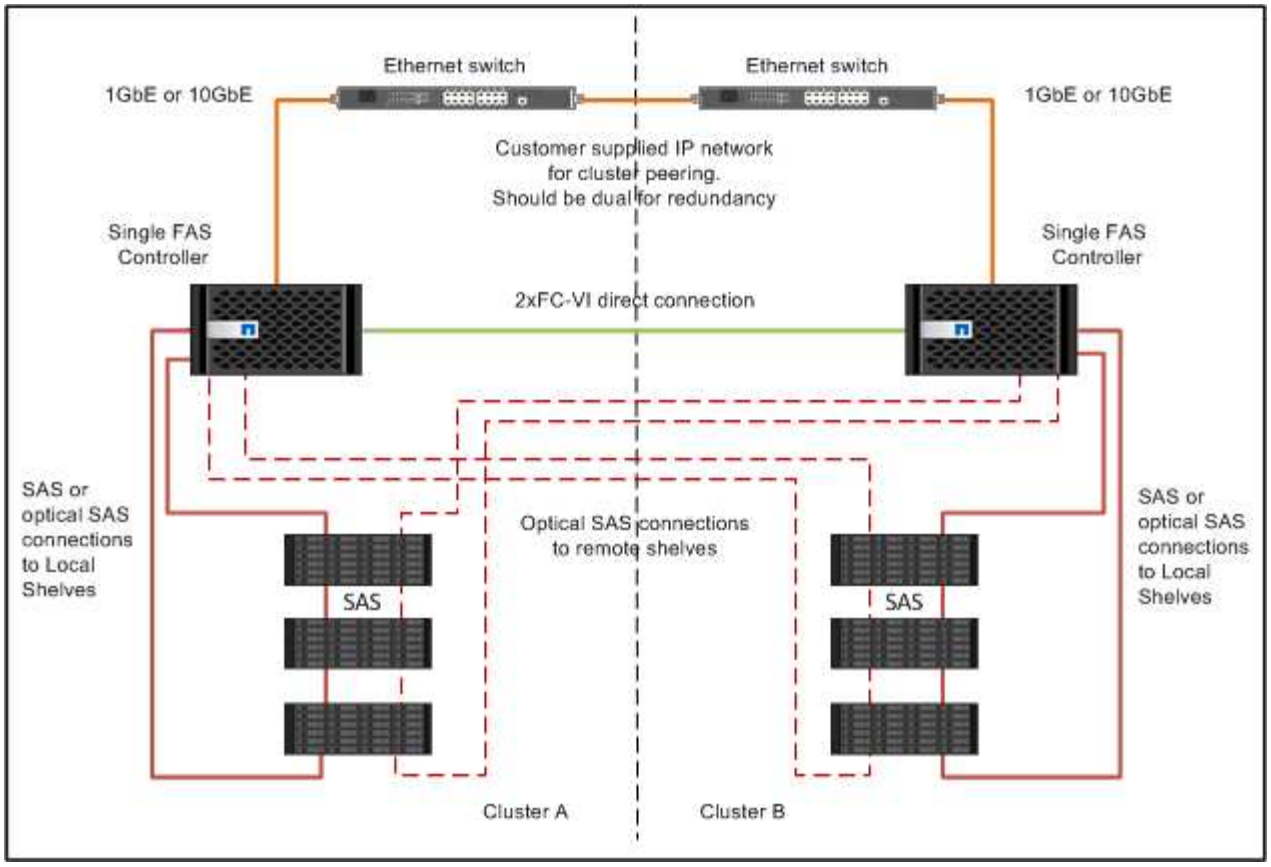


   Die obige Abbildung ist ein typischer repräsentativer Kabelanschluss. Die spezifischen FC-VI-Ports variieren je nach Controller-Modul.

   - 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

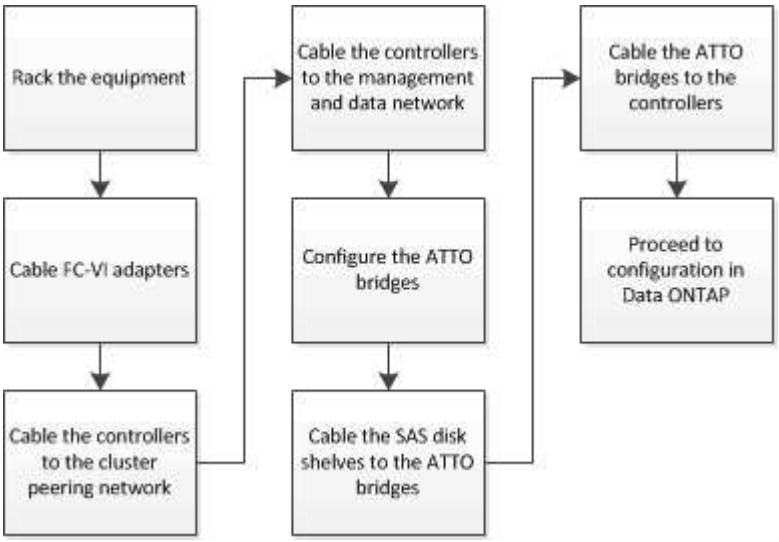
1. Verkabeln Sie die Management- und Daten-Ports des Controllers mit den Management- und Datennetzwerken am lokalen Standort.

   "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.



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.

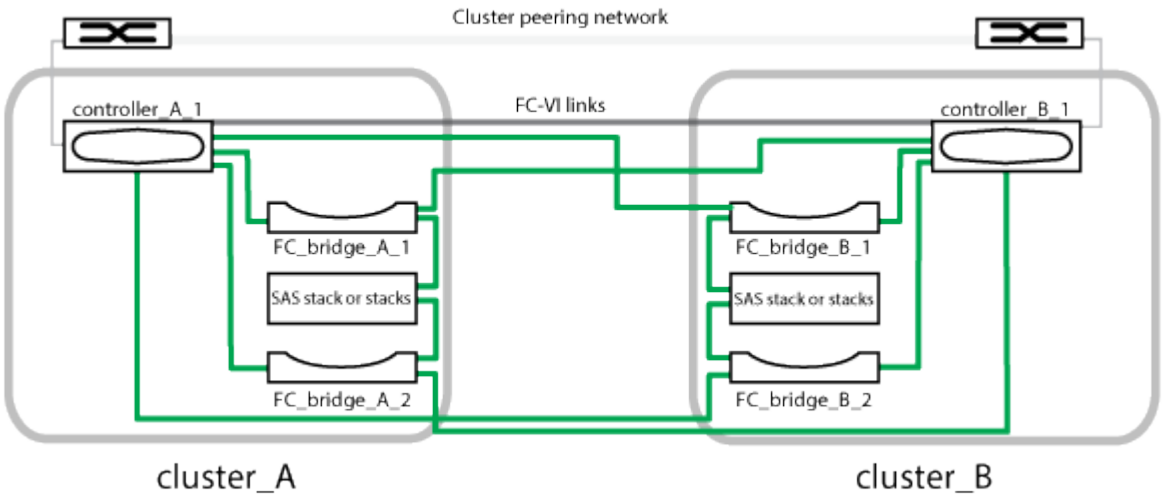
- FC-to-SAS-Bridges

  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. "IMT"

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.

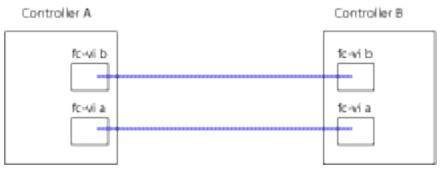
Die LED „Bridge Ready“ kann bis zu 30 Sekunden in Anspruch nehmen, was darauf hinweist, dass die Bridge ihre Selbsttestsequenz beim Einschalten abgeschlossen hat.

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"

Installation von FC-to-SAS-Bridges und SAS-Platten-Shelves

Installieren und verkabeln Sie ATTO FibreBridge Bridges und SAS-Platten-Shelfs, wenn Sie der Konfiguration neuen Speicher hinzufügen.

Über diese Aufgabe

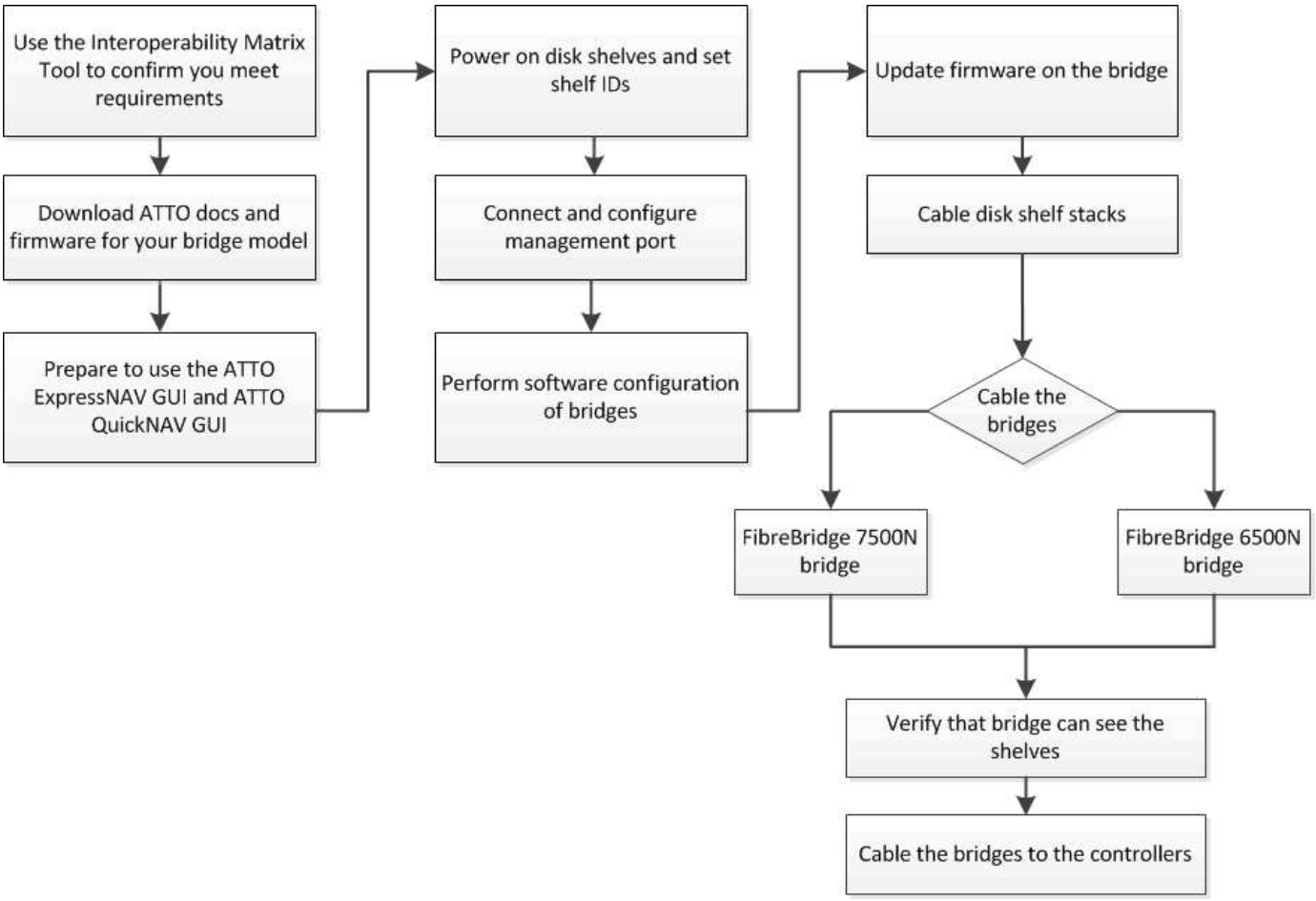
Bei den werkseitig eingegangenen Systemen sind die FC-zu-SAS-Bridges vorkonfiguriert und erfordern keine zusätzliche Konfiguration.

Dieses Verfahren wird mit der Annahme geschrieben, dass Sie die empfohlenen Bridge Management-Schnittstellen verwenden: Die ATTO ExpressNAV GUI und ATTO Quicknav Dienstprogramm.

Sie verwenden die ATTO ExpressNAV GUI, um eine Bridge zu konfigurieren und zu verwalten und die Bridge-Firmware zu aktualisieren. Sie verwenden das ATTO Quicknav Dienstprogramm, um den Bridge Ethernet Management 1 Port zu konfigurieren.

Stattdessen können Sie bei Bedarf andere Managementoberflächen verwenden, z. B. einen seriellen Port oder Telnet, um eine Bridge zu konfigurieren und zu verwalten, den Ethernet Management 1-Port zu konfigurieren und FTP, um die Bridge-Firmware zu aktualisieren.

Bei diesem Verfahren wird folgender Workflow verwendet:



In-Band-Management der FC-to-SAS-Bridges

Ab ONTAP 9.5 mit FibreBridge 7500N oder 7600N Bridges wird *in-Band-Management* der Brücken als Alternative zum IP-Management der Brücken unterstützt. Ab ONTAP 9.8 ist das Out-of-Band-Management veraltet.

> 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.

Bei der bandinternen Verwaltung können die Bridges über die ONTAP-CLI über die FC-Verbindung zur Bridge verwaltet und überwacht werden. Der physische Zugriff auf die Bridge über die Ethernet-Ports der Bridge ist nicht erforderlich, wodurch die Sicherheitslücke der Bridge verringert wird.

Die Verfügbarkeit der in-Band-Verwaltung der Brücken hängt von der Version von ONTAP ab:

- Ab ONTAP 9.8 werden Brücken standardmäßig über in-Band-Verbindungen verwaltet und die Out-of-Band-Verwaltung der Brücken über SNMP ist veraltet.
- ONTAP 9.5 bis 9.7: Entweder in-Band-Management oder Out-of-Band-SNMP-Management wird unterstützt.
- Vor ONTAP 9.5 wird nur die bandexterne SNMP-Verwaltung unterstützt.

Bridge-CLI-Befehle können über den ONTAP-Schnittstellenbefehl über die ONTAP-Schnittstelle ausgegeben `storage bridge run-cli -name <bridge_name> -command <bridge_command_name>` werden.

Die Verwendung von in-Band-Management mit deaktiviertem IP-Zugriff wird empfohlen, um die Sicherheit durch Beschränkung der physischen Konnektivität der Bridge zu verbessern.

FiberBridge 7600N und 7500N Brückengrenzen und Befestigungsregeln

Überprüfen Sie die Grenzwerte und Überlegungen beim Anbringen von FibreBridge 7600N- und 7500N-Brücken.

Grenzwerte für FibreBridge 7600N und 7500N-Brücken

- Die maximale Anzahl der kombinierten HDD- und SSD-Laufwerke beträgt 240.
- Die maximale Anzahl von SSD-Laufwerken beträgt 96.
- Es sind maximal 48 SSDs pro SAS-Port zulässig.
- Die maximale Anzahl von Shelfs pro SAS-Port ist 10.

Befestigungsregeln für FibreBridge 7600N und 7500N

- Verwenden Sie keine SSD- und HDD-Laufwerke zusammen am selben SAS-Port.
- Verteilen Sie die Shelfs gleichmäßig über die SAS-Ports.
- Sie sollten DS460 Shelfs nicht auf demselben SAS Port wie andere Shelf-Typen (z. B. DS212 oder DS224 Shelfs) einsetzen.

Beispielkonfiguration

Im Folgenden ist eine Beispielkonfiguration zum Anschluss von vier DS224-Shelfs mit SSD-Laufwerken und sechs DS224-Shelfs mit HDD-Laufwerken dargestellt:

SAS-Port	Shelfs und Laufwerke
SAS Port-A	2 DS224-Shelfs mit SSD-Laufwerken
SAS-Port-B	2 DS224-Shelfs mit SSD-Laufwerken
SAS-Port-C	3x DS224-Shelfs mit HDD-Laufwerken
SAS-Port-D	3x DS224-Shelfs mit HDD-Laufwerken

Bereiten Sie die Installation vor

Wenn Sie die Installation der Bridges als Teil Ihres neuen MetroCluster-Systems vorbereiten, müssen Sie sicherstellen, dass Ihr System bestimmte Anforderungen erfüllt, einschließlich der Erfüllung der Setup- und Konfigurationsanforderungen für die Bridges. Weitere Anforderungen sind das Herunterladen der erforderlichen Dokumente, das Dienstprogramm ATTO Quicknav und die Bridge-Firmware.

Bevor Sie beginnen

- Das System muss bereits in einem Rack installiert sein, wenn es nicht in einem Systemschrank ausgeliefert wurde.
- Ihre Konfiguration muss unterstützte Hardware-Modelle und Software-Versionen verwenden.

  Im können Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" Feld **Speicherlösung** Ihre MetroCluster-Lösung auswählen. Mit dem **Komponenten-Explorer** können Sie die Komponenten und die ONTAP-Version auswählen, um Ihre Suche zu verfeinern. Sie können **Ergebnisse anzeigen** auswählen, um die Liste der unterstützten Konfigurationen anzuzeigen, die den Kriterien entsprechen.

- Jeder FC-Controller muss über einen FC-Port verfügen, damit eine Bridge angeschlossen werden kann.
- Sie müssen mit der Handhabung von SAS-Kabeln und den Überlegungen und Best Practices für die Installation und Verkabelung von Festplatten-Shelfs vertraut sein.

  Das Handbuch „ *Installation and Service Guide*“ für Ihr Festplatten-Shelf-Modell beschreibt die Überlegungen und Best Practices.

- Der Computer, mit dem Sie die Brücken einrichten, muss einen ATTO-unterstützten Webbrowser betreiben, um die ATTO ExpressNAV GUI nutzen zu können.

  Die *ATTO Product Release Notes* verfügen über eine aktuelle Liste der unterstützten Webbrowser. Sie können auf dieses Dokument über die ATTO-Website zugreifen, wie in den folgenden Schritten beschrieben.

Schritte

1. Laden Sie das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell herunter:
   a. Greifen Sie über den Link Ihres FibreBridge-Modells auf die ATTO-Website zu, und laden Sie das Handbuch und das Quicknav-Dienstprogramm herunter.

   > Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihre Modellbrücke enthält weitere Informationen zu Management-Schnittstellen.
   >
   > Sie können auf diesen und andere Inhalte auf der ATTO-Website zugreifen, indem Sie den Link auf der ATTO FibreBridge-Beschreibungsseite verwenden.

2. Sammeln Sie die Hardware und Informationen, die benötigt werden, um die empfohlenen Bridge Management-Schnittstellen, die ATTO ExpressNAV GUI und das ATTO Quicknav Dienstprogramm zu verwenden:
   a. Legen Sie einen nicht standardmäßigen Benutzernamen und ein Kennwort fest (für den Zugriff auf die Brücken).

      Sie sollten den Standardbenutzernamen und das Standardpasswort ändern.

   b. Bei der Konfiguration für die IP-Verwaltung der Brücken benötigen Sie das abgeschirmte Ethernet-Kabel mit den Brücken (das vom Bridge Ethernet Management 1-Port mit Ihrem Netzwerk verbunden wird).
   c. Wenn Sie für das IP-Management der Brücken konfigurieren, benötigen Sie eine IP-Adresse, eine Subnetzmaske und Gateway-Informationen für den Ethernet-Management-Port 1 auf jeder Bridge.
   d. Deaktivieren Sie VPN-Clients auf dem Computer, den Sie für die Einrichtung verwenden.

      Aktive VPN-Clients führen zum Fehlschlagen des Quicknav-Scans für Brücken.

Installieren Sie die FC-to-SAS-Bridge und die SAS-Shelfs

Nachdem Sie sichergestellt haben, dass das System alle Anforderungen in „`Vorbereitung auf die Installation`“ erfüllt, können Sie Ihr neues System installieren.

Über diese Aufgabe

- Die Festplatten- und Shelf-Konfiguration an beiden Standorten sollte identisch sein.

  Wenn ein nicht gespiegeltes Aggregat verwendet wird, kann die Festplatten- und Shelf-Konfiguration an

jedem Standort unterschiedlich sein.

> Alle Festplatten in der Disaster Recovery-Gruppe müssen denselben Verbindungstyp verwenden und für alle Nodes innerhalb der Disaster Recovery-Gruppe sichtbar sein. Dabei spielt es keine Rolle, welche Festplatten für ein gespiegeltes oder nicht gespiegeltes Aggregat verwendet werden.

- Die Anforderungen an die Systemkonnektivität für maximale Entfernungen für Platten-Shelves, FC-Controller und Backup-Bandgeräte mit Multimode-Glasfaserkabeln von 50 Mikron gelten auch für FibreBridge Bridges.

  "NetApp Hardware Universe"

- Eine Kombination aus IOM12-Modulen und IOM3-Modulen wird im selben Storage-Stack nicht unterstützt. Wenn auf dem System eine unterstützte Version von ONTAP ausgeführt wird, wird im selben Storage Stack eine Kombination aus IOM12-Modulen und IOM6-Modulen unterstützt.

> In-Band ACP wird ohne zusätzliche Verkabelung in den folgenden Shelves und FibreBridge 7500N oder 7600N Bridge unterstützt:
>
> - IOM12 (DS460C) hinter einer 7500N bzw. 7600N Brücke mit ONTAP 9.2 und höher
> - IOM12 (DS212C und DS224C) hinter einer 7500N oder 7600N Brücke mit ONTAP 9.1 und höher

> SAS-Shelves in MetroCluster-Konfigurationen unterstützen keine ACP-Verkabelung.

Aktivieren Sie ggf. den IP-Port-Zugriff auf die FibreBridge 7600N-Brücke

Wenn Sie eine ONTAP-Version vor 9.5 verwenden oder anderweitig planen, Out-of-Band-Zugriff auf die FibreBridge 7600N-Brücke über Telnet oder andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) zu nutzen, können Sie die Zugriffsservices über den Konsolen-Port aktivieren.

Über diese Aufgabe

Im Gegensatz zu den ATTO FibreBridge 7500N Bridges wird die FibreBridge 7600N mit deaktivierten IP-Port-Protokollen und -Diensten ausgeliefert.

Ab ONTAP 9.5 wird *in-Band-Management* der Brücken unterstützt. Das bedeutet, dass die Brücken über die FC-Verbindung zur Bridge von der ONTAP-CLI konfiguriert und überwacht werden können. Physischer Zugang zur Bridge über die Bridge-Ethernet-Ports ist nicht erforderlich und die Bridge-Benutzeroberflächen sind nicht erforderlich.

Ab ONTAP 9.8 wird *in-Band-Management* der Bridges standardmäßig unterstützt und out-of-Band SNMP-Management ist veraltet.

Diese Aufgabe ist erforderlich, wenn Sie zur Verwaltung der Brücken * nicht* verwenden. In diesem Fall müssen Sie die Bridge über den Ethernet-Management-Port konfigurieren.

Schritte

1. Greifen Sie auf die Konsolenschnittstelle der Bridge zu, indem Sie ein serielles Kabel an den seriellen Port der FibreBridge 7600N-Brücke anschließen.
2. Aktivieren Sie die Zugriffsservices über die Konsole, und speichern Sie die Konfiguration:

```
set closeport none
```

```
saveconfiguration
```

Der `set closeport none` Befehl aktiviert alle Zugriffsservices auf der Bridge.

3. Deaktivieren Sie ggf. einen Dienst, indem Sie den ausstellen `set closeport` Befehl und Wiederholung des Befehls nach Bedarf, bis alle gewünschten Dienste deaktiviert sind:

   ```
   set closeport service
   ```

   Der `set closeport` Durch den Befehl wird ein einzelner Dienst gleichzeitig deaktiviert.

   Der Parameter *`service`* Kann wie folgt angegeben werden:

   - expressnav
   - ftp
   - icmp
   - quicknav
   - snmp
   - telnet

   Sie können mithilfe der überprüfen, ob ein bestimmtes Protokoll aktiviert oder deaktiviert ist `get closeport` Befehl.

4. Wenn Sie SNMP aktivieren, müssen Sie auch folgenden Befehl ausgeben:

   ```
   set SNMP enabled
   ```

   SNMP ist das einzige Protokoll, das einen separaten Enable-Befehl erfordert.

5. Konfiguration speichern:

   ```
   saveconfiguration
   ```

Konfigurieren Sie die FC-zu-SAS-Bridges

Bevor Sie das Modell der FC-zu-SAS-Brücken verkabeln, müssen Sie die Einstellungen in der FibreBridge-Software konfigurieren.

Bevor Sie beginnen

Sie sollten entscheiden, ob Sie die bandinterne Verwaltung der Brücken verwenden.

> 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.

Über diese Aufgabe

Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den

entsprechenden Schritten angegeben.

Schritte

1. Konfigurieren Sie den seriellen Konsolenport auf der ATTO FibreBridge, indem Sie die Portgeschwindigkeit auf 115000 Bauds einstellen:

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

   Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.

3. Wenn Sie die IP-Verwaltung konfigurieren, schließen Sie den Ethernet-Management-1-Port an jeder Bridge über ein Ethernet-Kabel an das Netzwerk an.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Der Ethernet Management 1 Port ermöglicht es Ihnen, schnell die Bridge-Firmware (über ATTO ExpressNAV oder FTP Management-Schnittstellen) herunterzuladen und Core-Dateien und Extrahieren von Logs abzurufen.

4. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

5. Konfigurieren Sie die Bridge.

   Notieren Sie sich den Benutzernamen und das Kennwort, den Sie bestimmen.

> Konfigurieren Sie die Zeitsynchronisierung auf ATTO FibreBridge 7600N oder 7500N nicht. Die Zeitsynchronisierung für ATTO FibreBridge 7600N oder 7500N ist auf die Cluster-Zeit eingestellt, nachdem die Brücke von ONTAP erkannt wurde. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

   Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle Verbindung mit der FibreBridge.

   Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

   ```
   set ipaddress mp1 ip-address

   set ipsubnetmask mp1 subnet-mask

   set ipgateway mp1 x.x.x.x

   set ipdhcp mp1 disabled

   set ethernetspeed mp1 1000
   ```

b. Konfigurieren Sie den Brückennamen.

   Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

   Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

   - Bridge_A_1a
   - Bridge_A_1b
   - Bridge_B_1a
   - Bridge_B_1b

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set bridgename <bridge_name>
   ```

c. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:

   ```
   set SNMP enabled
   ```

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

6. Konfigurieren Sie die Bridge-FC-Ports.

a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

   Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

   - Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
   - Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.

   > Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch vom FC-Port des Controller-Moduls unterstützt wird, mit dem der Bridge-Port verbunden wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set FCDataRate <port-number> <port-speed>
   ```

b. Wenn Sie eine FibreBridge 7500N-Bridge konfigurieren, konfigurieren Sie den Verbindungsmodus, den der Port für „ptp“ verwendet.

   > Die Einstellung FCConnMode ist nicht erforderlich, wenn Sie eine FibreBridge 7600N-Bridge konfigurieren.

   Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

   ```
   set FCConnMode <port-number> ptp
   ```

c. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, müssen Sie den FC2-Port konfigurieren oder deaktivieren.

   - Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
   - Wenn Sie den zweiten Port nicht verwenden, müssen Sie den Port deaktivieren:

     ```
     FCPortDisable <port-number>
     ```

   Im folgenden Beispiel wird die Deaktivierung von FC-Port 2 gezeigt:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

a. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, deaktivieren Sie die nicht verwendeten SAS-Ports:

   ```
   SASPortDisable sas-port
   ```

   > SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren.

Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein. Im folgenden Beispiel wird die Deaktivierung von SAS Port B gezeigt Sie müssen die SAS-Ports C und D ähnlich deaktivieren:

```
SASPortDisable b

SAS Port B has been disabled.
```

7. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration. Wählen Sie je nach Version des ONTAP, auf dem Ihr System ausgeführt wird, eine der folgenden Optionen aus.

ONTAP-Version	Schritte

ONTAP 9.5 oder höher	a. Den Status der Brücken anzeigen:
	`storage bridge show`
	Der Ausgang zeigt an, welche Brücke nicht gesichert ist.
	b. Sichern Sie die Brücke:
	`securebridge`

ONTAP 9.4 oder früher	a. Den Status der Brücken anzeigen:
	
	`storage bridge show`
	
	Der Ausgang zeigt an, welche Brücke nicht gesichert ist.
	
	b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:
	
	`info`
	
	Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.
	
	c. Wenn Ethernet-Port MP1 aktiviert ist, führen Sie folgende Schritte aus:
	
	`set EthernetPort mp1 disabled`
	
	Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.
	
	d. Die Konfiguration der Bridge speichern.
	
	Sie müssen die folgenden Befehle ausführen:
	
	`SaveConfiguration`
	
	`FirmwareRestart`
	
	Sie werden aufgefordert, die Bridge neu zu starten.

8. Verwenden Sie nach Abschluss der MetroCluster-Konfiguration das `flashimages` Befehl zum Überprüfen der Version der FibreBridge-Firmware und, wenn die Brücken nicht die neueste unterstützte Version verwenden, aktualisieren Sie die Firmware auf allen Brücken in der Konfiguration.

   "Warten von MetroCluster-Komponenten"

Verkabeln Sie die Platten-Shelfs mit den Bridges

Für die Verkabelung Ihrer Platten-Shelves müssen die richtigen FC-to-SAS-Bridges verwendet werden.

Wahlmöglichkeiten

- Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM12-Modulen
- Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM6- oder IOM3-Modulen

Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Festplatten-Shelfs mit IOM12-Modulen

Nach der Konfiguration der Bridge können Sie mit der Verkabelung Ihres neuen Systems beginnen.

Über diese Aufgabe

Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche.

Schritte

1. Schalten Sie die Festplatten-Shelfs in den einzelnen Stacks in Reihe:

   a. Beginnend mit dem logischen ersten Shelf im Stack verbinden Sie IOM A-Port 3 mit IOM A-Port 1 im nächsten Shelf, bis jedes IOM A im Stack verbunden ist.

   b. Wiederholen Sie den vorherigen Unterschritt für IOM B.

   c. Wiederholen Sie die vorherigen Unterschritte für jeden Stack.

   Das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell bietet detaillierte Informationen zum Verketten von Platten-Shelfs in Reihe.

2. Schalten Sie die Festplatten-Shelfs ein und legen Sie dann 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.

3. Verkabeln Sie die Platten-Shelves mit den FibreBridge Bridges.

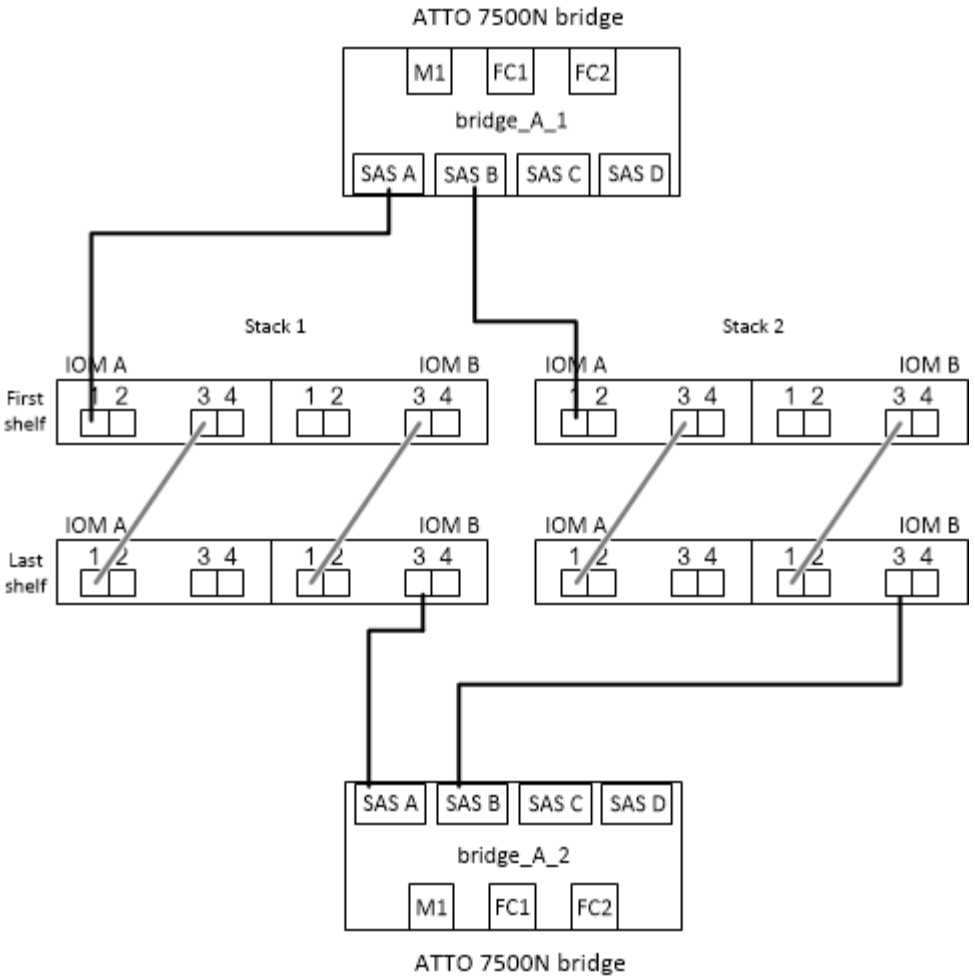
   a. Verkabeln Sie für den ersten Stack der Festplatten-Shelfs IOM A des ersten Shelfs zu SAS-Port A auf FibreBridge A und verkabeln Sie IOM B des letzten Shelfs zum SAS-Port A auf FibreBridge B

   b. Wiederholen Sie für weitere Shelf-Stacks den vorherigen Schritt mit dem nächsten verfügbaren SAS-Port der FibreBridge-Brücken, wobei Port B für den zweiten Stack, Port C für den dritten Stack und Port D für den vierten Stack verwendet wird.

   c. Schließen Sie während der Verkabelung die auf IOM12- und IOM3-/IOM6-Modulen basierenden Stacks an dieselbe Bridge an, solange sie mit separaten SAS-Ports verbunden sind.

   > Jeder Stack kann unterschiedliche IOM-Modelle verwenden. Alle Festplatten-Shelfs in einem Stack müssen jedoch dasselbe Modell verwenden.

   Die folgende Abbildung zeigt die mit einem Paar FibreBridge 7600N- oder 7500N-Brücken verbundenen Platten-Shelves:



Verkabeln Sie eine FibreBridge 7600N- oder 7500N-Bridge mit Shelfs mit IOM6- oder IOM3-Modulen

Nach der Konfiguration der Bridge können Sie mit der Verkabelung Ihres neuen Systems beginnen. Die FibreBridge 7600N oder 7500N Bridge nutzt Mini-SAS-Anschlüsse und unterstützt Shelfs, die IOM6- oder IOM3-Module verwenden.

Über diese Aufgabe

IOM3-Module werden von FibreBridge 7600N-Brücken nicht unterstützt.

Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche.

Schritte

1. Schalten Sie die Regale in den einzelnen Stapeln in Reihe.

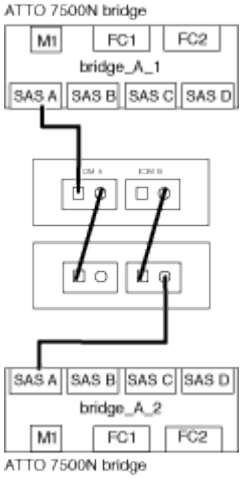
    a. Verkabeln Sie beim ersten Stapel von Shelves IOM Einen quadratischen Port des ersten Shelfs zu SAS-Port A auf FibreBridge A

    b. Verkabeln Sie für den ersten Stapel von Shelves IOM B-Kreis-Port des letzten Shelfs zu SAS-Port A auf FibreBridge B.

    Das *Installation and Service Guide* für Ihr Shelf-Modell enthält detaillierte Informationen zum Verketten von Shelfs.

    "Installation und Service Guide für SAS-Platten-Shelfs für DS4243, DS2246, DS4486 und DS4246"

Die folgende Abbildung zeigt eine Reihe von Brücken, die mit einem Regal verbunden sind:



2. Wiederholen Sie für weitere Shelf-Stacks die vorherigen Schritte mithilfe des nächsten verfügbaren SAS-Ports der FibreBridge-Brücken, wobei Port B für einen zweiten Stack, Port C für einen dritten Stack und Port D für einen vierten Stack verwendet wird.

   Die folgende Abbildung zeigt vier Stapel, die mit einem Paar FibreBridge 7600N oder 7500N-Brücken verbunden sind.

Überprüfen Sie die Bridge-Konnektivität und verkabeln Sie die FC-zu-SAS-Brücken mit den Controller-FC-Ports

Sie müssen die Bridges in einer über Bridge verbundenen MetroCluster-Konfiguration mit den Controller-FC-Ports verkabeln.

Schritte

1. Vergewissern Sie sich, dass jede Bridge alle Festplattenlaufwerke und Festplatten-Shelfs erkennen kann, mit denen die Bridge verbunden ist:

   ```
   sastargets
   ```

   Der `sastargets` In der Befehlsausgabe werden die mit der Bridge verbundenen Geräte (Festplatten und Festplatten-Shelfs) angezeigt. Die Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können.

   Die folgende Ausgabe zeigt, dass 10 Festplatten angeschlossen sind:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

2. Vergewissern Sie sich, dass die Befehlsausgabe anzeigt, dass die Bridge mit den richtigen Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Schritt 1 Für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie, ob die SAS-Kabel lose sind oder korrigieren Sie die SAS-Verkabelung, indem Sie die Platten-Shelves an den Bridges neu verkabeln. Verkabeln Sie die Platten-Shelfs mit den Bridges b. Wiederholen Schritt 1 Für jede verbleibende Brücke.

3. Verkabeln Sie jede Brücke mit den FC-Ports des Controllers:

   a. Verkabeln Sie den FC-Port 1 der Bridge mit einem FC-Port am Controller in „Cluster_A“

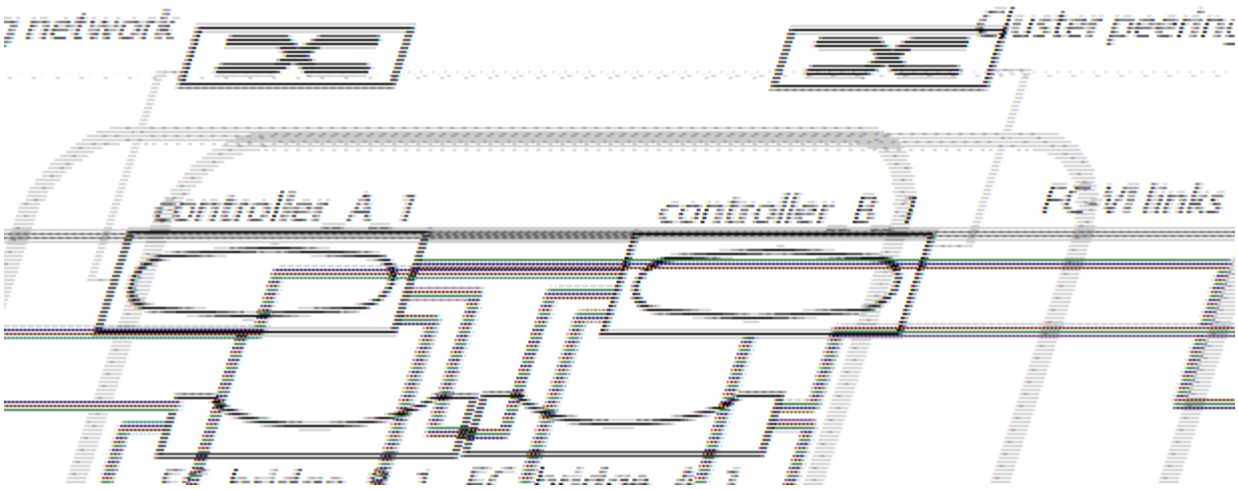
   b. Verkabeln Sie den FC-Port 2 der Bridge mit einem FC-Port am Controller in „Cluster_B.“

   - Wenn der Controller mit einem FC-Adapter mit vier Ports konfiguriert ist, stellen Sie sicher, dass die Bridges an beiden Enden des Storage-Stacks nicht mit zwei FC-Ports auf demselben ASIC verbunden sind. Beispiel:
     - Port A und Port B teilen sich denselben ASIC.
     - Port c und Port d teilen sich denselben ASIC.

       Verbinden Sie in diesem Beispiel FC_Bridge_A_1 mit Port A und FC_Bridge_A2 mit Port c.

   - Wenn der Controller mit mehr als einem FC-Adapter konfiguriert ist, verkabeln Sie die Brücken an einem der Enden des Storage Stacks nicht mit demselben Adapter.

     In diesem Szenario sollten Sie FC_Bridge_A_1 mit einem integrierten FC-Port verbinden und FC_Bridge_A_2 mit einem FC-Port an einem Adapter in einem Erweiterungssteckplatz verbinden.



4. Wiederholen Schritt 3 An den anderen Brücken bis alle Brücken verkabelt sind.

Sichern oder unsichern Sie die FibreBridge-Brücke

Um potenziell unsichere Ethernet-Protokolle auf einer Bridge einfach zu deaktivieren, können Sie ab ONTAP 9.5 die Bridge sichern. Dadurch werden die Ethernet-Ports der Bridge deaktiviert. Sie können auch den Ethernet-Zugriff erneut aktivieren.

Über diese Aufgabe

- Durch das Sichern der Brücke werden Telnet und andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) auf der Brücke deaktiviert.
- Bei diesem Verfahren wird die Out-of-Band-Verwaltung mithilfe der ONTAP-Eingabeaufforderung verwendet, die ab ONTAP 9.5 verfügbar ist.

  Sie können die Befehle aus der Bridge-CLI ausgeben, wenn Sie keine Out-of-Band-Verwaltung verwenden.

- Der `unsecurebridge` Mit dem Befehl können die Ethernet-Ports wieder aktiviert werden.
- In ONTAP 9.7 und früher, Ausführen der `securebridge` Durch den Befehl auf der ATTO FibreBridge wird der Bridge-Status auf dem Partner-Cluster möglicherweise nicht korrekt aktualisiert. Führen Sie in diesem Fall den aus `securebridge` Befehl aus dem Partner-Cluster.

> 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. Sichern Sie die Bridge an der ONTAP-Eingabeaufforderung des Clusters mit der Bridge oder unsichern Sie sie.
   - Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
     ```

   - Mit dem folgenden Befehl wird Bridge_A_1 aufgehoben:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. Speichern Sie in der ONTAP-Eingabeaufforderung des Clusters, der die Bridge enthält, die Bridge-Konfiguration:

   ```
   storage bridge run-cli -bridge <bridge-name> -command saveconfiguration
   ```

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. Starten Sie an der ONTAP-Eingabeaufforderung des Clusters, das die Bridge enthält, die Firmware der Bridge neu:

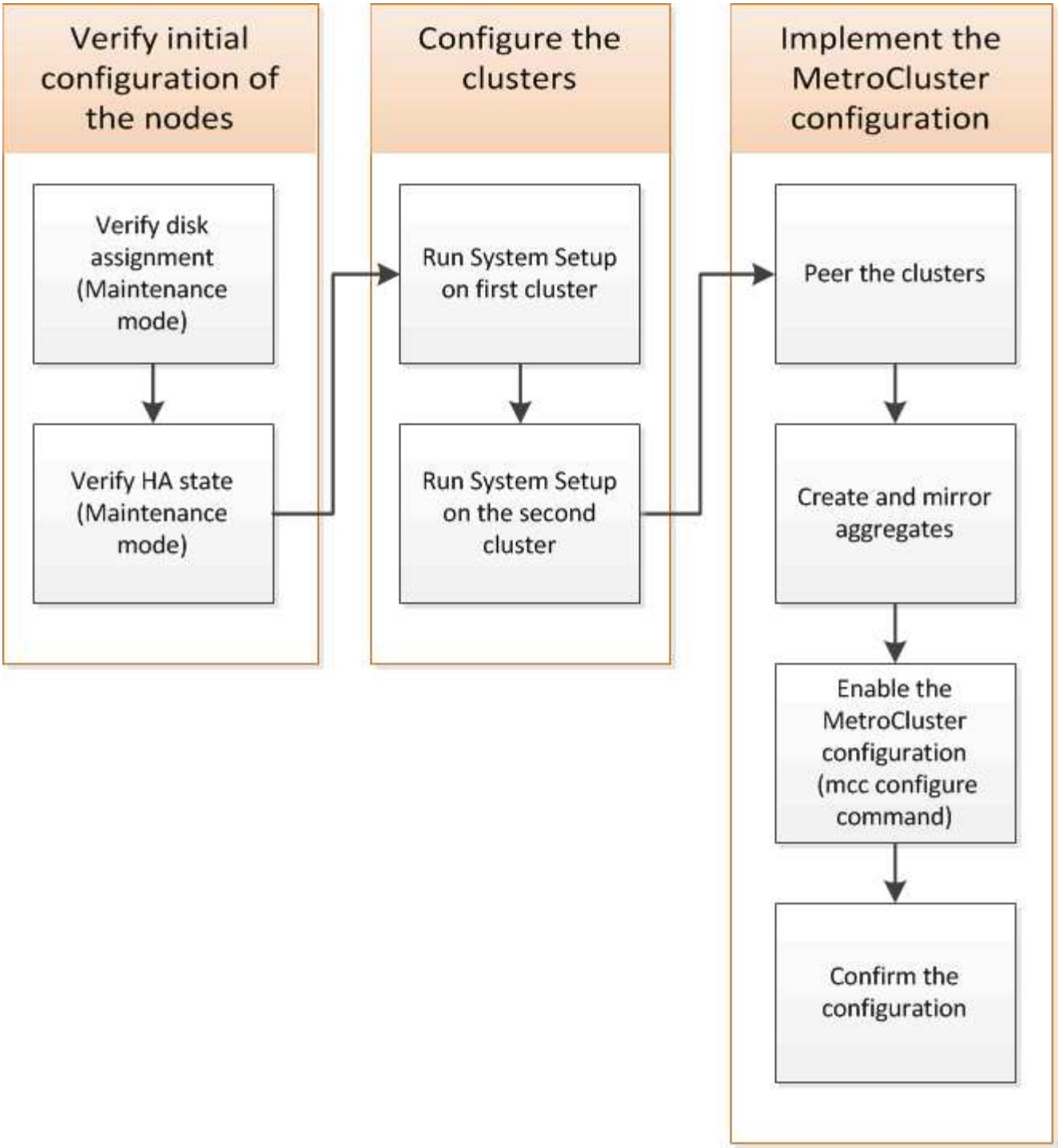
   ```
   storage bridge run-cli -bridge <bridge-name> -command firmwarerestart
   ```

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
   ```

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.

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

  "Festplatten- und Aggregatmanagement"

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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
- Anzahl der zu einführenden Laufwerke

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

- Prüfsummenstil, den Sie für das Aggregat verwenden möchten
- Typ der zu verwendenden Laufwerke
- Die Größe der zu verwendenden Laufwerke
- Fahrgeschwindigkeit zu verwenden
- RAID-Typ für RAID-Gruppen auf dem Aggregat
- Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
- 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 in dem 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 sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- 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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - 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 Verfahren für ausgehandelte Umschaltung, Healing und Switchback, die in der beschrieben sind "Durchführung von Umschaltung, Healing und Switchback".

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
   ```

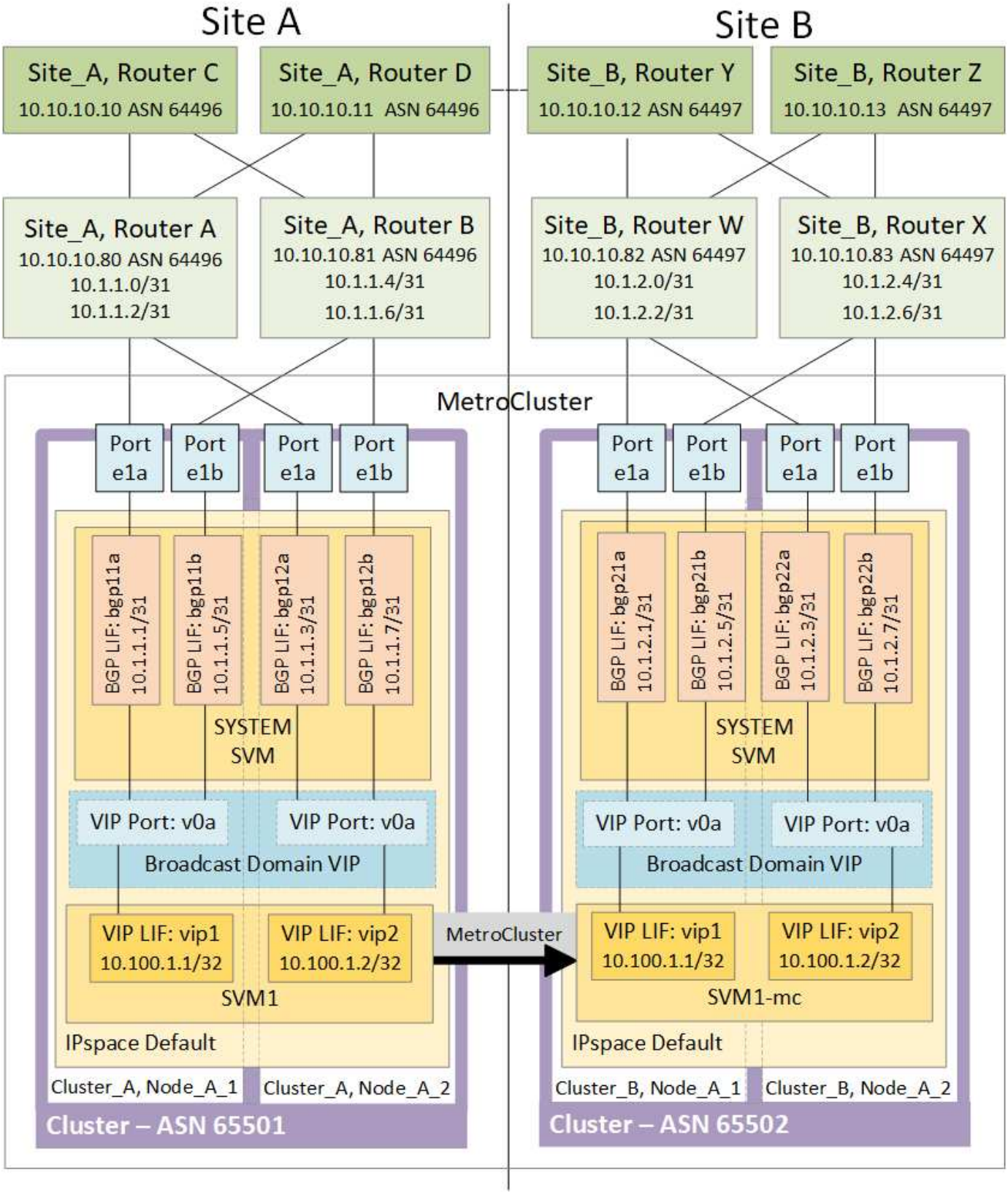
   Der "Cluster-Management mit der CLI" Enthält zusätzliche Informationen unter dem Abschnitt *Verwalten von Konfigurations-Backups*.

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
```

MetroCluster-Konfigurationen entfernen

Wenden Sie sich an den technischen Support, wenn Sie die MetroCluster Konfiguration entfernen müssen.

Kontaktieren Sie den technischen Support von NetApp und lesen Sie das entsprechende Handbuch für Ihre Konfiguration von "Entfernen von Knoten aus einer MetroCluster Konfiguration - Auflösungsleitfaden."

Die Konfiguration von MetroCluster kann nicht rückgängig gemacht werden. Dieses Verfahren sollte nur mit Unterstützung durch den technischen Support erfolgen. Nach dem Entfernen der MetroCluster-Konfiguration sollten alle Festplatten-Konnektivität und Interconnects auf einen unterstützten Zustand eingestellt werden.

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

Weitere Konfigurations- und Überwachungsfunktionen sind mit dem Active IQ Unified Manager und dem ONTAP System Manager möglich

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-Dokumentation"

Synchronisieren Sie die Systemzeit mit NTP

Jedes Cluster benötigt einen eigenen NTP-Server (Network Time Protocol), um die Zeit zwischen den Nodes und ihren Clients zu synchronisieren.

Über diese Aufgabe

- Sie können nach dem Takeover die Zeitzoneneinstellungen für einen ausgefallenen Node oder den Partner-Node nicht ändern.
- Jedes Cluster in der Stretch-MetroCluster-Konfiguration sollte über einen eigenen, separaten NTP-Server oder Server verfügen, die von den Nodes am MetroCluster-Standort verwendet werden.
- Wenn Sie die MetroCluster Tiebreaker Software verwenden, sollte es auch einen eigenen separaten NTP-Server haben.

Abhängig von Ihrer ONTAP-Version können Sie den NTP über die Registerkarte **Cluster** oder **Insights** in der Benutzeroberfläche des Systemmanagers konfigurieren.

Cluster

In System Manager können Sie den NTP auf der Registerkarte **Cluster** mit zwei verschiedenen Optionen konfigurieren, je nach ONTAP-Version:

ONTAP 9.8 oder höher:

Führen Sie die folgenden Schritte aus, um das NTP von der Registerkarte **Cluster** in ONTAP 9.8 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Wählen Sie dann die Option und dann

Bearbeiten.
3. Wählen Sie im Fenster **Cluster-Details bearbeiten** die Option **+Hinzufügen** unter NTP-Servern aus.
4. Fügen Sie den Namen und den Speicherort hinzu, und geben Sie die IP-Adresse des Zeitservers an.
5. Wählen Sie dann **Speichern**.
6. Wiederholen Sie die Schritte für weitere Zeitserver.

ONTAP 9.11.1 oder höher:

Führen Sie die folgenden Schritte aus, um den NTP vom Fenster **Insights** auf der Registerkarte **Cluster** in ONTAP 9.11.1 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Scrollen Sie auf der Seite nach unten zum Fenster **Insights**, suchen Sie **zu wenige NTP-Server sind konfiguriert**, und wählen Sie dann **Fix IT**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Einblick

In ONTAP 9.11.1 oder höher können Sie NTP auch über die Registerkarte **Insights** in System Manager konfigurieren:

Schritte

1. Wechseln Sie in der System Manager-Benutzeroberfläche zur Registerkarte **Insights**.
2. Scrollen Sie nach unten zu **zu wenige NTP-Server sind konfiguriert** und wählen Sie **Fix it**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

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 zum externen Objektspeicher gelangen 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.
- Sie sollten ein Subnetz-Objekt erstellen, bevor Sie eine LIF erstellen. Mithilfe eines Subnetzobjekts kann ONTAP Failover-Ziele auf dem Zielcluster ermitteln, da ihm eine Broadcast-Domäne zugeordnet ist.

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.

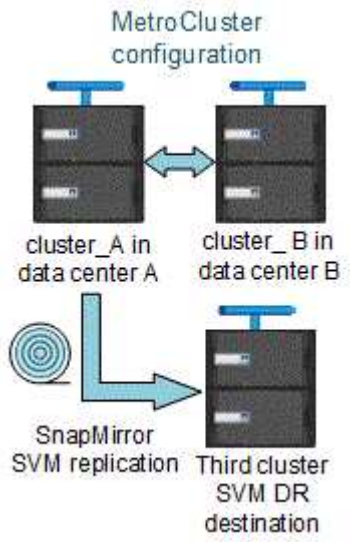
Bei der Verwendung von SVMs mit SnapMirror Disaster Recovery sollten Sie die folgenden Anforderungen und Einschränkungen beachten:

- 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.

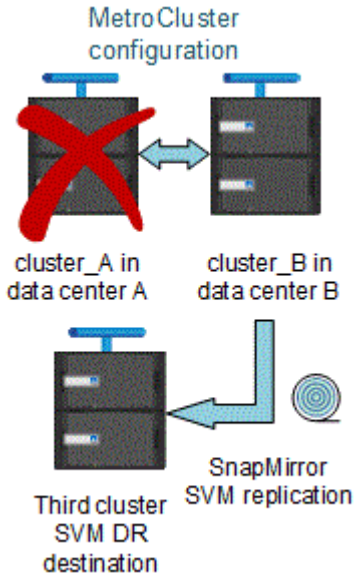
- Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind.

  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.

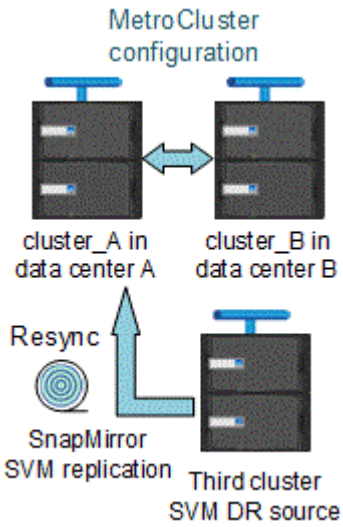
  Nach Abschluss des Switchover- oder Switch-Prozesses werden jedoch die nächsten geplanten SVM-DR-Updates erfolgreich durchgeführt.

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“ in "Installation und Konfiguration von Fabric-Attached MetroCluster".

   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

Installation und Konfiguration von MetroCluster Tiebreaker

Was ist neu

Jede Version enthält Erweiterungen der MetroCluster Tiebreaker Software. Die aktuellen Versionen von MetroCluster Tiebreak enthalten alle Neuigkeiten.

Vorgestellt Werden

ONTAP Tiebreaker Version	Vorgestellt Werden
1.6P1	• Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.6	• Einfachere Installation • Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.5	• Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.4	• Aktualisierung der unterstützenden Bibliotheken

OS Support-Matrix

Die folgende Tabelle zeigt die unterstützten Betriebssysteme für die einzelnen Versionen von Tiebreaker.

Betriebssystem für Tiebreaker	1.6P1	1.6	1.5	1.4
Rocky Linux 9.4	Ja.	Nein	Nein	Nein
Rocky Linux 9.0	Nein	Ja.	Nein	Nein
Rocky Linux 8.10	Ja.	Nein	Nein	Nein
Red Hat Enterprise Linux (RHEL) 9.5	Ja.	Nein	Nein	Nein
RHEL 9.4	Ja.	Nein	Nein	Nein
RHEL 9.3	Nein	Nein	Nein	Nein

RHEL 9.2	Ja.	Ja.	Nein	Nein
RHEL 9.1	Nein	Ja.	Nein	Nein
RHEL 9.0	Nein	Ja.	Nein	Nein
RHEL 8.11 – 9.0	Nein	Ja.	Nein	Nein
RHEL 8.10	Ja.	Ja.	Nein	Nein
RHEL 8.9	Nein	Ja.	Nein	Nein
RHEL 8.8	Ja.	Ja.	Nein	Nein
RHEL 8.1 – 8.7	Nein	Ja.	Ja.	Ja.
RHEL 7 – 7.9	Nein	Nein	Nein	Ja.
CentOS 7 - 7.9	Nein	Nein	Nein	Ja.

Überblick über die Tiebreaker Software

Es ist hilfreich zu verstehen, was die NetApp MetroCluster Tiebreaker Software ist und wie sie zwischen verschiedenen Arten von Fehlern unterscheidet, sodass Sie Ihre MetroCluster Konfigurationen effizient überwachen können. Mit der Tiebreaker CLI können Einstellungen gemanagt und der Status und der Betrieb der MetroCluster Konfigurationen überwacht werden.

Erkennen von Ausfällen mit der NetApp MetroCluster Tiebreaker Software

Sie benötigen die Tiebreaker Software nur, wenn zwei Cluster und der Konnektivitätsstatus zwischen ihnen von einem dritten Standort aus überwacht werden soll. Die Tiebreaker Software befindet sich auf einem Linux Host am dritten Standort, sodass jeder Partner in einem Cluster bei einem Standortausfall zwischen einem ISL-Ausfall und einem Standortausfall unterscheiden kann.

Nachdem Sie die Tiebreaker Software auf einem Linux-Host installiert haben, können Sie die Cluster in einer MetroCluster-Konfiguration konfigurieren, um auf Notfälle zu überwachen.

Die Tiebreaker Software überwacht bis zu 15 MetroCluster Konfigurationen gleichzeitig. Die Lösung unterstützt eine Kombination aus MetroCluster IP, MetroCluster FC und Stretch MetroCluster Konfigurationen.

Wie die Tiebreaker Software Standortausfällen erkennt

Die NetApp MetroCluster Tiebreaker Software überprüft die Erreichbarkeit der Nodes in einer MetroCluster Konfiguration und des Clusters, um zu ermitteln, ob ein Standortausfall aufgetreten ist. Über die Tiebreaker Software wird auch unter bestimmten Bedingungen eine Warnmeldung ausgelöst.

Komponenten, die über die Tiebreaker Software überwacht werden

Die Tiebreaker Software überwacht jeden Controller in der MetroCluster-Konfiguration, indem redundante Verbindungen über mehrere Pfade zu einer Node-Management-LIF und zur Cluster-Management-LIF erstellt werden, die beide im IP-Netzwerk gehostet werden.

Die Tiebreaker Software überwacht folgende Komponenten in der MetroCluster Konfiguration:

- Nodes über lokale Node-Schnittstellen
- Ein Cluster über die vom Cluster vorgegebenen Schnittstellen durchführen
- Überlebendes Cluster, um zu ermitteln, ob Verbindung zum Disaster-Standort vorhanden ist (NV Interconnect, Storage und Cluster-Peering)

Wenn es einen Verlust der Verbindung zwischen der Tiebreaker Software und allen Nodes im Cluster und dem Cluster selbst gibt, wird das Cluster durch die Tiebreaker Software als „`nicht erreichbar`“ deklariert. Es dauert etwa drei bis fünf Sekunden, einen Verbindungsfehler zu erkennen. Wenn ein Cluster über die Tiebreaker Software nicht erreichbar ist, muss das verbleibende Cluster (das Cluster, das noch erreichbar ist) angeben, dass alle Links zum Partner-Cluster getrennt werden, bevor die Tiebreaker Software eine Meldung auslöst.

> Alle Links werden getrennt, wenn das verbliebene Cluster nicht mehr über FC (NV Interconnect und Storage) und Intercluster-Peering mit dem Cluster am Disaster-Standort kommunizieren kann.

Ausfallszenarien, während denen Tiebreaker Software eine Warnmeldung auslöst

Die Tiebreaker Software löst eine Warnmeldung aus, wenn das Cluster (alle Nodes) an der Disaster-Site ausgefallen ist oder nicht erreichbar ist und das Cluster auf der überlebenden Site den Status „`AllLinksSevered`“ anzeigt.

Die Tiebreaker Software löst keine Warnmeldung (oder der Alarm wird über ein Vetos ausgelöst) in den folgenden Szenarien aus:

- Wenn in einer MetroCluster Konfiguration mit acht Nodes ein HA-Paar am Disaster-Standort ausfällt
- In einem Cluster, in dem alle Knoten am Katastrophenstandort ausgefallen sind, ein HA-Paar an der überlebenden Site unten und das Cluster auf der überlebenden Site zeigt den Status „`AllLinksSevered`“ an

  Die Tiebreaker Software löst eine Warnmeldung aus, jedoch vetoes ONTAP diese Warnmeldung aus. In dieser Situation ist auch ein manuelles Switchover vetoed vetoed

- In jedem Szenario, in dem die Tiebreaker Software mindestens einen Node oder die Cluster-Schnittstelle am Disaster-Standort erreichen kann, kann der verbleibende Standort über FC (NV Interconnect und Storage) oder Intercluster Peering einen Node am Disaster-Standort erreichen

Verwandte Informationen

"Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

So erkennt die Tiebreaker Software Konnektivitätsausfälle zwischen Standorten

Die MetroCluster Tiebreaker Software benachrichtigt Sie, wenn alle Verbindungen zwischen den Standorten verloren gehen.

Arten von Netzwerkpfaden

Je nach Konfiguration gibt es drei Typen von Netzwerkpfaden zwischen den beiden Clustern in einer MetroCluster Konfiguration:

- **FC-Netzwerk (in Fabric-Attached MetroCluster-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten FC Switch Fabrics. Jede Switch-Fabric verfügt über zwei FC-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei FC-Switches, eine von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige FC-Switches (NV Interconnect und FCP Initiator) verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

- **Intercluster Peering-Netzwerk**

  Dieser Netzwerktyp besteht aus einem redundanten IP-Netzwerkpfad zwischen den beiden Clustern. Das Cluster-Peering-Netzwerk bietet die Konnektivität, die zur Spiegelung der Konfiguration der Storage Virtual Machine (SVM) erforderlich ist. Die Konfiguration aller SVMs auf einem Cluster wird vom Partner-Cluster gespiegelt.

- **IP-Netzwerk (in MetroCluster IP-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten IP Switch-Netzwerken. Jedes Netzwerk verfügt über zwei IP-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei IP-Switches, einer von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige FC-Switches verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

Monitoring der Konnektivität zwischen Standorten

Die Tiebreaker Software ruft regelmäßig den Status der Konnektivität zwischen Standorten von den Nodes ab. Wenn die NV-Interconnect-Konnektivität verloren geht und das Intercluster-Peering nicht auf Pings reagiert, gehen die Cluster davon aus, dass die Sites isoliert sind und die Tiebreaker Software eine Warnung mit „`AllLinksSevered`“ auslöst. Wenn ein Cluster den Status „`AllLinksSevered`“ identifiziert und der andere Cluster nicht über das Netzwerk erreichbar ist, löst die Tiebreaker Software eine Warnung mit dem Namen „`disaster`“ aus.

Auswirkungen verschiedener Ausfalltypen auf die Tiebreaker Software-Erkennungszeit

Für eine bessere Disaster Recovery-Planung benötigt die MetroCluster Tiebreaker Software einige Zeit, um einen Ausfall zu erkennen. Diese Zeit ist die “disaster detection time”. Die MetroCluster Tiebreaker Software erkennt den Standortausfall innerhalb von 30 Sekunden nach dem Zwischenfall und löst den Disaster Recovery-Vorgang aus, sodass Sie über den Notfall benachrichtigt werden.

Die Erkennungszeit hängt auch von der Art des Ausfalls ab und kann in einigen Szenarien 30 Sekunden überschreiten, die zumeist als „`Rolling Disasters`“ bekannt sind. Die wichtigsten Arten von Rolling Disaster sind:

- Stromausfall
- Panik
- Anhalten oder Neustarten
- Verlust von FC Switches am Disaster-Standort

Stromausfall

Die Tiebreaker Software löst sofort eine Warnmeldung aus, wenn der Node nicht mehr ausgeführt wird. Bei einem Stromausfall halten alle Verbindungen und Updates, wie Intercluster Peering, NV Interconnect und Mailbox-Festplatte, an. Die Zeit, die zwischen dem Cluster nicht mehr erreichbar war, die Erkennung des Ausfalls und der Auslöser, einschließlich der standardmäßigen Silent Time von 5 Sekunden, sollten 30 Sekunden nicht überschreiten.

Panik

In MetroCluster FC-Konfigurationen löst die Tiebreaker Software eine Warnmeldung aus, wenn die NV-Interconnect-Verbindung zwischen den Standorten ausfällt und der verbleibende Standort den Status „`AllLinksSevered`“ anzeigt. Dies geschieht nur, nachdem der Cordump-Prozess abgeschlossen ist. In diesem Szenario könnte die Zeit, die zwischen dem Cluster nicht mehr erreichbar wurde und der Erkennung eines Ausfalls mehr oder ungefähr der Zeit entsprechen, die für den Cordump-Prozess benötigt wurde. In vielen Fällen beträgt die Erkennungszeit mehr als 30 Sekunden.

Wenn ein Knoten nicht mehr funktioniert, aber keine Datei für den coredump-Prozess generiert, sollte die Erkennungszeit nicht länger als 30 Sekunden sein. In MetroCluster-IP-Konfigurationen stoppt der NV die Kommunikation, und der verbleibende Standort erkennt den coredump-Prozess nicht.

Anhalten oder Neustarten

Die Tiebreaker Software löst eine Warnmeldung nur aus, wenn der Knoten nicht verfügbar ist und die überlebende Seite den Status „`AllLinksSevered`“ anzeigt. Die Zeit, die zwischen dem Cluster, das nicht mehr erreichbar ist, und dem Erkennen eines Ausfalls dauert, könnte länger als 30 Sekunden sein. In diesem Szenario hängt die für die Erkennung eines Notfall benötigte Zeit davon ab, wie lange es dauert, bis die Nodes am Disaster-Standort heruntergefahren werden.

Verlust von FC Switches am Disaster-Standort (Fabric-Attached MetroCluster-Konfiguration)

Die Tiebreaker Software löst eine Warnmeldung aus, wenn ein Node nicht mehr ausgeführt wird. Wenn FC-Switches verloren gehen, versucht der Node, den Pfad zu einer Festplatte für ca. 30 Sekunden wiederherzustellen. Während dieser Zeit reagiert der Node auf das Peering-Netzwerk. Wenn beide FC-Switches ausgefallen sind und der Pfad zu einer Festplatte nicht wiederhergestellt werden kann, verursacht der Node einen MultiDiskFailure-Fehler und stoppt. Die zwischen dem FC-Switch-Ausfall und der Anzahl der Male, die die Nodes MultiDiskFailure-Fehler produzierten, beträgt ca. 30 Sekunden länger. Diese zusätzlichen 30 Sekunden müssen zur Notfallerkennungszeit hinzugefügt werden.

Über die Tiebreaker CLI und die man-Pages

Über die Tiebreaker CLI können Sie die Tiebreaker Software per Remote konfigurieren und die MetroCluster Konfigurationen überwachen.

Die CLI-Eingabeaufforderung wird als NetApp MetroCluster Tiebreaker dargestellt::.

Die man-Pages sind in der CLI verfügbar. Geben Sie dazu den entsprechenden Befehlsnamen an der Eingabeaufforderung ein.

Installation der Tiebreaker Software

Tiebraker Installations-Workflow

Die Tiebreaker Software bietet Monitoring-Funktionen für eine Clustered Storage-Umgebung. Außerdem sendet er SNMP-Benachrichtigungen, wenn Probleme mit der Node-Konnektivität oder im Falle eines Standortnotfalls auftreten.

Informationen zu diesem Workflow

Sie können über diesen Workflow die Tiebreaker Software installieren oder aktualisieren.

1. **"Bereiten Sie sich auf die Installation der Tiebreaker Software vor"**

Vergewissern Sie sich vor der Installation und Konfiguration der Tiebreaker Software, dass Ihr System bestimmte Anforderungen erfüllt.

2. **"Sichern Sie die Installation"**

Bei Konfigurationen mit MetroCluster Tiebreaker 1.5 und höher können Sie das Host-Betriebssystem und die Datenbank sichern und absichern.

3. **"Installieren Sie das Tiebreaker Softwarepaket"**

Führen Sie eine Neuinstallation oder ein Upgrade der Tiebreaker Software durch. Der Installationsvorgang hängt von der Version von Tiebreaker ab, die Sie installieren möchten.

Bereiten Sie sich auf die Installation der Tiebreaker Software vor

Vor der Installation und Konfiguration der Tiebreaker Software sollten Sie überprüfen, ob Ihr System bestimmte Anforderungen erfüllt.

Softwareanforderungen

Je nach der zu installierenden Version von Tiebreaker müssen Sie die folgenden Software-Anforderungen erfüllen.

ONTAP Tiebreaker Version	Unterstützte ONTAP-Versionen	Unterstützte Linux-Versionen	Java/MariaDB-Anforderungen
1.6P1	ONTAP 9.12.1 und höher	Siehe "OS Support Matrix" Entsprechende Details.	Keine. Die Abhängigkeiten werden mit der Installation gebündelt.
1.6	ONTAP 9.12.1 und höher	Siehe "OS Support Matrix" Entsprechende Details.	Keine. Die Abhängigkeiten werden mit der Installation gebündelt.

1.5	ONTAP 9.8 bis ONTAP 9.14.1	• Red hat Enterprise Linux 8.1 bis 8.7	Mit Red hat Enterprise Linux 8.1 bis 8.7: • MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert wird) • OpenJDK 17, 18 oder 19
1.4	ONTAP 9.1 bis ONTAP 9.9.1	• Red hat Enterprise Linux 8.1 bis 8.7 • Red hat Enterprise Linux 7 bis 7.9 • CentOS 7 auf 7.9 64 Bit	Mit CentOS: • MariaDB 5.5.52.x/MySQL Server 5.6x • 4 GB RAM • Öffnen Sie JRE 8 Mit Red hat Enterprise Linux 8.1 bis 8.7: • MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert wird) • JRE 8

Zusätzlichen Anforderungen

Sie müssen die folgenden zusätzlichen Anforderungen kennen:

- Die Tiebreaker Software wird auf einem dritten Standort installiert, wodurch die Software zwischen einem Switch-Link- (ISL)-Fehler (wenn Verbindungen zwischen den Standorten ausgefallen sind) und einem Standortausfall unterscheiden kann. Ihr Host-System muss bestimmte Anforderungen erfüllen, bevor Sie die Tiebreaker Software zur Überwachung der MetroCluster Konfiguration installieren oder aktualisieren können.
- Sie müssen über „Root“-Berechtigungen verfügen, um die MetroCluster Tiebreaker Software und die abhängigen Pakete zu installieren.
- Sie können pro MetroCluster-Konfiguration nur einen MetroCluster Tiebreaker Monitor verwenden, um Konflikte mit mehreren Tiebreaker Monitoren zu vermeiden.
- Wenn Sie die NTP-Quelle (Network Time Protocol) für die Tiebreaker Software auswählen, müssen Sie eine lokale NTP-Quelle verwenden. Die Tiebreaker Software sollte nicht dieselbe Quelle wie die MetroCluster Standorte verwenden, die von der Tiebreaker Software überwacht werden.
- Festplattenkapazität: 8 GB
- Firewall:
  - Direkter Zugriff zum Einrichten von AutoSupport Meldungen
  - SSH (Port 22/TCP), HTTPS (Port 443/TCP) und Ping (ICMP)

Sicherung der Tiebreaker Host- und Datenbankinstallation

Bei Konfigurationen mit MetroCluster Tiebreaker 1.5 und höher können Sie das Host-Betriebssystem und die Datenbank sichern und absichern.

Sichern Sie den Host

Die folgenden Richtlinien zeigen Ihnen, wie Sie den Host sichern, auf dem die Tiebreaker Software installiert ist.

Empfehlungen für das Benutzermanagement

- Beschränken Sie den Zugriff des „root“-Benutzers.
  - Sie können Benutzer verwenden, die über Root-Zugriff verfügen, um die Tiebreaker Software zu installieren und zu verwalten.
  - Sie können Benutzer verwenden, die nicht in der Lage sind, den Root-Zugriff zu erhöhen, um Tiebreaker Software zu verwalten.
  - Während der Installation müssen Sie eine Gruppe namens „mcctbgrp“ erstellen. Der Host-Root-Benutzer und der Benutzer, der während der Installation erstellt wurde, müssen beide Mitglieder sein. Nur Mitglieder dieser Gruppe können die Tiebreaker Software vollständig verwalten.

    > Benutzer, die nicht Mitglied dieser Gruppe sind, können nicht auf die Tiebreaker Software oder CLI zugreifen. Sie können zusätzliche Benutzer auf dem Host erstellen und sie zu Mitgliedern der Gruppe machen. Diese zusätzlichen Mitglieder können die Tiebreaker Software nicht vollständig verwalten. Sie haben Lesezugriff und können keine Monitore hinzufügen, ändern oder löschen.

  - Führen Sie Tiebreaker nicht als Root-Benutzer aus. Verwenden Sie ein dediziertes, nicht privilegiertes Servicekonto, um Tiebreaker auszuführen.
- Ändern Sie die Standard-Community-Zeichenfolge in der Datei „/etc/snmp/snmpd.conf“.
- Minimale Schreibberechtigungen zulassen. Das unprivilegierte Tiebreaker-Dienstkonto sollte keinen Zugriff haben, um seine ausführbare Binärdatei oder Konfigurationsdateien zu überschreiben. Nur Verzeichnisse und Dateien für lokalen Tiebreaker Storage (z. B. für integrierten Back-End Storage) oder Audit-Protokolle sollten vom Tiebreaker Benutzer beschreibbar sein.
- Erlauben Sie anonyme Benutzer nicht.
  - Setzen Sie AllowTcpForwarding auf „Nein“ oder verwenden Sie die Anweisung „Match“, um anonyme Benutzer zu beschränken.

Verwandte Informationen

- "Produktdokumentation zu Red hat Enterprise Linux 8"
- "Produktdokumentation zu Red hat Enterprise Linux 9"
- "Rocky Linux-Produktdokumentation"

Grundlegende Empfehlungen für die Host-Sicherheit

- Verwenden Sie Festplattenverschlüsselung
  - Sie können die Festplattenverschlüsselung aktivieren. Dabei kann es sich um FullDiskEncryption (Hardware) oder Verschlüsselung durch Hostos (Software) oder durch den SVM-Host handeln.
- Deaktivieren Sie nicht verwendete Dienste, die eingehende Verbindungen zulassen. Sie können jeden Dienst deaktivieren, der nicht verwendet wird. Die Tiebreaker Software erfordert keinen Service für eingehende Verbindungen, da alle Verbindungen aus der Tiebreaker Installation abgehend sind. Folgende Dienste können standardmäßig aktiviert und deaktiviert werden:
  - HTTP/HTTPS-Server

- FTP-Server
- Telnet, RSH, rlogin
- NFS-, CIFS- und anderer Protokollzugriff
- RDP (RemoteDesktopProtocol), X11 Server, VNC oder andere Remote-Service-Provider für Desktop-PCs.

> Sie müssen entweder den seriellen Konsolenzugriff (falls unterstützt) oder mindestens ein Protokoll aktivieren, um den Host Remote zu verwalten. Wenn Sie alle Protokolle deaktivieren, benötigen Sie physischen Zugriff auf den Host für die Administration.

- Sicherung des Hosts über FIPS
  - Sie können das Host-Betriebssystem im FIPS-konformen Modus installieren und dann Tiebreaker installieren.

    > OpenJDK 19 überprüft beim Start, ob der Host im FIPS-Modus installiert ist. Es sollten keine manuellen Änderungen erforderlich sein.

  - Wenn Sie den Host sichern, müssen Sie sicherstellen, dass der Host ohne Benutzereingriff starten kann. Wenn ein Benutzereingriff erforderlich ist, ist die Tiebreaker-Funktion möglicherweise nicht verfügbar, wenn der Host unerwartet neu startet. In diesem Fall ist die Tiebreaker-Funktion nur nach dem manuellen Eingriff und nach dem vollständigen Booten des Hosts verfügbar.
- Shell-Befehlsverlauf Deaktivieren.
- Aktualisieren Sie häufig. Tiebreaker wird aktiv weiterentwickelt. Regelmäßige Aktualisierungen sind wichtig, um Sicherheitfixes und alle Änderungen an Standardeinstellungen wie Schlüssellängen oder Chiffre Suites zu integrieren.
- Abonnieren Sie die HashiCorp Announcement Mailing-Liste, um Ankündigungen über neue Versionen zu erhalten, und besuchen Sie das Tiebreaker CHANGELOG, um weitere Informationen über aktuelle Updates für neue Versionen zu erhalten.
- Verwenden Sie die richtigen Dateiberechtigungen. Stellen Sie immer sicher, dass die erforderlichen Berechtigungen auf Dateien angewendet werden, bevor Sie die Tiebreaker Software starten, insbesondere auf Dateien mit vertraulichen Informationen.
- Die Multi-Faktor-Authentifizierung (MFA) erhöht die Sicherheit Ihres Unternehmens, da Administratoren mehr als nur einen Benutzernamen und ein Kennwort verwenden müssen, um sich selbst zu identifizieren. Obwohl wichtig, sind Benutzernamen und Passwörter anfällig für Brute-Force-Angriffe und können von Dritten gestohlen werden.
  - Red hat Enterprise Linux 8 bietet MFA, bei dem Benutzer mehr als eine Information bereitstellen müssen, um sich erfolgreich bei einem Konto oder Linux-Host zu authentifizieren. Die zusätzlichen Informationen können ein Einmalpasswort sein, das per SMS an Ihr Mobiltelefon gesendet wird, oder Anmeldedaten von einer App wie Google Authenticator, Twilio Authy oder FreeOTP.

Verwandte Informationen

- "Produktdokumentation zu Red hat Enterprise Linux 8"
- "Produktdokumentation zu Red hat Enterprise Linux 9"
- "Rocky Linux-Produktdokumentation"

Sichern Sie die Datenbankinstallation

Die folgenden Richtlinien zeigen, wie Sie die MariaDB 10.x Datenbankinstallation sichern und absichern können.

- Beschränken Sie den Zugriff des „root“-Benutzers.
  - Tiebreaker verwendet ein dediziertes Konto. Das Konto und die Tabellen zum Speichern von (Konfigurations-)Daten werden während der Installation von Tiebreaker erstellt. Nur während der Installation ist ein erhöhter Zugriff auf die Datenbank erforderlich.
- Während der Installation sind folgende Zugriffsrechte und Berechtigungen erforderlich:
  - Die Fähigkeit, eine Datenbank und Tabellen zu erstellen
  - Die Fähigkeit, globale Optionen zu erstellen
  - Die Möglichkeit, einen Datenbankbenutzer zu erstellen und das Kennwort festzulegen
  - Die Möglichkeit, den Datenbankbenutzer mit der Datenbank und den Tabellen zu verknüpfen und Zugriffsrechte zuzuweisen

  > Das Benutzerkonto, das Sie während der Tiebreaker-Installation angeben, muss über alle diese Berechtigungen verfügen. Die Verwendung mehrerer Benutzerkonten für die verschiedenen Aufgaben wird nicht unterstützt.

- Verwenden Sie die Verschlüsselung der Datenbank
  - Die Verschlüsselung ruhender Daten wird unterstützt."Weitere Informationen zur Verschlüsselung ruhender Daten"
  - Die aktiven Daten sind nicht verschlüsselt. Die Daten im Flug verwenden eine lokale „SOCKS“-Dateiverbindung.
  - FIPS-Konformität für MariaDB — die FIPS-Konformität der Datenbank muss nicht aktiviert werden. Die Installation des Hosts im FIPS-konformen Modus reicht aus.

    "Weitere Informationen zu MySQL Enterprise Transparent Data Encryption (TDE)"

  > Die Verschlüsselungseinstellungen müssen vor der Installation der Tiebreaker Software aktiviert sein.

Verwandte Informationen

- Benutzerverwaltung der Datenbank

  "Zugriffssteuerung und Account-Management"

- Sichern Sie die Datenbank

  "MySQL Secure gegen Angreifer"

  "Sicherung von MariaDB"

- Sichern Sie die Vault-Installation

  "Produktionshärtung"

Installieren Sie das Tiebreaker Softwarepaket

Wählen Sie den Installationsvorgang aus

Das Tiebreaker Installationsverfahren, das Sie durchführen, hängt von der Version von Tiebreaker ab, die Sie installieren.

Tiebreaker Version	Gehe zu…
Tiebreak 1.6 oder höher	"Tiebreaker 1.6 oder höher installieren"
Tiebreak 1.5	"Installieren Sie Tiebreaker 1.5"
Tiebreak 1.4	"Installieren Sie Tiebreaker 1.4"

Tiebreaker 1.6 oder höher installieren

Führen Sie eine neue Installation oder ein Upgrade auf Tiebreaker 1.6 oder Tiebreaker 1.6P1 auf Ihrem Linux Host-Betriebssystem durch, um die MetroCluster-Konfigurationen zu überwachen.

Über diese Aufgabe

- Auf Ihrem Storage-System muss ONTAP 9.12.1 oder höher ausgeführt werden.
- Sie können MetroCluster Tiebreaker als Benutzer ohne Root installieren, der über ausreichende Administratorrechte verfügt, um die Tiebreaker Installation durchzuführen, Tabellen und Benutzer zu erstellen und das Benutzerpasswort festzulegen.

Installation oder Upgrade auf Tiebreaker 1.6P1

Sie können Tiebreaker 1.6P1 installieren oder auf Tiebreaker 1.6P1 aus Tiebreaker 1.6, 1.5 oder 1.4 aktualisieren.

Schritte

1. Laden Sie die Software MetroCluster Tiebreaker 1.6P1 herunter.

   "MetroCluster Tiebreaker (Downloads) – NetApp Support-Website"

2. Melden Sie sich beim Host als Root-Benutzer an.
3. Wenn Sie ein Upgrade durchführen, überprüfen Sie die Version von Tiebreaker, die Sie ausführen:

   Das folgende Beispiel zeigt Tiebreaker 1.5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Installieren oder aktualisieren Sie die Tiebreaker Software.

Tiebreaker 1.6P1 installieren

Führen Sie die folgenden Schritte für eine Neuinstallation von Tiebreaker 1.6P1 aus.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Starten der Installation:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
```

```
                    Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
```

```
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
restored
```

```
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
```

```
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6P1.
```

Upgrade 1.6 auf 1.6P1

Gehen Sie wie folgt vor, um ein Upgrade der Tiebreaker 1.6 Softwareversion auf Tiebreaker 1.6P1 durchzuführen.

> Nach dem Upgrade auf Tiebreaker 1.6P1 von 1.6 entfernen Sie die vorhandenen Monitore und fügen die MetroCluster-Konfiguration für die Überwachung erneut hinzu.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
NetApp-MetroCluster-Tiebreaker-Software-1.6P1-1.x86_64
Error making API request.

URL: GET
https://127.0.0.1:8200/v1/sys/internal/ui/mounts/mcctb/data/db
Code: 403. Errors:

* permission denied
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.19.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.mail-2.0.1.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
```

```
/


Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
    2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

b. Entfernen Sie die MetroCluster-Konfiguration, und fügen Sie sie erneut hinzu, indem Sie die Schritte in ausführen"Konfigurieren der Tiebreaker Software".

Upgrade 1.5 auf 1.6P1

Gehen Sie wie folgt vor, um ein Upgrade der Tiebreaker 1.5 Softwareversion auf Tiebreaker 1.6P1 durchzuführen.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Upgrade 1.4 auf 1.6P1

Gehen Sie wie folgt vor, um ein Upgrade der Tiebreaker 1.4 Softwareversion auf Tiebreaker 1.6P1 durchzuführen.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6P1
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6P1-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6P1.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Installieren Sie Tiebreaker 1.6 oder führen Sie ein Upgrade durch

Sie können Tiebreaker 1.6 installieren oder ein Upgrade auf Tiebreaker 1.6 über Tiebreaker 1.5 oder 1.4 durchführen.

Schritte

1. Laden Sie die Software MetroCluster Tiebreaker 1.6 herunter.

   "MetroCluster Tiebreaker (Downloads) – NetApp Support-Website"

2. Melden Sie sich beim Host als Root-Benutzer an.
3. Wenn Sie ein Upgrade durchführen, überprüfen Sie die Version von Tiebreaker, die Sie ausführen:

   Das folgende Beispiel zeigt Tiebreaker 1.5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Installieren oder aktualisieren Sie die Tiebreaker Software.

Installieren Sie Tiebreaker 1.6

Führen Sie die folgenden Schritte aus, um Tiebreaker 1.6 neu zu installieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Starten der Installation:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish
to create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
```

```
                    Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
```

```
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities
restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token
generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities
restored
```

```
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
```

```
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-
software.service → /etc/systemd/system/netapp-metrocluster-
tiebreaker-software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6.
```

Upgrade 1.5 auf 1.6

Gehen Sie wie folgt vor, um die Tiebreaker 1.5 Softwareversion auf Tiebreaker 1.6 zu aktualisieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener:
rpc listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
```

```
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing
version history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier
not initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
```

```
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token
generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping
rollback manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping
token key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
```

```
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting
rollback manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities
restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge
collection is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Upgrade 1.4 auf 1.6

Gehen Sie wie folgt vor, um die Tiebreaker 1.4 Softwareversion auf Tiebreaker 1.6 zu aktualisieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

Beispiel

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish
to create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for
admin access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE,
HOME, HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME,
LS_COLORS, MAIL, PATH, PWD, SHELL, SHLVL, SSH_CLIENT,
SSH_CONNECTION, SSH_TTY, STAF_TEMP_DIR, TERM, USER,
VAULT_ADDR, VAULT_TOKEN, XDG_RUNTIME_DIR, XDG_SESSION_ID, _,
vault_Addr, which_declare
```

```
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing
version history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier
not initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
```

```
path=token/ namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token
generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping
rollback manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-
listener.tcp: starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping
token key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully
mounted: type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=identity version="v1.14.0+builtin.vault"
path=identity/ namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully
mounted: type=cubbyhole version="v1.14.0+builtin.vault"
path=cubbyhole/ namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully
mounted: type=token version="v1.14.0+builtin.vault"
path=token/ namespace="ID: root. Path: "
```

```
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting
rollback manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities
restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge
collection is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is
Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
```

```
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-
cli is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable
netapp-metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software
to version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################ [100%]
```

Installieren Sie Tiebreaker 1.5

Konfigurieren Sie den Administratorzugriff auf die ONTAP-API und SSH

Sie können den Administratorzugriff auf ONTAP-API und SSH konfigurieren.

Schritte

1. Erstellen Sie einen Admin-Benutzer mit ONTAP-API-Zugriff: `security login create -user-or -group-name` *`mcctb`* `-application ontapi -authentication-method` *`password`*
2. Erstellen Sie einen Admin-Benutzer mit SSH-Zugriff: `security login create -user-or-group -name` *`mcctb`* `-application` *`ssh`* `-authentication-method` *`password`*
3. Überprüfen Sie, ob die neuen Admin-Benutzer erstellt wurden: `security login show`
4. Wiederholen Sie diese Schritte auf dem Partner-Cluster.

> "Administratorauthentifizierung und RBAC" Ist implementiert.

Installieren Sie MetroCluster Tiebreaker 1.5-Abhängigkeiten

Abhängig von Ihrem Linux-Host-Betriebssystem müssen Sie einen MySQL- oder

MariaDB-Server installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren.

Schritte

1. Installieren Sie JDK
2. Installieren und konfigurieren Sie Vault
3. MySQL oder MariaDB Server installieren:

Wenn der Linux-Host lautet	Dann…
Red hat Enterprise Linux 7/CentOS 7	Installieren Sie MySQL Server 5.5.30 oder höher und 5.6.x-Versionen unter Red hat Enterprise Linux 7 oder CentOS 7
Red Hat Enterprise Linux 8	Installieren Sie den MariaDB-Server unter Red hat Enterprise Linux 8

Installieren Sie JDK

Sie müssen JDK auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren. Tiebreaker 1.5 und höher unterstützt OpenJDK 17, 18 oder 19.

Schritte

1. Melden Sie sich als „root“-Benutzer oder als sudo-Benutzer an, der in den erweiterten Berechtigungsmodus wechseln kann.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Prüfen Sie auf verfügbare JDK-Versionen:

```
yum search openjdk
```

3. Installieren Sie JDK 17,18 oder 19.

   Mit dem folgenden Befehl wird JDK 17 installiert:

```
yum install java-17-openjdk
```

4. Überprüfen Sie die Installation:

```
java -version
```

   Bei einer erfolgreichen Installation wird die folgende Ausgabe angezeigt:

```
openjdk version "17.0.2" 2022-01-18 LTS
OpenJDK Runtime Environment 21.9 (build 17.0.2+8-LTS)
OpenJDK 64-Bit Server VM 21.9 (build 17.0.2+8-LTS, mixed mode, sharing)
```

Installieren und konfigurieren Sie Vault

Wenn Sie den lokalen Vault-Server nicht verwenden möchten oder haben, müssen Sie Vault installieren. Sie können diese Standardanleitung für die Installation von Vault verwenden oder alternative Richtlinien in der Hashicorp-Installationsanleitung nachlesen.

> Wenn sich in Ihrem Netzwerk ein Vault-Server befindet, können Sie den MetroCluster Tiebreaker Host für die Verwendung dieser Vault-Installation konfigurieren. Wenn Sie dies tun, müssen Sie Vault nicht auf dem Host installieren.

Schritte

1. Navigieren Sie zum `/bin` Verzeichnis:

```
[root@mcctb] cd /bin
```

2. Laden Sie die Vault-ZIP-Datei herunter.

```
[root@mcctb /bin]#  curl -sO
https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
```

3. Entpacken Sie die Vault-Datei.

```
[root@mcctb /bin]# unzip vault_1.12.2_linux_amd64.zip
Archive:  vault_1.12.2_linux_amd64.zip
  inflating: vault
```

4. Überprüfen Sie die Installation.

```
[root@mcctb /bin]# vault -version
Vault v1.12.2 (415e1fe3118eebd5df6cb60d13defdc01aa17b03), built 2022-11-
23T12:53:46Z
```

5. Navigieren Sie zum `/root` Verzeichnis:

```
[root@mcctb /bin] cd /root
```

6. Erstellen Sie eine Vault-Konfigurationsdatei unter `/root` Verzeichnis.

   Am `[root@mcctb ~]` Um den zu erstellen, kopieren Sie den folgenden Befehl, und führen Sie ihn aus `config.hcl` Datei:

```
# cat > config.hcl << EOF
 storage "file" {
  address = "127.0.0.1:8500"
  path    = "/mcctb_vdata/data"
 }
 listener "tcp" {
   address     = "127.0.0.1:8200"
   tls_disable = 1
 }
EOF
```

7. Starten Sie den Vault-Server:

```
[root@mcctb ~] vault server -config config.hcl &
```

8. Exportieren Sie die Vault-Adresse.

```
[root@mcctb ~]# export VAULT_ADDR="http://127.0.0.1:8200"
```

9. Vault Initialisieren.

```
[root@mcctb ~]# vault operator init
2022-12-15T14:57:22.113+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.113+0530 [INFO]  core: seal configuration missing,
not initialized
2022-12-15T14:57:22.114+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.116+0530 [INFO]  core: security barrier initialized:
stored=1 shares=5 threshold=3
2022-12-15T14:57:22.118+0530 [INFO]  core: post-unseal setup starting
2022-12-15T14:57:22.137+0530 [INFO]  core: loaded wrapping token key
2022-12-15T14:57:22.137+0530 [INFO]  core: Recorded vault version: vault
version=1.12.2 upgrade time="2022-12-15 09:27:22.137200412 +0000 UTC"
build date=2022-11-23T12:53:46Z
2022-12-15T14:57:22.137+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T14:57:22.137+0530 [INFO]  core: no mounts; adding default
mount table
2022-12-15T14:57:22.143+0530 [INFO]  core: successfully mounted backend:
type=cubbyhole version="" path=cubbyhole/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=system version="" path=sys/
```

```
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=identity version="" path=identity/
2022-12-15T14:57:22.148+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T14:57:22.149+0530 [INFO]  rollback: starting rollback manager
2022-12-15T14:57:22.149+0530 [INFO]  core: restoring leases
2022-12-15T14:57:22.150+0530 [INFO]  expiration: lease restore complete
2022-12-15T14:57:22.150+0530 [INFO]  identity: entities restored
2022-12-15T14:57:22.150+0530 [INFO]  identity: groups restored
2022-12-15T14:57:22.151+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T14:57:23.385+0530 [INFO]  core: post-unseal setup complete
2022-12-15T14:57:23.387+0530 [INFO]  core: root token generated
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown starting
2022-12-15T14:57:23.387+0530 [INFO]  rollback: stopping rollback manager
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown complete
Unseal Key 1: <unseal_key_1_id>
Unseal Key 2: <unseal_key_2_id>
Unseal Key 3: <unseal_key_3_id>
Unseal Key 4: <unseal_key_4_id>
Unseal Key 5: <unseal_key_5_id>

Initial Root Token: <initial_root_token_id>


Vault initialized with 5 key shares and a key threshold of 3. Please
securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to
unseal it
before it can start servicing requests.

Vault does not store the generated root key. Without at least 3 keys to
reconstruct the root key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum
of
existing unseal keys shares. See "vault operator rekey" for more
information.
```

Sie müssen die Schlüssel-IDs und das erste Root-Token an einem sicheren Ort aufzeichnen und speichern, um es später in dem Verfahren verwenden zu können.

10. Exportieren Sie das Vault-Root-Token.

```
[root@mcctb ~]#  export VAULT_TOKEN="<initial_root_token_id>"
```

11. Heben Sie die Versiegelung des Tresors auf, indem Sie drei der fünf erstellten Schlüssel verwenden.

    Sie müssen den ausführen `vault operator unseal` Befehl für jeden der drei Tasten:

    a. Lösen Sie den Tresor mit dem ersten Schlüssel:

    ```
    [root@mcctb ~]# vault operator unseal
    Unseal Key (will be hidden):
    Key                Value
    ---                -----
    Seal Type          shamir
    Initialized        true
    Sealed             true
    Total Shares       5
    Threshold          3
    Unseal Progress    1/3
    Unseal Nonce       <unseal_key_1_id>
    Version            1.12.2
    Build Date         2022-11-23T12:53:46Z
    Storage Type       file
    HA Enabled         false
    ```

    b. Lösen Sie den Tresor mit dem zweiten Schlüssel:

    ```
    [root@mcctb ~]# vault operator unseal
    Unseal Key (will be hidden):
    Key                Value
    ---                -----
    Seal Type          shamir
    Initialized        true
    Sealed             true
    Total Shares       5
    Threshold          3
    Unseal Progress    2/3
    Unseal Nonce       <unseal_key_2_id>
    Version            1.12.2
    Build Date         2022-11-23T12:53:46Z
    Storage Type       file
    HA Enabled         false
    ```

    c. Lösen Sie den Tresor mit dem dritten Schlüssel:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=127.0.0.1:8201
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener: serving
cluster requests: cluster_listen_address=127.0.0.1:8201
2022-12-15T15:15:00.981+0530 [INFO]  core: post-unseal setup starting
2022-12-15T15:15:00.981+0530 [INFO]  core: loaded wrapping token key
2022-12-15T15:15:00.982+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T15:15:00.983+0530 [INFO]  core: successfully mounted
backend: type=system version="" path=sys/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=identity version="" path=identity/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=cubbyhole version="" path=cubbyhole/
2022-12-15T15:15:00.986+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T15:15:00.986+0530 [INFO]  rollback: starting rollback
manager
2022-12-15T15:15:00.987+0530 [INFO]  core: restoring leases
2022-12-15T15:15:00.987+0530 [INFO]  expiration: lease restore
complete
2022-12-15T15:15:00.987+0530 [INFO]  identity: entities restored
2022-12-15T15:15:00.987+0530 [INFO]  identity: groups restored
2022-12-15T15:15:00.988+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T15:15:00.989+0530 [INFO]  core: post-unseal setup complete
2022-12-15T15:15:00.989+0530 [INFO]  core: vault is unsealed
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

12. Vergewissern Sie sich, dass der Status „Vault Sealed“ falsch ist.

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

13. Konfigurieren Sie den Vault-Dienst für den Start beim Booten.
    a. Führen Sie den folgenden Befehl aus: `cd /etc/systemd/system`

    ```
    [root@mcctb ~]#  cd /etc/systemd/system
    ```

    b. Am `[root@mcctb system]` Um die Vault-Dienstdatei zu erstellen, kopieren Sie den folgenden Befehl, und führen Sie ihn aus.

    ```
    # cat > vault.service << EOF
    [Unit]
    Description=Vault Service
    After=mariadb.service

    [Service]
    Type=forking
    ExecStart=/usr/bin/vault server -config /root/config.hcl &
    Restart=on-failure

    [Install]
    WantedBy=multi-user.target
    EOF
    ```

    c. Führen Sie den folgenden Befehl aus: `systemctl daemon-reload`

    ```
    [root@mcctb system]#  systemctl daemon-reload
    ```

    d. Führen Sie den folgenden Befehl aus: `systemctl enable vault.service`

```
[root@mcctb system]#  systemctl enable vault.service
Created symlink /etc/systemd/system/multi-
user.target.wants/vault.service → /etc/systemd/system/vault.service.
```

Sie werden während der Installation von MetroCluster Tiebreaker aufgefordert, diese Funktion zu verwenden. Wenn Sie die Methode zum Entsiegeln von Tresor ändern möchten, müssen Sie die MetroCluster Tiebreaker Software deinstallieren und neu installieren.

Installieren Sie MySQL Server 5.5.30 oder höher und 5.6.x-Versionen unter Red hat Enterprise Linux 7 oder CentOS 7

Sie müssen MySQL Server 5.5.30 oder höher und 5.6.x-Version auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker-Software installieren oder aktualisieren. Für Red Hat Enterprise Linux 8 Installieren Sie den MariaDB-Server.

Schritte

1. Melden Sie sich als Root-Benutzer oder sudo-Benutzer an, der in den erweiterten Berechtigungsmodus wechseln kann.

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
   ```

2. Fügen Sie das MySQL-Repository zum Host-System hinzu:

   ```
   [root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
   release-el6-11.noarch.rpm
   ```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
========
Package               Arch   Version
                                     Repository
Size
=============================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
=============================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Deaktivieren Sie das MySQL 57-Repository:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Aktivieren Sie das MySQL 56-Repository:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Repository aktivieren:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Installieren Sie den MySQL Community Server:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
======
Package                          Arch   Version       Repository
Size
=============================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
=================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ---------------------------------------------------------------------------
--------
Total                                               289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. MySQL-Server starten:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Bestätigen Sie, dass MySQL-Server ausgeführt wird:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                          hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Überprüfen Sie, ob die MySQL-Anmeldung funktioniert:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Wenn der MySQL-Login funktioniert, endet die Ausgabe am `mysql>` Eingabeaufforderung:

Aktivieren Sie die Einstellung MySQL Autostart

Sie sollten überprüfen, ob die Autostart-Funktion für den MySQL-Daemon aktiviert ist. Durch Aktivieren des MySQL-Daemon wird MySQL automatisch neu gestartet, wenn das System, auf dem die MetroCluster Tiebreaker Software ausgeführt wird, neu gestartet wird. Wenn der MySQL-Daemon nicht ausgeführt wird, wird die Tiebreaker-Software weiterhin ausgeführt, kann aber nicht neu gestartet werden und

Konfigurationsänderungen können nicht vorgenommen werden.

Schritt

1. Vergewissern Sie sich, dass MySQL beim Starten automatisch gestartet wird:

   ```
   [root@mcctb ~]# systemctl list-unit-files mysqld.service
   ```

   ```
   UNIT FILE          State
   ------------------ ----------
   mysqld.service     enabled
   ```

   Wenn MySQL beim Starten nicht aktiviert ist, lesen Sie die MySQL-Dokumentation, um die Autostart-Funktion für Ihre Installation zu aktivieren.

Installieren Sie den MariaDB-Server unter Red hat Enterprise Linux 8

Sie müssen MariaDB Server auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren. Für Red hat Enterprise Linux 7 oder CentOS 7, Installieren Sie MySQL Server.

Bevor Sie beginnen

Ihr Hostsystem muss unter Red hat Enterprise Linux (RHEL) 8 ausgeführt werden.

Schritte

1. Melden Sie sich als an `root` Benutzer oder ein Benutzer, der in den erweiterten Berechtigungsmodus wechseln kann.

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
   ```

2. Installieren Sie den MariaDB-Server:

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   ```

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
    ...
    ...

   ================================================================================
    Package                      Arch   Version         Repository
   Size
   ================================================================================
   Installing:
   ```

```
mariadb-server               x86_64   1:5.5.56-2.el7   base
11 M
Installing for dependencies:

Transaction Summary
=========================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
-------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. MariaDB-Server starten:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Überprüfen Sie, ob der MariaDB-Server gestartet wurde:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

> Wenn Sie zur Eingabe des Root-Passworts aufgefordert werden, lassen Sie es leer, und drücken Sie die EINGABETASTE, um mit der Konfiguration der Sicherheits- und Kennworteinstellungen fortzufahren.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
```

```
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Aktivieren Sie die Autostart-Einstellung für den MariaDB-Server

Überprüfen Sie, ob die Autostart-Funktion für den MariaDB-Server aktiviert ist. Wenn Sie die Autostart-Funktion nicht aktivieren und das System, auf dem sich die MetroCluster Tiebreaker Software befindet, neu gestartet werden muss, wird die Tiebreaker Software ausgeführt, der MariaDB-Service kann jedoch nicht neu gestartet werden und Konfigurationsänderungen können nicht vorgenommen werden.

Schritte

1. Aktivieren des Autostart-Dienstes:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Vergewissern Sie sich, dass MariaDB beim Starten automatisch gestartet wird:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Installieren Sie Tiebreaker 1.5 oder führen Sie ein Upgrade durch

Führen Sie eine Neuinstallation oder ein Upgrade auf Tiebreaker 1.5 auf Ihrem Linux-Host-Betriebssystem durch, um die MetroCluster-Konfigurationen zu überwachen.

Über diese Aufgabe

- Auf Ihrem Storage-System muss eine unterstützte Version von ONTAP ausgeführt werden. Siehe "Softwareanforderungen" Tabelle für weitere Details.
- Sie müssen OpenJDK mithilfe der installiert haben `yum install java-x.x.x-openjdk` Befehl. Tiebreaker 1.5 und höher unterstützt OpenJDK 17, 18 oder 19.
- Sie können MetroCluster Tiebreaker als Benutzer ohne Root installieren, der über ausreichende Administratorrechte verfügt, um die Tiebreaker Installation durchzuführen, Tabellen und Benutzer zu erstellen und das Benutzerpasswort festzulegen.

Schritte

1. Laden Sie die MetroCluster Tiebreaker Software und den Schlüssel MetroCluster_Tiebreaker_RPM_GPG herunter.

   > Der Schlüssel „MetroCluster_Tiebreaker_RPM_GPG“ kann über dieselbe Seite heruntergeladen werden, die Sie auch das Software-Paket für Tiebreaker 1.5 auf der NetApp Support-Website herunterladen.

   "MetroCluster Tiebreaker (Downloads) – NetApp Support-Website"

2. Melden Sie sich beim Host als Root-Benutzer an.
3. Erstellen Sie einen Benutzer, der kein Root-Benutzer ist, und den `mcctbgrp` Gruppieren.

   a. Erstellen Sie einen Benutzer, der kein Root-Benutzer ist, und legen Sie das Passwort fest.

      Mit den folgenden Beispielbefehlen wird ein nicht-root-Benutzer mit dem Namen erstellt `mcctbuser1`:

```
[root@mcctb ~]# useradd mcctbuser1
[root@mcctb ~]# passwd mcctbuser1
Changing password for user mcctbuser1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

b. Erstellen Sie eine Gruppe mit dem Namen `mcctbgrp`:

```
[root@mcctb ~~]# groupadd mcctbgrp
```

c. Fügen Sie den nicht-Root-Benutzer, den Sie erstellt haben, zum hinzu `mcctbgrp` Gruppieren.

Mit dem folgenden Befehl wird hinzugefügt `mcctbuser1` Bis zum `mcctbgrp` Gruppe:

```
[root@mcctb ~]# usermod -a -G mcctbgrp mcctbuser1
```

4. Überprüfen Sie die RPM-Datei.

Führen Sie die folgenden Teilschritte aus dem Verzeichnis mit dem RPM-Schlüssel aus.

a. Laden Sie die RPM-Schlüsseldatei herunter, und importieren Sie sie:

```
[root@mcctb ~]# rpm --import MetroCluster_Tiebreaker_RPM_GPG.key
```

b. Überprüfen Sie, ob der richtige Schlüssel importiert wurde, indem Sie den Fingerabdruck überprüfen.

Das folgende Beispiel zeigt einen korrekten Schlüsselfinger:

```
root@mcctb:~/signing/mcctb-rpms# gpg --show-keys --with-fingerprint
MetroCluster_Tiebreaker_RPM_GPG.key
pub   rsa3072 2022-11-17 [SCEA] [expires: 2025-11-16]
      65AC 1562 E28A 1497 7BBD  7251 2855 EB02 3E77 FAE5
uid                      MCCTB-RPM (mcctb RPM production signing)
<mcctb-rpm@netapp.com>
```

a. Überprüfen Sie die Signatur: `rpm --checksig NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

```
NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm: digests OK
```

> Sie dürfen mit der Installation erst fortfahren, nachdem Sie die Signatur erfolgreich verifiziert haben.

5. Installieren oder aktualisieren Sie die Tiebreaker Software:

> Ein Upgrade auf Tiebreaker Version 1.5 ist nur möglich, wenn Sie ein Upgrade von Tiebreaker Version 1.4 durchführen. Ein Upgrade von früheren Versionen auf Tiebreaker 1.5 wird nicht unterstützt.

Wählen Sie das richtige Verfahren aus, je nachdem, ob Sie eine neue Installation durchführen oder eine vorhandene Installation aktualisieren.

Führen Sie eine neue Installation durch

a. Abrufen und Aufzeichnen des absoluten Pfads für Java:

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Führen Sie den folgenden Befehl aus:
`rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

> Wenn Sie während der Installation dazu aufgefordert werden, geben Sie den nicht-Root-Benutzer an, den Sie zuvor erstellt und dem zugewiesen haben `mcctbgrp` Gruppieren.

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Enter database user name:
root
Please enter database password for root
Enter password:
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.5.
```

Aktualisierung einer vorhandenen Installation

a. Überprüfen Sie, ob eine unterstützte Version von OpenJDK installiert ist und die aktuelle Java-Version auf dem Host ist.

> Für Upgrades auf Tiebreaker 1.5 müssen Sie entweder OpenJDK Version 17, 18 oder 19 installieren.

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Überprüfen Sie, ob der Vault-Dienst entsiegelt ist und ausgeführt wird: `vault status`

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault
Cluster ID      <cluster_id>
HA Enabled      false
```

c. Upgrade der Tiebreaker Software

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.5-1.x86_64.rpm
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]

Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Enter database user name : root
Please enter database password for root
Enter password:
Password updated successfully in the database.
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.5.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

> Wenn Sie das falsche MySQL-Root-Passwort eingeben, zeigt die Tiebreaker Software an, dass sie erfolgreich installiert wurde, zeigt aber „Access Denied“-Meldungen an. Um das Problem zu lösen, müssen Sie die Tiebreaker Software mit verwenden `rpm -e` Führen Sie einen Befehl aus, und installieren Sie dann die Software mit dem richtigen MySQL-Root-Passwort neu.

6. Prüfen Sie die Tiebreaker Konnektivität zur MetroCluster Software, indem Sie über den Tiebreaker Host eine SSH-Verbindung zu jedem Node-Management-LIFs und Cluster-Management-LIFs öffnen.

Verwandte Informationen

"NetApp Support"

Installieren Sie Tiebreaker 1.4

Installieren Sie MetroCluster Tiebreaker 1.4-Abhängigkeiten

Installieren Sie je nach Linux-Betriebssystem einen MySQL- oder MariaDB-Server, bevor Sie die Tiebreaker Software installieren oder aktualisieren.

Schritte

1. Installieren Sie JDK.
2. MySQL oder MariaDB Server installieren:

Wenn der Linux-Host lautet	Dann…
Red hat Enterprise Linux 7/CentOS 7	Installieren Sie MySQL Server 5.5.30 oder höher und 5.6.x-Versionen unter Red hat Enterprise Linux 7 oder CentOS 7
Red Hat Enterprise Linux 8	Installieren Sie den MariaDB-Server unter Red hat Enterprise Linux 8

Installieren Sie JDK

Sie müssen JDK auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren. Tiebreaker 1.4 und frühere Versionen unterstützen JDK 1.8.0. (JRE 8).

Schritte

1. Melden Sie sich als „root“-Benutzer an.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Installieren Sie JDK 1.8.0:

```
yum install java-1.8.0-openjdk.x86_64
```

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

=================================================================================
Package                Arch   Version                  Repository    Size
=================================================================================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4 updates      238 k
 ..
 ..
Transaction Summary
=================================================================================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Installieren Sie MySQL Server 5.5.30 oder höher und 5.6.x-Versionen unter Red hat Enterprise Linux 7 oder CentOS 7

Sie müssen MySQL Server 5.5.30 oder höher und 5.6.x-Version auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker-Software installieren oder aktualisieren. Für Red Hat Enterprise Linux 8 Installieren Sie den MariaDB-Server.

Schritte

1. Melden Sie sich als Root-Benutzer an.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Fügen Sie das MySQL-Repository zum Host-System hinzu:

```
[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
========
Package               Arch   Version
                                     Repository
Size
=============================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
=============================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Deaktivieren Sie das MySQL 57-Repository:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Aktivieren Sie das MySQL 56-Repository:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Repository aktivieren:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Installieren Sie den MySQL Community Server:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
======
Package                          Arch   Version       Repository
Size
=============================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
=================================================================================
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ---------------------------------------------------------------------------
--------
Total                                               289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. MySQL-Server starten:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Bestätigen Sie, dass MySQL-Server ausgeführt wird:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                          hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Überprüfen Sie, ob die MySQL-Anmeldung funktioniert:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Wenn die MySQL-Anmeldung wie erwartet funktioniert, endet die Ausgabe am `mysql>` Eingabeaufforderung:

Aktivieren Sie die Einstellung MySQL Autostart

Sie sollten überprüfen, ob die Autostart-Funktion für den MySQL-Daemon aktiviert ist. Durch Aktivieren des MySQL-Daemon wird MySQL automatisch neu gestartet, wenn das System, auf dem die MetroCluster Tiebreaker Software ausgeführt wird, neu gestartet wird. Wenn der MySQL-Daemon nicht ausgeführt wird, wird

die Tiebreaker-Software weiterhin ausgeführt, kann aber nicht neu gestartet werden und Konfigurationsänderungen können nicht vorgenommen werden.

Schritt

1. Vergewissern Sie sich, dass MySQL beim Starten automatisch gestartet wird:

   `[root@mcctb ~]# systemctl list-unit-files mysqld.service`

   ```
   UNIT FILE           State
   ------------------ ----------
   mysqld.service      enabled
   ```

   Wenn MySQL beim Starten nicht aktiviert ist, lesen Sie die MySQL-Dokumentation, um die Autostart-Funktion für Ihre Installation zu aktivieren.

Installieren Sie den MariaDB-Server unter Red hat Enterprise Linux 8

Sie müssen MariaDB Server auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren. Für Red hat Enterprise Linux 7 oder CentOS 7, Installieren Sie MySQL Server.

Bevor Sie beginnen

Ihr Hostsystem muss unter Red hat Enterprise Linux (RHEL) 8 ausgeführt werden.

Schritte

1. Melden Sie sich als an `root` Benutzer:

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
   ```

2. Installieren Sie den MariaDB-Server:

   `[root@mcctb ~]# yum install mariadb-server.x86_64`

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
    ...
    ...

   ==========================================================================
   ===
    Package                      Arch   Version         Repository
   Size
   ==========================================================================
   ===
   Installing:
   ```

```
mariadb-server               x86_64   1:5.5.56-2.el7   base
11 M
Installing for dependencies:

Transaction Summary
=================================================================================
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
---------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. MariaDB-Server starten:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Überprüfen Sie, ob der MariaDB-Server gestartet wurde:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

> Wenn Sie zur Eingabe des Root-Passworts aufgefordert werden, lassen Sie es leer, und drücken Sie die EINGABETASTE, um mit der Konfiguration der Sicherheits- und Kennworteinstellungen fortzufahren.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
```

```
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

  ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Aktivieren Sie die Autostart-Einstellung für den MariaDB-Server

Überprüfen Sie, ob die Autostart-Funktion für den MariaDB-Server aktiviert ist. Wenn Sie die Autostart-Funktion nicht aktivieren und das System, auf dem sich die MetroCluster Tiebreaker Software befindet, neu gestartet werden muss, wird die Tiebreaker Software ausgeführt, der MariaDB-Service kann jedoch nicht neu gestartet werden und Konfigurationsänderungen können nicht vorgenommen werden.

Schritte

1. Aktivieren des Autostart-Dienstes:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Vergewissern Sie sich, dass MariaDB beim Starten automatisch gestartet wird:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Installieren Sie Tiebreaker 1.4 oder führen Sie ein Upgrade durch

Führen Sie eine Neuinstallation oder ein Upgrade auf Tiebreaker 1.4 auf Ihrem Linux-Host-Betriebssystem durch, um die MetroCluster-Konfigurationen zu überwachen.

Über diese Aufgabe

- Auf Ihrem Storage-System muss eine unterstützte Version von ONTAP ausgeführt werden. Siehe "Softwareanforderungen" Tabelle für weitere Details.
- Sie müssen OpenJDK mithilfe der installiert haben `yum install java-x.x.x-openjdk` Befehl. Tiebreaker 1.4 und frühere Versionen unterstützen JDK 1.8.0 (JRE 8).

Schritte

1. Laden Sie die MetroCluster Tiebreaker Software herunter.

   "MetroCluster Tiebreaker (Downloads) – NetApp Support-Website"

2. Melden Sie sich beim Host als Root-Benutzer an.
3. Installieren oder aktualisieren Sie die Tiebreaker Software:

   Wählen Sie das richtige Verfahren aus, je nachdem, ob Sie eine neue Installation durchführen oder eine vorhandene Installation aktualisieren.

Führen Sie eine neue Installation durch

a. Installieren Sie die Tiebreaker-Software, indem Sie die folgende ausführen:

```
rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.4-1.x86_64.rpm
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Post installation start Fri Apr  5 02:28:09 EDT 2024
Enter MetroCluster Tiebreaker user password:

Please enter mysql root password when prompted
Enter password:
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post installation end Fri Apr  5 02:28:22 EDT 2024
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.4.
```

Aktualisieren einer vorhandenen Installation

a. Upgrade der Tiebreaker Software

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.4-1.x86_64.rpm
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Upgrading NetApp MetroCluster Tiebreaker software....
Stopping NetApp MetroCluster Tiebreaker software services before
upgrade.
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Post installation start Mon Apr  8 06:29:51 EDT 2024
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post upgrade end Mon Apr  8 06:29:51 EDT 2024
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.4.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

> Wenn Sie das falsche MySQL-Root-Passwort eingeben, zeigt die Tiebreaker Software an, dass sie erfolgreich installiert wurde, zeigt aber „Access Denied“-Meldungen an. Um das Problem zu lösen, müssen Sie die Tiebreaker Software mit verwenden `rpm -e` Führen Sie einen Befehl aus, und installieren Sie dann die Software mit dem richtigen MySQL-Root-Passwort neu.

4. Prüfen Sie die Tiebreaker Konnektivität zur MetroCluster Software, indem Sie über den Tiebreaker Host eine SSH-Verbindung zu jedem Node-Management-LIFs und Cluster-Management-LIFs öffnen.

Verwandte Informationen

"NetApp Support"

Aktualisieren Sie den Host, auf dem der Tiebreaker Monitor ausgeführt wird

Unter Umständen müssen Sie den Host aktualisieren, auf dem der Tiebreaker Monitor ausgeführt wird.

Schritte

1. Deinstallieren Sie die Tiebreaker Software:

   ```
   rpm -e NetApp-MetroCluster-Tiebreaker-Software
   ```

2. Aktualisieren Sie den Host. Weitere Informationen finden Sie in der Dokumentation zum Host-Betriebssystem.
3. Installieren Sie die Tiebreaker Software neu.

   Führen Sie eine Neuinstallation von Tiebreaker durch, indem Sie die unter beschriebenen Schritte ausführen "Installation der Tiebreaker Software".

Konfigurieren der Tiebreaker Software

Nach der Installation der Tiebreaker Software können MetroCluster Konfigurationen hinzugefügt oder geändert oder aus der Tiebreaker Software entfernt werden.

Starten der Tiebreaker Software-CLI

Nach der Installation der Tiebreaker Software müssen Sie die CLI starten, um die Software zu konfigurieren.

1. Starten Sie die CLI von der Eingabeaufforderung des Hosts, auf dem Sie die Software installiert haben:

   ```
   netapp-metrocluster-tiebreaker-software-cli
   ```

2. Geben Sie nach der Installation und während des ersten Startvorgangs das Kennwort für den Tiebreaker-Benutzer ein, um auf die Datenbank zuzugreifen. Dies ist das Kennwort, das Sie während der Installation für den Datenbankbenutzer angegeben haben.

Hinzufügen von MetroCluster Konfigurationen

Nach der Installation der NetApp MetroCluster Tiebreaker Software können mehrere MetroCluster Konfigurationen gleichzeitig hinzugefügt werden.

Sie müssen die MetroCluster-Konfiguration in einer ONTAP-Umgebung installiert und die Einstellungen in der Software aktiviert haben.

1. Über die Tiebreaker Befehlszeilenschnittstelle (CLI) können Sie mit dem Hinzufügungs-Befehl MetroCluster-Konfigurationen hinzufügen.

   Wenn Sie den Hostnamen verwenden, muss dieser der vollständig qualifizierte Domänenname (FQDN)

sein.

Im folgenden Beispiel wird die Konfiguration von Cluster_A gezeigt:

```
NetApp MetroCluster Tiebreaker :> monitor add wizard
Enter monitor Name: cluster_A
Enter Cluster IP Address: 10.222.196.130
Enter Cluster Username: admin
Enter Cluster Password:
Enter Peer Cluster IP Address: 10.222.196.40
Enter Peer Cluster Username: admin
Enter Peer Cluster Password:
Successfully added monitor to NetApp MetroCluster Tiebreaker software.
```

2. Überprüfen Sie, ob die MetroCluster-Konfiguration ordnungsgemäß mit der Tiebreaker CLI hinzugefügt wurde `monitor show -status` Befehl.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

3. Deaktivieren Sie den Observer-Modus für die Tiebreaker-Software, um eine Umschaltung automatisch zu starten, nachdem ein Standortfehler erkannt wurde:

   `monitor modify -monitor-name monitor_name -observer-mode false`

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
-observer-mode false
Warning: If you are turning observer-mode to false, make sure to review
the 'risks and limitations'
as described in the MetroCluster Tiebreaker installation and
configuration.
Are you sure you want to enable automatic switchover capability for
monitor "8pack"? [Y/N]: y
```

Verwandte Informationen

"Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

Befehle zum Ändern von MetroCluster Tiebreaker Konfigurationen

Sie können die MetroCluster-Konfiguration jederzeit ändern, wenn Sie die Einstellungen ändern möchten.

Der Tiebreaker CLI-Monitor-Änderungsbefehl kann mit einer der folgenden Optionen verwendet werden. Mit dem Befehl Monitor show -Status können Sie Ihre Änderungen bestätigen.

Option	Beschreibung

-Monitor-Name	Name der MetroCluster-Konfiguration
-Monitor aktivieren	Aktiviert und deaktiviert die Überwachung der MetroCluster-Konfiguration
-Stumm-Periode	Zeitraum in Sekunden, für die die MetroCluster Tiebreaker Software nach der Erkennung einen Standortausfall bestätigt
-Observer-Modus	Der Observer-Modus (True) bietet nur Überwachung und löst bei einem Standortunfall keine Umschaltung aus. Der Online-Modus (false) löst bei einem Standortausfall eine Umschaltung aus. • "Wie die Tiebreaker Software Standortausfällen erkennt" • "Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

Im folgenden Beispiel wird der Silent Period für die Konfiguration geändert.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

Über die Tiebreaker CLI `debug` Mit dem Befehl kann der Protokollierungsmodus geändert werden.

Befehl	Beschreibung
Debug-Status	Zeigt den Status des Debug-Modus an
Debug aktivieren	Aktiviert den Debug-Modus für die Protokollierung
Debug deaktivieren	Deaktiviert den Debug-Modus für die Protokollierung

Bei Systemen mit Tiebreaker 1.4 und älteren Versionen bietet die Tiebreaker CLI `update-mcctb-password` Mit dem Befehl kann das Benutzerpasswort aktualisiert werden. Dieser Befehl ist in Tiebreak 1.5 und höher veraltet.

Befehl	Beschreibung
Update-mcctb-password	Das Benutzerpasswort wurde erfolgreich aktualisiert

Entfernen von MetroCluster-Konfigurationen

Sie können die MetroCluster-Konfiguration entfernen, die von der Tiebreaker Software überwacht wird, wenn Sie keine MetroCluster-Konfiguration mehr überwachen möchten.

1. Verwenden Sie die Tiebreaker CLI `monitor remove` Befehl zum Entfernen der MetroCluster-

Konfiguration.

Im folgenden Beispiel wird „`Cluster_A`“ aus der Software entfernt:

```
NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
Successfully removed monitor from NetApp MetroCluster Tiebreaker
software.
```

2. Überprüfen Sie, ob die MetroCluster-Konfiguration ordnungsgemäß mithilfe der Tiebreaker CLI entfernt wird `monitor show -status` Befehl.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

Konfigurieren von SNMP-Einstellungen für Tiebreaker Software

Um SNMP mit der Tiebreaker Software verwenden zu können, müssen Sie die SNMP-Einstellungen konfigurieren.

Über diese Aufgabe

- Tiebreaker 1.6 unterstützt nur SNMPv3.
- Obwohl Tiebreaker 1.5 und 1.4 SNMPv1 und SNMPv3 unterstützen, empfiehlt NetApp dringend, SNMPv3 für optimale Sicherheit zu konfigurieren.

Schritte

1. Verwenden Sie die Tiebreaker CLI `snmp config wizard` Befehl zum Hinzufügen von MetroCluster-Konfigurationen.

   Derzeit wird nur ein SNMP-Trap-Host unterstützt.

   Die `snmp config wizard` Antwort auf die Befehle hängt von der Version von Tiebreaker ab, die Sie ausführen.

Tiebreak 1.6

Das folgende Beispiel zeigt die Konfiguration eines SNMP-Empfängers, der SNMPv3 mit einer IP-Adresse 192.0.2.255 und der Portnummer 162 für Trap-Nachrichten unterstützt. Die Tiebreaker Software ist bereit, Traps an den von Ihnen angegebenen SNMP-Empfänger zu senden.

Tiebreaker 1.6 unterstützt nur SNMPv3

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
```

Tiebreak 1.5 und 1.4

Das folgende Beispiel zeigt die Konfiguration eines SNMP-Empfängers, der SNMPv3 mit einer IP-Adresse 192.0.2.255 und der Portnummer 162 für Trap-Nachrichten unterstützt. Die Tiebreaker Software ist bereit, Traps an den von Ihnen angegebenen SNMP-Empfänger zu senden.

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Version[V1/V3]: v3
Enter SNMP Host: 192.0.2.255
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
Enter SNMP V3 Privacy password:
Engine ID : 8000031504932eff571825192a6f1193b265e24593
Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
software.
```

Sie sollten SNMPv3 konfigurieren, da SNMPv1 nicht sicher ist. Stellen Sie sicher, dass der Standard-Community-String **NOT** auf public gesetzt ist.

2. Vergewissern Sie sich, dass die SNMP-Einstellungen konfiguriert sind:

   `snmp config test`

   Das folgende Beispiel zeigt, dass die Tiebreaker Software einen SNMP Trap für den Event TEST_SNMP_CONFIG senden kann:

```
NetApp MetroCluster Tiebreaker :> snmp config test
Sending SNMP trap to localhost. Version : V3.
Successfully sent SNMP trap for event TEST_SNMP_CONFIG
NetApp MetroCluster Tiebreaker :>
```

Monitoring der MetroCluster-Konfiguration

Die MetroCluster Tiebreaker Software automatisiert den Recovery-Prozess, da Kunden damit den MetroCluster-Konfigurationsstatus überwachen, SNMP-Ereignisse und Traps bewerten, die an den NetApp Kunden-Support gesendet werden, und den Status von Monitoring-Vorgängen anzeigen können.

AutoSupport wird konfiguriert

Standardmäßig werden AutoSupport-Meldungen eine Woche nach der Installation der Tiebreaker Software an NetApp gesendet. Ereignisse, die die AutoSupport-Benachrichtigung auslösen, sind eine Panik der Tiebreaker Software, die Erkennung von Ausfallszenarien für MetroCluster-Konfigurationen oder ein unbekannter MetroCluster-Konfigurationsstatus.

Bevor Sie beginnen

Sie müssen über einen direkten Zugriff für das Einrichten von AutoSupport Meldungen verfügen.

Schritte

1. Verwenden Sie den Tiebreaker CLI-AutoSupport-Befehl mit einer der folgenden Optionen:

Option	Beschreibung
-Rufe	Sendet eine AutoSupport-Nachricht an den Kundensupport
-Configure Wizard	Assistent zum Konfigurieren der Anmeldeinformationen für den Proxyserver
-Delete-Konfiguration	Löscht die Anmeldeinformationen des Proxyservers
--aktivieren	Aktiviert die AutoSupport-Benachrichtigung (dies ist die Standardeinstellung).
-Disable	Deaktiviert die AutoSupport-Benachrichtigung
-Anzeigen	Zeigt den AutoSupport-Status an

Im folgenden Beispiel wird AutoSupport aktiviert oder deaktiviert und das Ziel, an das der AutoSupport Inhalt gesendet wird, angezeigt:

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status            : disabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status            : enabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission      : success
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

Das folgende Beispiel zeigt AutoSupport, die über einen authentifizierten Proxy-Server mit einer IP-Adresse und Portnummer konfiguriert sind:

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

Im folgenden Beispiel wird das Löschen einer AutoSupport-Konfiguration gezeigt:

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

SNMP-Ereignisse und -Traps

Die NetApp MetroCluster Tiebreaker Software verwendet SNMP-Traps, um Sie über wichtige Ereignisse zu informieren. Diese Fallen sind Teil der NetApp MIB Datei. Jeder Köder enthält die folgenden Informationen: Trap-Name, Schweregrad, Impact-Level, Zeitstempel und Nachricht.

Ereignis-Name	Ereignisdetails	Fallnummer
MetroCluster Tie-Breaker kann die MetroCluster-Konfiguration nicht erreichen	Weist den Administrator darauf hin, dass die Software einen Notfall nicht erkennen kann. Dieses Ereignis tritt auf, wenn beide Cluster nicht erreichbar sind.	25000
MetroCluster Tie-Breaker kann den Cluster nicht erreichen	Warnt den Administrator, dass die Software keinen der Cluster erreichen kann.	25001
MetroCluster Tie-Breaker hat einen Notfall am Cluster erkannt	Benachrichtigt den Administrator, dass die Software einen Standortausfall erkennt. Es wird eine Benachrichtigung zugestellt.	25002
Alle Verbindungen zwischen dem Partner-Cluster werden getrennt.	Die Software erkennt, dass beide Cluster erreichbar sind, aber alle Netzwerkpfade zwischen den beiden Clustern sind ausgefallen, und die Cluster können nicht miteinander kommunizieren.	25005
SNMP-Test-Trap	Die SNMP-Konfiguration kann nun durch Ausführen des befehls snmp config Test getestet werden.	25006

Anzeigen des Status von Monitoring-Vorgängen

Sie können den Gesamtstatus der Überwachungsvorgänge für eine MetroCluster-Konfiguration anzeigen.

Schritt

1. Verwenden Sie den Tiebreaker CLI-Monitor-Befehl, um den Status eines MetroCluster-Vorgangs mit einer der folgenden Optionen anzuzeigen:

Option	Beschreibung
-Monitor-Name	Zeigt den Status des angegebenen Monitornamens an
-Operation-history	Zeigt bis zu 10 Überwachungsvorgänge an, die zuletzt auf einem Cluster durchgeführt wurden
-Stats	Zeigt die Statistiken zum angegebenen Cluster an
-Status	Zeigt den Status des angegebenen Clusters an **Hinweis:** die MetroCluster Tiebreaker Software kann bis zu 10 Minuten dauern, um den Status des Abschlusses von Vorgängen wie Heal Aggregates, Heal Roots oder Switchback zu reflektieren.

   Im folgenden Beispiel wird gezeigt, dass die Cluster „Cluster_A“ und „Cluster_B“ verbunden und sich in

einem ordnungsgemäßen Zustand befinden:

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

Im folgenden Beispiel werden die letzten sieben Vorgänge angezeigt, die auf Cluster_B ausgeführt wurden:

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

Anzeigen von Informationen über die MetroCluster-Konfiguration

Sie können den Monitornamen und die IP-Adresse aller Instanzen von MetroCluster-Konfigurationen in der Tiebreaker Software anzeigen.

Schritt

1. Zeigen Sie mit dem Tiebreaker CLI-Konfigurationsbefehl die MetroCluster-Konfigurationsinformationen an.

   Im folgenden Beispiel werden die Informationen für Cluster „Cluster_A“ und „Cluster_B“ angezeigt:

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

Erstellen von Dump-Dateien

Sie speichern den Gesamtstatus der Tiebreaker Software in einer Dump-Datei für Debugging-Zwecke.

Schritt

1. Verwenden Sie den Tiebreaker CLI Monitor Dump -Status-Befehl, um eine Dump-Datei des Gesamtstatus aller MetroCluster-Konfigurationen zu erstellen.

   Das folgende Beispiel zeigt die erfolgreiche Erstellung der Dump-Datei /var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus

Umschaltung bei Erkennung eines Standortausfalls wird automatisch ausgeführt. MetroCluster Tiebreaker befindet sich im aktiven Modus. Dieser Modus kann zur Ergänzung der Funktion zur automatischen Umschaltung von ONTAP/FAS verwendet werden.

Wenn Sie MetroCluster Tiebreaker im aktiven Modus implementieren, können die folgenden bekannten Probleme zu Datenverlust führen:

- Wenn die Verbindung zwischen den Standorten fehlschlägt, werden die Controller auf jedem Standort weiterhin mit den Clients verbunden. Die Controller werden jedoch nicht gespiegelt. Der Ausfall eines Controllers an einem Standort wird als Standortausfall erkannt und der MetroCluster Tiebreaker initiiert eine Umschaltung. Die Daten, die nach dem Ausfall der Verbindung zwischen den Standorten mit dem Remote Standort nicht gespiegelt werden, gehen verloren.
- Eine Umschaltung findet statt, wenn die Aggregate am Remote-Standort eingeschränkt sind. Die Daten werden nicht repliziert, wenn die Umschaltung erfolgt ist, bevor die Aggregat-Resynchronisierung erfolgt ist.
- Wenn die Umschaltung abgeschlossen wird, tritt ein Remote-Storage-Ausfall auf.
- Nicht-flüchtiger Speicher (NVRAM oder NVMEM, je nach Plattformmodell) in den Storage-Controllern wird nicht vom Remote Disaster Recovery (DR)-Partner am Partnerstandort gespiegelt.
- Die Metadaten gehen verloren, wenn das Cluster-Peering-Netzwerk über einen längeren Zeitraum ausfällt und die Metadaten-Volumes nach einem Switchover nicht online sind.

> Möglicherweise treten Szenarien auf, die nicht erwähnt werden. NetApp ist nicht verantwortlich für jegliche Schäden, die sich aus der Verwendung von MetroCluster Tiebreaker im aktiven Modus ergeben können. Verwenden Sie MetroCluster Tiebreaker nicht im aktiven Modus, wenn die Risiken und Einschränkungen für Sie nicht akzeptabel sind.

Firewall-Anforderungen für MetroCluster Tiebreaker

MetroCluster Tiebreaker nutzt eine Reihe von Ports, um mit bestimmten Services zu kommunizieren.

In der folgenden Tabelle sind die Ports aufgeführt, die Sie in Ihrer Firewall zulassen müssen:

Port/Services	Quelle	Ziel	Zweck
443 / TCP	Tiebreaker	Internet	Senden von AutoSupport Meldungen an NetApp

22 / TCP	Management-Host	Tiebreaker	Tiebreaker Management
443 / TCP	Tiebreaker	Cluster-Management-LIFs	Sichere Kommunikation zum Cluster über HTTP (SSL)
22 / TCP	Tiebreaker	Cluster-Management-LIFs	Sichere Kommunikation zum Cluster über SSH
443 / TCP	Tiebreaker	Node-Management-LIFs	Sichere Kommunikation mit Knoten über HTTP (SSL)
22 / TCP	Tiebreaker	Node-Management-LIFs	Sichere Kommunikation mit Knoten über SSH
162 / UDP	Tiebreaker	SNMP-Trap-Host	Wird zum Senden von SNMP-Traps für Warnmeldungen verwendet
ICMP (Ping)	Tiebreaker	Cluster-Management-LIFs	Überprüfen, ob Cluster-IP erreichbar ist
ICMP (Ping)	Tiebreaker	Node-Management-LIFs	Überprüfen Sie, ob die Knoten-IP erreichbar ist

Ereignisprotokolldateien für MetroCluster Tiebreaker

Die Event-Log-Datei enthält ein Protokoll aller Aktionen, die von der MetroCluster Tiebreaker Software durchgeführt werden.

Die Tiebreaker Software führt folgende Aktionen durch:

- Erkennt Standortausfälle
- Erkennt Konfigurationsänderungen in Verbindung mit der Datenbank, anderen Tiebreaker Monitoren oder der MetroCluster Tiebreaker Software
- Erkennt SSH-Verbindungen und -Verbindungen
- Erkennung von MetroCluster-Konfigurationen

Diese Aktionen werden in der Ereignis-Log-Datei im folgenden Format protokolliert:

Zeitstempel der Schweregrad/des Thread-id-Moduls auf Protokollebene

```
2022-09-07 06:14:30,797 INFO  [MCCTBCommandServer-16] [SslSupport]
Successfully initiated SSL context. Protocol used is TLSv1.3.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16] [DataBase]
Successfully read MCCTB database.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16]
[ConfigurationMonitor] Debug mode disabled.
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen
"Technischer Bericht 4375 zu NetApp MetroCluster für ONTAP 9.3"	• Eine technische Übersicht über Konfiguration und Betrieb von MetroCluster • Best Practices für die Konfiguration von MetroCluster.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von MetroCluster IP"	• MetroCluster IP Architektur • Verkabelung der MetroCluster IP-Konfiguration • Konfigurieren der MetroCluster in ONTAP

"Warten der MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster Konfiguration • Entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweiterung einer Fabric-Attached oder Stretch MetroCluster Konfiguration mit vier Nodes auf eine MetroCluster Konfiguration mit acht Nodes
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

MetroCluster Datensicherung und Disaster Recovery verstehen

MetroCluster Datensicherung und Disaster Recovery verstehen

Es ist hilfreich zu verstehen, wie MetroCluster die Daten sichert und transparentes Recovery bei Ausfällen bietet, sodass Sie Ihre Switchover- und Switchover-Aktivitäten einfach und effizient managen können.

MetroCluster verwendet Spiegelung, um die Daten in einem Cluster zu schützen. Es bietet Disaster Recovery über einen einzigen MetroCluster-Befehl, bei dem ein sekundäres System am Survivor-Standort aktiviert wird und so die gespiegelten Daten anliefert, die ursprünglich einem primären Standort gehören, von einem Ausfall betroffen sind.

MetroCluster Konfigurationen mit acht oder vier Nodes bieten lokalen Failover und Switchover

MetroCluster Konfigurationen mit acht oder vier Nodes sichern Daten auf lokaler Ebene und auf Cluster-Ebene. Bei der Einrichtung einer MetroCluster Konfiguration müssen Sie wissen, wie MetroCluster Konfigurationen Ihre Daten schützen.

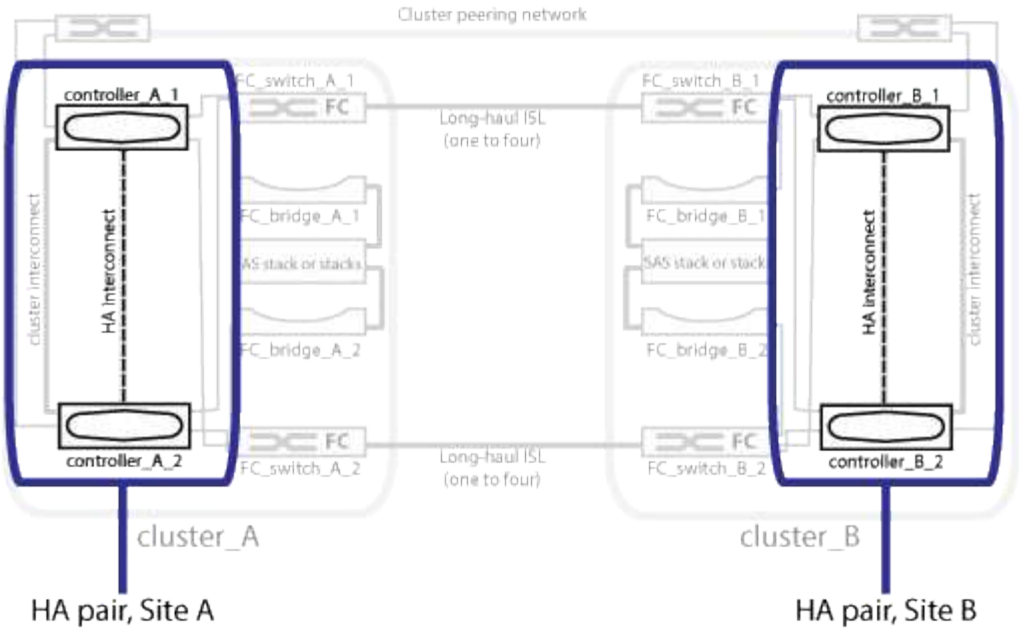
MetroCluster Konfigurationen sichern Daten durch zwei physisch getrennte, gespiegelte Cluster. Jedes Cluster spiegelt synchron die Daten- und Storage Virtual Machine (SVM)-Konfiguration des anderen Clusters. Im Falle eines Ausfalls an einem Standort kann ein Administrator die gespiegelte SVM aktivieren und damit beginnen, die gespiegelten Daten vom verbleibenden Standort aus bereitzustellen. Darüber hinaus werden die Nodes in jedem Cluster als HA-Paar konfiguriert, wodurch ein Level des lokalen Failover bereitgestellt wird.

Funktionsweise der lokalen HA-Datensicherung in einer MetroCluster Konfiguration

Sie müssen verstehen, wie HA-Paare in der MetroCluster Konfiguration funktionieren.

Die beiden Cluster im Peering-Netzwerk bieten bidirektionale Disaster Recovery, bei der jedes Cluster als Quelle und Backup des anderen Clusters verwendet werden kann. Jedes Cluster enthält zwei Nodes, die als HA-Paar konfiguriert sind. Bei einem Ausfall oder einer erforderlichen Wartung innerhalb der Konfiguration eines einzelnen Node kann der Storage Failover die Vorgänge des Nodes an seinen lokalen HA-Partner übertragen.

Die folgende Abbildung zeigt eine MetroCluster FC-Konfiguration. Die HA-Funktion ist in MetroCluster IP-Konfigurationen identisch, mit der Ausnahme, dass der HA Interconnect durch die Cluster Switches bereitgestellt wird.



Verwandte Informationen

"Hochverfügbarkeitskonfiguration"

Durchführen von Daten- und Konfigurations-Replizierung mit MetroCluster Konfigurationen

MetroCluster Konfigurationen nutzen eine Vielzahl von ONTAP Funktionen für die synchrone Replizierung von Daten und Konfiguration zwischen den beiden MetroCluster Standorten.

Konfigurationsschutz mit dem Configuration Replication Service

Der ONTAP Configuration Replication Service (CRS) schützt die MetroCluster-Konfiguration, indem die Informationen automatisch an den DR-Partner repliziert werden.

Die CRS repliziert die lokale Node-Konfiguration synchron zum DR-Partner im Partner-Cluster. Diese Replikation wird über das Cluster-Peering-Netzwerk durchgeführt.

Zu den replizierten Informationen gehören die Cluster-Konfiguration und die SVM-Konfiguration.

Replizierung von SVMs während des MetroCluster-Betriebs

Der ONTAP Configuration Replication Service (CRS) bietet eine redundante Konfiguration des Datenservers und eine Spiegelung der zu der SVM gehörenden Daten-Volumes. Bei einer Umschaltung wird die Quell-SVM heruntergefahren und die Ziel-SVM, die sich im verbleibenden Cluster befindet, wird aktiv.

> Ziel-SVMs in der MetroCluster-Konfiguration haben das Suffix „`-mc`“ automatisch an ihren Namen angehängt, um sie zu identifizieren. Eine MetroCluster-Konfiguration hängt das Suffix „ `-mc`“ an den Namen der Ziel-SVMs an. Wenn der SVM-Name einen Zeitraum enthält, wird das Suffix „`-mc`“ vor dem ersten Zeitraum angewendet. Wenn der SVM-Name beispielsweise SVM.DNS.NAME lautet, wird das Suffix „`-mc`“ als SVM-MC.DNS.NAME angehängt.

Das folgende Beispiel zeigt die SVMs für eine MetroCluster-Konfiguration: „`SVM_Cluster_A`“ ist eine SVM auf dem Quellstandort und „`SVM_Cluster_A-mc`“ ist ein Synchronisationskreiseziel-Aggregat auf dem Disaster-Recovery-Standort.

- SVM_Cluster_A stellt Daten auf Cluster A bereit

  Es handelt sich um eine synchrone Quell-SVM, die die SVM-Konfiguration (LIFs, Protokolle und Services) und die Daten in Volumes der SVM darstellt. Die Konfiguration und die Daten werden zu SVM_Cluster_A-mc repliziert, einer synchronen Ziel-SVM auf Cluster B.

- SVM_Cluster_B stellt Daten auf Cluster B bereit

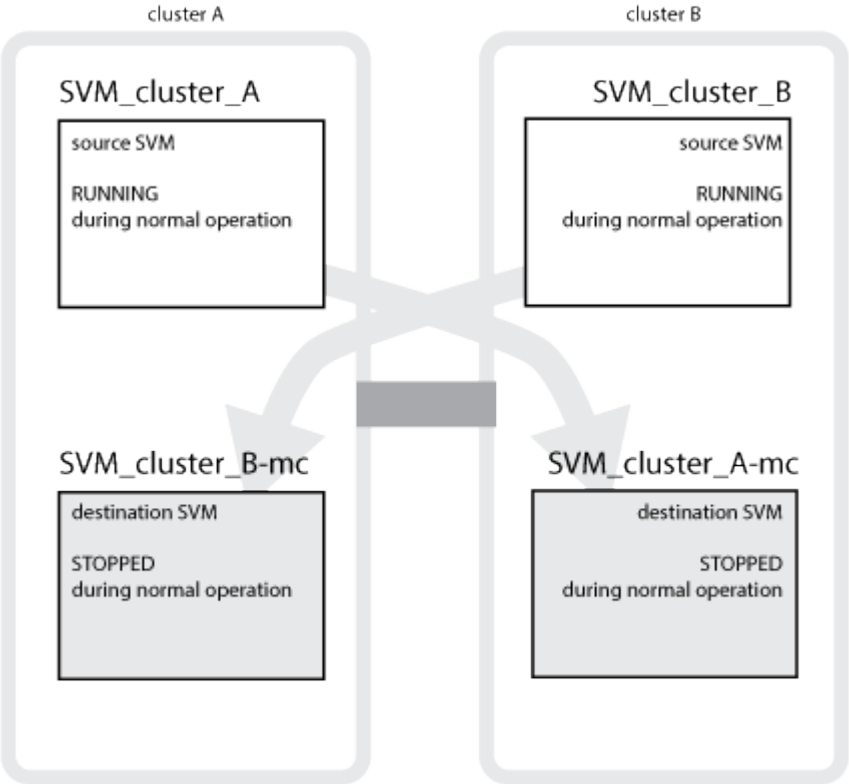
  Es handelt sich um eine synchrone Quell-SVM, die Konfiguration und Daten für SVM_Cluster_B-mc auf Cluster A darstellt

- SVM_Cluster_B-mc ist eine synchrone Ziel-SVM, die während des normalen, ordnungsgemäßen Betriebs der MetroCluster-Konfiguration angehalten wird.

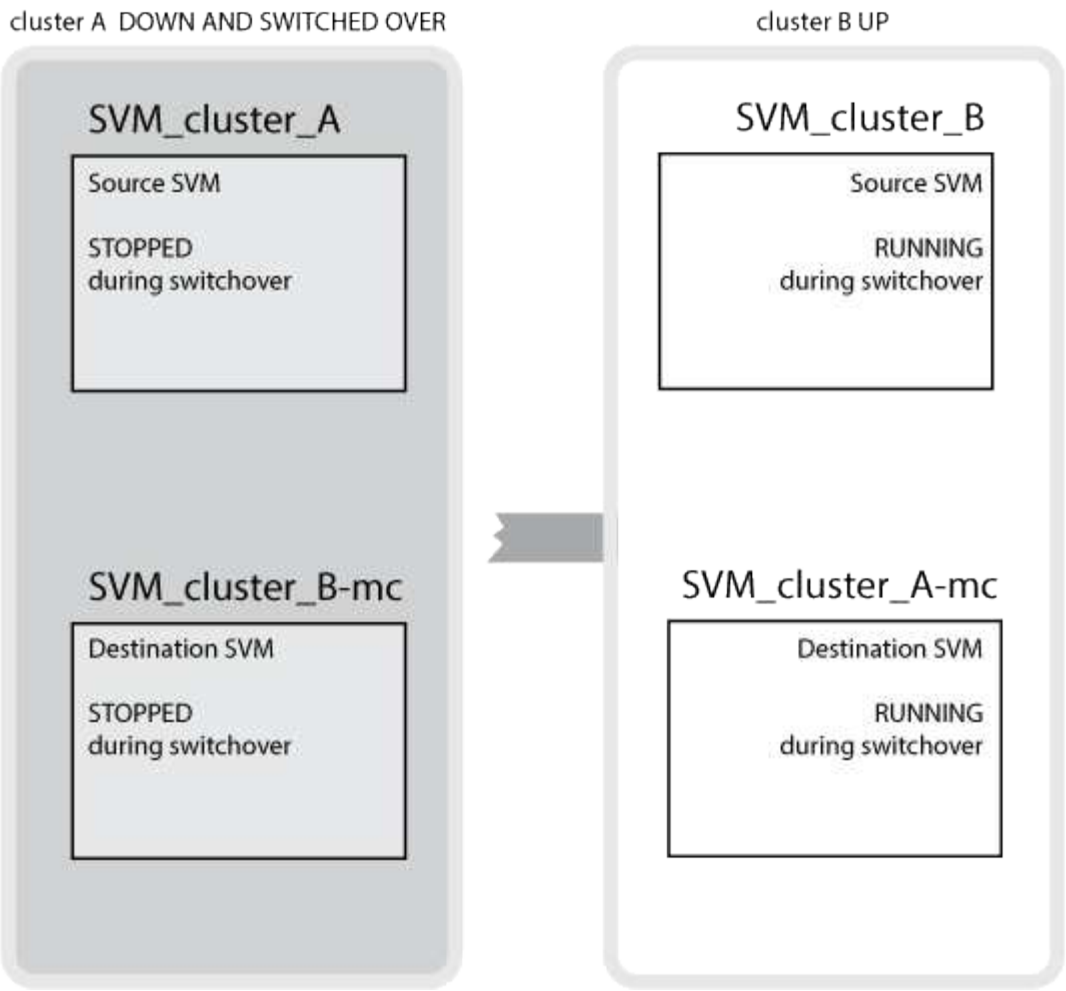
  Bei einer erfolgreichen Umschaltung von Cluster B zu Cluster A wird SVM_Cluster_B angehalten und SVM_Cluster_B-mc aktiviert, und beginnt mit der Bereitstellung von Daten aus Cluster A

- SVM_Cluster_A-mc ist eine synchrone Ziel-SVM, die während des normalen, ordnungsgemäßen Betriebs der MetroCluster-Konfiguration angehalten wird.

  Bei einer erfolgreichen Umschaltung von Cluster A auf Cluster B wird SVM_Cluster_A angehalten und SVM_Cluster_A-mc aktiviert, sodass die Daten von Cluster B bereit werden



Tritt eine Umschaltung auf, wird der Remote-Plex auf dem verbleibenden Cluster online geschaltet, und die sekundäre SVM stellt die Daten bereit.



Die Verfügbarkeit von Remote-Plexen nach Umschaltung hängt vom Konfigurationstyp MetroCluster ab:

- Bei MetroCluster FC-Konfigurationen bleiben lokale und Remote-Plexe nach Umschaltung online, wenn auf den Disaster-Site-Storage über ISLs zugegriffen werden kann.

  Wenn die ISLs ausfallen und der Storage am Disaster-Standort nicht verfügbar ist, beginnt die SVM des synchronen Ziels, die Daten vom verbleibenden Standort bereitzustellen.

- Bei MetroCluster IP-Konfigurationen hängt die Verfügbarkeit der Remote-Plexe von der ONTAP-Version ab:
  - Ab ONTAP 9.5 bleiben sowohl lokale als auch Remote-Plexe online, wenn die Knoten des Disaster-Standorts weiterhin gestartet werden.
  - Vor ONTAP 9.5 ist der Storage nur aus dem lokalen Plex auf dem überlebenden Standort verfügbar.

    Die SVM auf dem synchronen Ziel beginnt, Daten vom verbleibenden Standort bereitzustellen.

Verwandte Informationen

"Systemadministration"

MetroCluster-Konfigurationen nutzen SyncMirror zur Bereitstellung von Datenredundanz

Gespiegelte Aggregate mit der SyncMirror-Funktionalität bieten Datenredundanz und enthalten die Volumes der Quell- und Ziel-Storage Virtual Machine (SVM). Daten werden in Festplatten-Pools im Partner-Cluster repliziert. Auch nicht gespiegelte Aggregate werden unterstützt.

In der folgenden Tabelle ist der Status (online oder offline) eines nicht gespiegelten Aggregats nach einer Umschaltung dargestellt:

Art der Umschaltung	Status der MetroCluster FC-Konfiguration	MetroCluster IP-Konfigurationsstatus
Ausgehandelte Umschaltung (NSO)	Online	Offline (Hinweis 1)
Automatische ungeplante Umschaltung (AUSO)	Online	Offline (Hinweis 1)
Ungeplante Umschaltung (USO)	• Wenn kein Speicher verfügbar ist: Offline • Wenn Speicher verfügbar ist: Online	Offline (Hinweis 1)

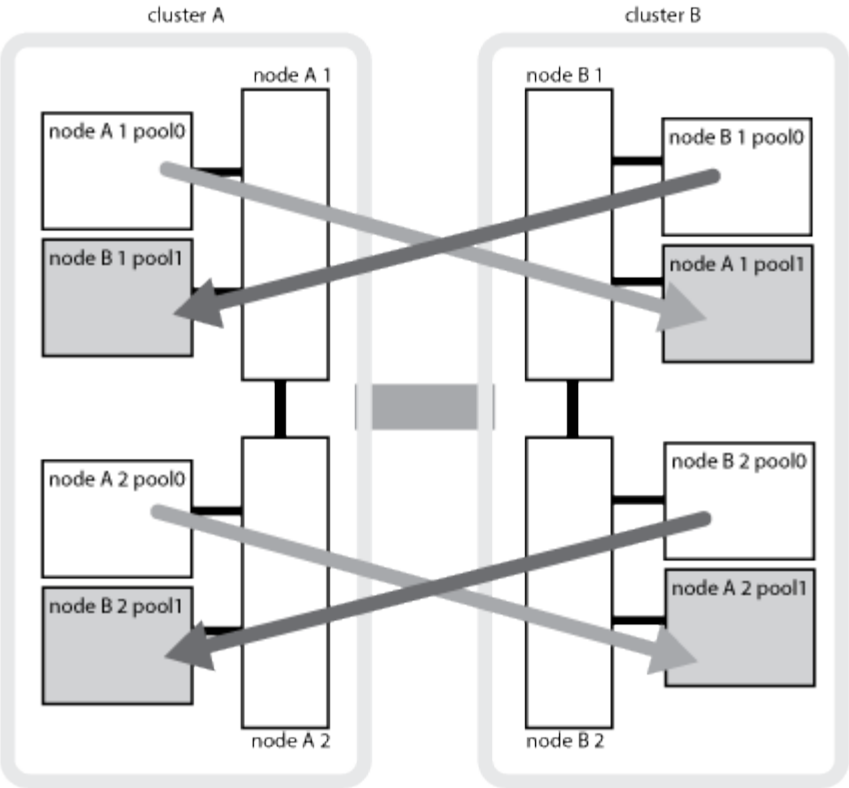
Hinweis 1: In MetroCluster IP-Konfigurationen können Sie nach Abschluss der Umschaltung die nicht gespiegelten Aggregate manuell online bringen.

Weitere Informationen zu Unterschiede bei der Umschaltung zwischen MetroCluster FC- und IP-Konfigurationen.

Wenn sich das nicht gespiegelte Aggregat nach einer Umschaltung auf den DR-Partnerknoten befindet und ein Inter-Switch-Link-Ausfall (ISL) auftritt, kann ein lokaler Node ausfallen.

Die folgende Abbildung zeigt, wie Disk Pools zwischen den Partner-Clustern gespiegelt werden. Daten auf lokalen Plexen (in Pool0) werden auf Remote-Plexe (in Pool1) repliziert.

Bei Verwendung von hybriden Aggregaten kann es zu einer Performance-Verschlechterung kommen, nachdem ein SyncMirror Plex fehlgeschlagen ist. Dabei ist die SSD-Schicht (Solid State Disk) gefüllt.



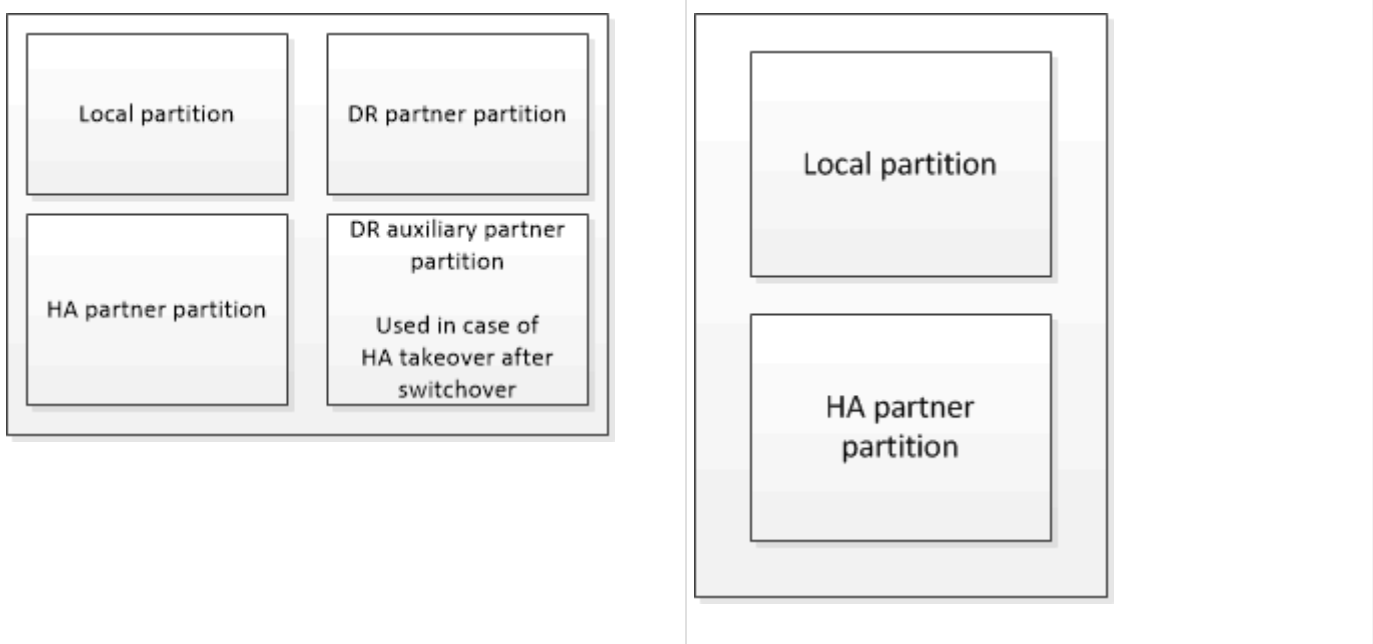
Funktionsweise von NVRAM- oder NVMEM-Cache-Spiegelung und Dynamic Mirroring in MetroCluster Konfigurationen

Der nicht-flüchtige Speicher (NVRAM oder NVMEM, je nach Plattformmodell) in den Storage Controllern wird sowohl lokal bei einem lokalen HA-Partner als auch am Remote-Standort zu einem DR-Partner (Remote Disaster Recovery) am Partnerstandort gespiegelt. Bei einem lokalen Failover oder einer Umschaltung können Daten aus diesem nicht-flüchtigen Cache beibehalten.

In einem HA-Paar, das nicht Teil einer MetroCluster Konfiguration ist, behält jeder Storage Controller zwei nicht-flüchtige Cache-Partitionen bei: Eine für sich und eine für seinen HA-Partner.

Der nicht-flüchtige Cache eines jeden Storage-Controllers ist in eine MetroCluster-Konfiguration mit vier Nodes unterteilt. In einer MetroCluster-Konfiguration mit zwei Nodes werden die HA-Partnerpartition und die DR-Zusatzpartition nicht verwendet, da die Storage Controller nicht als HA-Paar konfiguriert sind.

Nicht-flüchtige Caches für einen Storage Controller	
In einer MetroCluster-Konfiguration	In einem nicht-MetroCluster HA-Paar



Die nicht-flüchtigen Caches speichern folgenden Inhalt:

- Die lokale Partition enthält Daten, die der Speicher-Controller noch nicht auf die Festplatte geschrieben hat.
- Die HA-Partnerpartition ist eine Kopie des lokalen Caches des HA-Partners des Storage Controllers.

  In einer MetroCluster Konfiguration mit zwei Nodes gibt es keine HA-Partnerpartition, da die Storage Controller nicht als HA-Paar konfiguriert sind.

- Die DR-Partnerpartition enthält eine Kopie des lokalen Caches des DR-Partners des Storage Controllers.

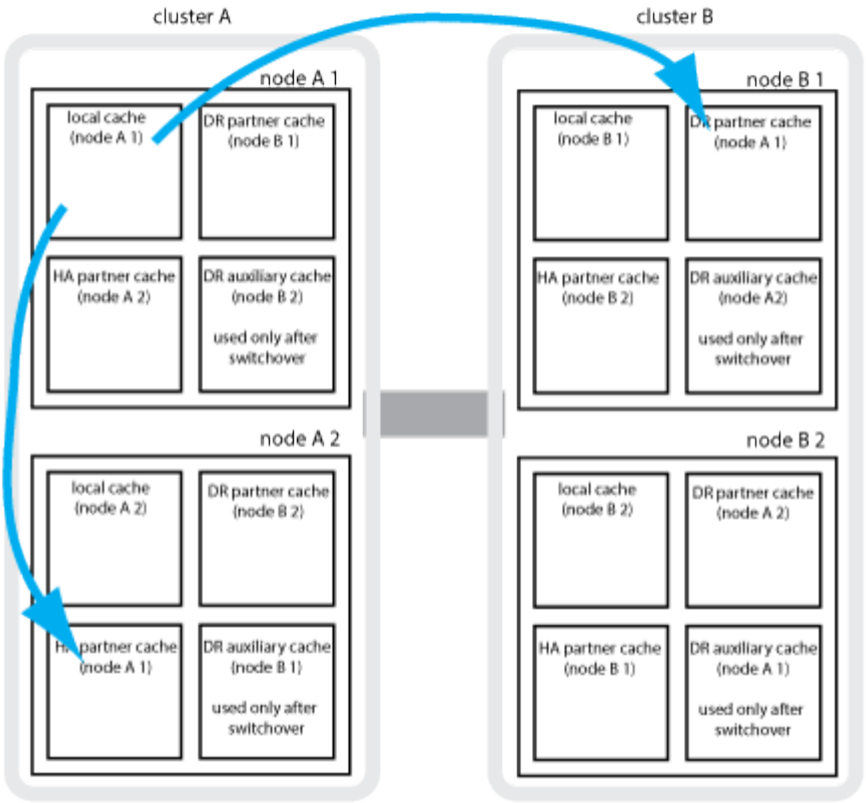
  Der DR-Partner ist ein Knoten im Partner-Cluster, der mit dem lokalen Knoten gepaart wird.

- Die zusätzliche DR-Partnerpartition enthält eine Kopie des lokalen Caches des DR-Hilfspartners des Storage-Controllers.

  Der DR-Hilfspartner ist der HA-Partner des DR-Partners des lokalen Knotens. Dieser Cache ist erforderlich, wenn ein HA-Takeover vorliegt (entweder wenn die Konfiguration im normalen Betrieb oder nach einer MetroCluster-Umschaltung).

  In einer MetroCluster Konfiguration mit zwei Nodes gibt es keine zusätzliche DR-Partnerpartition, da die Storage Controller nicht als HA-Paar konfiguriert sind.

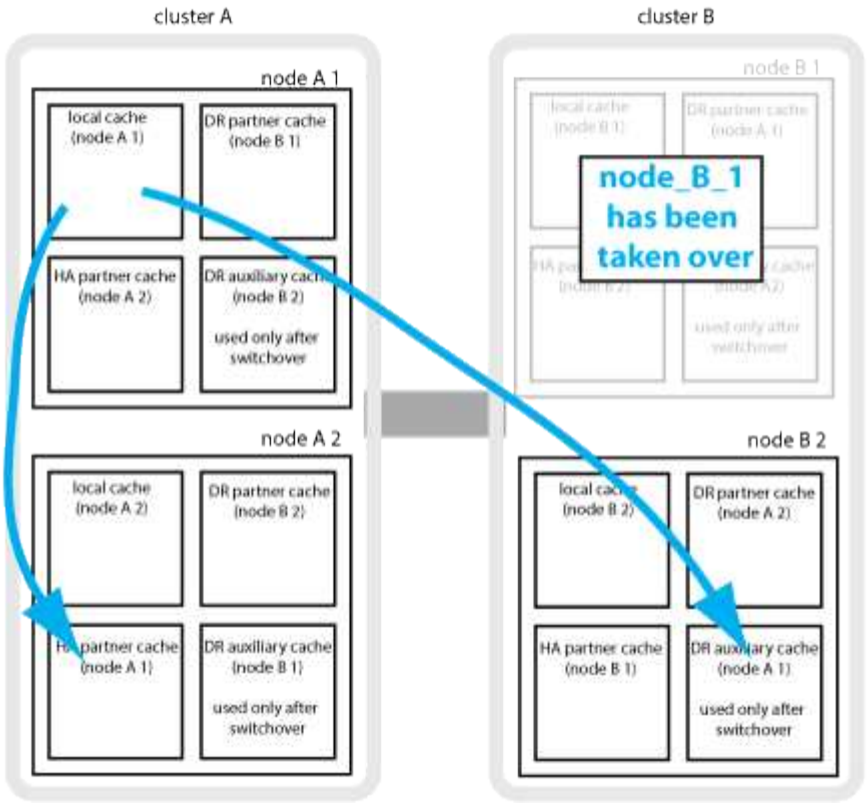
Beispielsweise wird der lokale Cache eines Node (Node_A_1) sowohl lokal als auch Remote an den MetroCluster Standorten gespiegelt. Die folgende Abbildung zeigt, dass der lokale Cache von Node_A_1 für den HA-Partner (Node_A_2) und DR-Partner (Node_B_1) gespiegelt wird:



Dynamische Spiegelung im Falle einer lokalen HA-Übernahme

Wenn eine lokale HA-Übernahme in einer MetroCluster Konfiguration mit vier Nodes stattfindet, kann der übernnahmene Node nicht mehr als Spiegelung für seinen DR-Partner fungieren. Damit die DR-Spiegelung fortgesetzt werden kann, wechselt die Spiegelung automatisch zum DR-Hilfspartner. Nach erfolgreicher Rückgabe wird die Spiegelung automatisch an den DR-Partner zurückgeführt.

Beispiel: Node_B_1 schlägt fehl und wird von Node_B_2 übernommen. Der lokale Cache von Node_A_1 kann nicht mehr auf Node_B_1 gespiegelt werden. Die Spiegelung wechselt zum DR-Hilfspartner Node_B_2.



Arten von Disaster- und Recovery-Methoden

Sie müssen mit verschiedenen Arten von Ausfällen und Katastrophen vertraut sein, damit Sie die MetroCluster Konfiguration entsprechend nutzen können.

- Single-Node-Ausfall

  Eine einzelne Komponente im lokalen HA-Paar fällt aus.

  In einer MetroCluster-Konfiguration mit vier Nodes kann dieser Ausfall je nach ausgefallener Komponente zu einer automatischen oder ausgehandelten Übernahme des beeinträchtigten Knotens führen. Datenwiederherstellung wird in beschrieben "Paarverwaltung mit hoher Verfügbarkeit" .

  In einer MetroCluster-Konfiguration mit zwei Nodes führt dieser Ausfall zu einer automatischen ungeplanten Umschaltung (AUSO).

- Site-weiter Controller-Ausfall

  Alle Controller-Module werden an einem Standort aufgrund eines Stromausfalls, des Austauschs von Geräten oder eines Notfalls ausfallen. Normalerweise können MetroCluster-Konfigurationen Ausfälle und Ausfälle nicht unterscheiden. Witness-Software wie die MetroCluster Tiebreaker Software kann jedoch zwischen ihnen unterscheiden. Ein standortweiter Controller-Ausfall kann zu einem automatischen Switchover führen, wenn Inter-Switch Link (ISL)-Links und -Switches verfügbar sind und der Storage zugänglich ist.

  "Paarverwaltung mit hoher Verfügbarkeit" Hat weitere Informationen zur Wiederherstellung nach standortweiten Controller-Ausfällen, die keine Controller-Ausfälle umfassen, sowie Fehlern, die einen oder mehrere Controller umfassen.

- ISL-Fehler

Die Verbindungen zwischen den Sites schlagen fehl. Die MetroCluster-Konfiguration hat keine Aktion. Jeder Node stellt weiterhin Daten normal bereit. Die Spiegelungen werden jedoch nicht auf die entsprechenden Disaster Recovery-Standorte geschrieben, da der Zugriff auf sie verloren geht.

- Mehrere sequenzielle Ausfälle

  Mehrere Komponenten schlagen nacheinander fehl. Ein Controller-Modul, ein Switch Fabric und ein Shelf versagen beispielsweise in einer Sequenz und führen zu einem Storage Failover, Fabric-Redundanz und einem SyncMirror-System, das sequenziell gegen Ausfallzeiten und Datenverlust schützt.

In der folgenden Tabelle sind die Fehlertypen und der entsprechende Disaster Recovery-Mechanismus (DR) und Wiederherstellungsmethode aufgeführt:

> AUSO (automatische ungeplante Umschaltung) wird in MetroCluster IP-Konfigurationen nicht unterstützt.

Fehlertyp	DR-Mechanismus		Zusammenfassung der Wiederherstellungsmethode	
	Konfiguration mit vier Nodes	Konfiguration mit zwei Nodes	Konfiguration mit vier Nodes	Konfiguration mit zwei Nodes
Single-Node-Ausfall	Lokaler HA-Failover	AUSO	Ist nicht erforderlich, wenn automatisches Failover und Giveback aktiviert ist.	Nach dem Wiederherstellen des Node erfolgt die manuelle Reparatur und wechseln mit dem zurück `metrocluster heal -phase aggregates`, `metrocluster heal -phase root-aggregates`, und `metrocluster switchback` Diese Befehle sind erforderlich. HINWEIS: Der `metrocluster heal` Befehle sind für MetroCluster IP Konfigurationen mit ONTAP 9.5 oder höher nicht erforderlich.

Standortausfall	MetroCluster Umschaltung		Nach dem Wiederherstellen des Node erfolgt die manuelle Reparatur und wechseln mit dem zurück `metrocluster healing` Und `metrocluster switchback` Diese Befehle sind erforderlich. Der `metrocluster heal` Bei MetroCluster IP-Konfigurationen, auf denen ONTAP 9.5 ausgeführt wird, sind keine Befehle erforderlich.
Site-weiter Controller-Ausfall	AUSO nur, wenn der Storage am Disaster-Site zugänglich ist.	AUSO (wie bei Ausfall eines einzelnen Nodes)	
Mehrere sequenzielle Ausfälle	Lokales HA-Failover, gefolgt von MetroCluster-erzwungener Umschaltung mit dem MetroCluster Switchover-Forced-on-Disaster-Befehl. HINWEIS: Je nach ausgefallener Komponente ist eine erzwungene Umschaltung möglicherweise nicht erforderlich.	MetroCluster erzwungene Umschaltung mit dem `metrocluster switchover -forced-on -disaster` Befehl.	
ISL-Fehler	Kein MetroCluster-Switchover: Die beiden Cluster stellen unabhängig voneinander ihre Daten bereit		Nicht erforderlich für diese Art von Fehler. Nach dem Wiederherstellen der Verbindung wird der Speicher automatisch neu synchronisiert.

Unterbrechungsfreiem Betrieb dank MetroCluster Konfiguration mit acht oder vier Nodes

Im Fall eines Problems, das auf einen einzelnen Knoten beschränkt ist, sorgt ein Failover und die Rückgabe innerhalb des lokalen HA-Paars für einen unterbrechungsfreien Betrieb. In diesem Fall erfordert die MetroCluster Konfiguration keine Umschaltung auf den Remote-Standort.

Da die MetroCluster Konfiguration mit acht oder vier Nodes aus einem oder mehreren HA-Paaren an jedem Standort besteht, kann jeder Standort lokalen Ausfällen standhalten und einen unterbrechungsfreien Betrieb durchführen, ohne dass ein Switchover zum Partnerstandort erforderlich ist. Der Betrieb des HA-Paars ist derselbe wie für HA-Paare in anderen Konfigurationen als MetroCluster.

Bei MetroCluster Konfigurationen mit vier oder acht Nodes können Node-Ausfälle aufgrund von Panic-Meldungen oder Stromausfällen zu einem automatischen Switchover führen.

"Paarverwaltung mit hoher Verfügbarkeit"

Falls nach einem lokalen Failover ein zweiter Ausfall auftritt, sorgt das MetroCluster Switchover-Ereignis für einen unterbrechungsfreien Betrieb. Ähnlich sieht es nach einem Switchover bei einem zweiten Ausfall in einem der verbleibenden Nodes aus, so dass ein lokales Failover-Ereignis einen unterbrechungsfreien Betrieb ermöglicht. In diesem Fall stellt der noch funktionsfähige Node die Daten der anderen drei Nodes in der DR-Gruppe bereit.

Umschaltung und zurückwechseln während MetroCluster Transition

Der MetroCluster FC-to-IP Umstieg erfordert zusätzliche MetroCluster IP Nodes und IP Switches zu einer vorhandenen MetroCluster FC-Konfiguration. Anschließend werden die MetroCluster FC Nodes ausgemustert. Je nach Phase des Übergangs verwenden die MetroCluster Switchover-, Healing- und Switchback-Vorgänge unterschiedliche Workflows.

Siehe "Umschaltung, Healing und Switchback-Betrieb während des Übergangs".

Konsequenzen des lokalen Failover nach Switchover

Wenn eine MetroCluster-Umschaltung stattfindet und ein Problem am verbleibenden Standort auftritt, kann ein lokaler Failover einen kontinuierlichen, unterbrechungsfreien Betrieb ermöglichen. Das System ist jedoch gefährdet, da sich dieses nicht mehr in einer redundanten Konfiguration befindet.

Falls nach einer Umschaltung ein lokaler Failover erfolgt, stellt ein einzelner Controller die Daten aller Storage-Systeme in der MetroCluster Konfiguration bereit. Dadurch können Ressourcenprobleme auftreten und sind anfällig für zusätzliche Ausfälle.

Durchführen einer MetroCluster Konfiguration mit zwei Nodes für einen unterbrechungsfreien Betrieb

Falls an einem der beiden Standorte aufgrund eines Panikzustands Probleme auftreten, ermöglicht die MetroCluster-Umschaltung einen kontinuierlichen unterbrechungsfreien Betrieb. Wenn ein Stromausfall sowohl den Node als auch den Storage beeinträchtigt, ist die Umschaltung nicht automatisch und es kommt zu einer Unterbrechung, bis der `metrocluster switchover` Befehl wird ausgegeben.

Da jeder Storage gespiegelt wird, kann ein Switchvorgang verwendet werden, so dass er bei einem Standortausfall eine unterbrechungsfreie Ausfallsicherheit bietet, ähnlich wie bei einem Storage Failover in einem HA-Paar bei einem Node-Ausfall.

Bei Konfigurationen mit zwei Nodes werden dieselben Ereignisse, die einen automatischen Storage Failover in einem HA-Paar auslösen, eine automatische ungeplante Umschaltung (AUSO) auslösen. Das bedeutet, dass eine MetroCluster Konfiguration mit zwei Nodes denselben Schutz bietet wie ein HA-Paar.

Verwandte Informationen

"Automatisches, ungeplantes Switchover in MetroCluster FC-Konfigurationen"

Überblick über den Switchover-Prozess

Die Umschaltung auf MetroCluster ermöglicht den sofortigen Wiederaufnahme von Services nach einem Ausfall, indem der Storage und der Client-Zugriff vom Quellcluster zum Remote-Standort verschoben werden. Sie müssen sich darüber im Klaren sein, welche Änderungen zu erwarten sind und welche Aktionen bei einem Switchover ausgeführt werden müssen.

Während eines Umschaltvorgangs führt das System folgende Aktionen durch:

- Das Eigentum an den Festplatten, die zum Disaster-Site gehören, wird zum Disaster-Recovery-Partner (DR) geändert.

  Dies ähnelt dem Fall eines lokalen Failover in einem Hochverfügbarkeitspaar (HA-Paar), bei dem das Eigentum an den zum Partner gehörenden Festplatten in einem gesunden Partner geändert wird.

- Die verbleibenden Plexe, die sich auf dem verbleibenden Standort befinden, doch zu den Knoten im

Disaster-Cluster gehören, werden auf dem Cluster am verbleibenden Standort online geschaltet.

- Die zum Disaster-Standort gehörende SVM-Storage-Maschine (Sync-Source Storage Virtual Machine) wird nur während einer ausgehandelten Umschaltung heruntergefahren.

  Dies ist nur auf eine ausgehandelte Umschaltung anwendbar.

- Die SVM des synchronen Ziels, die zum Disaster-Standort gehört, wird aufgerufen.

Während der Umstellung werden die Root-Aggregate des DR-Partners nicht online gestellt.

Der `metrocluster switchover` Command Switches über die Nodes in allen DR-Gruppen in der MetroCluster Konfiguration. In einer MetroCluster Konfiguration mit acht Nodes wechselt sie beispielsweise über die Nodes in beiden DR-Gruppen.

Wenn ein Wechsel ausschließlich für Services zum Remote-Standort erfolgt, sollte eine ausgehandelte Umschaltung ohne Fencing des Standorts durchgeführt werden. Falls Storage oder Geräte unzuverlässig sind, sollten Sie den Disaster-Standort einschiebern und anschließend eine ungeplante Umschaltung durchführen. Fechten verhindert RAID-Rekonstruktionen beim Einschalten der Festplatten mit gestaffelter Weise.

Dieses Verfahren sollte nur verwendet werden, wenn der andere Standort stabil ist und nicht offline gebracht werden soll.

Verfügbarkeit von Befehlen während der Umschaltung

Die folgende Tabelle zeigt die Verfügbarkeit von Befehlen während der Umschaltung:

Befehl	Gesteigerte
`storage aggregate create`	Sie können ein Aggregat erstellen: • Ist er im Besitz eines Node, der Teil des verbleibenden Clusters ist Sie können kein Aggregat erstellen: • Für einen Node am Disaster-Site • Für einen Node, der Teil des verbleibenden Clusters ist
`storage aggregate delete`	Sie können ein Datenaggregat löschen.
`storage aggregate mirror`	Sie können einen Plex für ein nicht gespiegeltes Aggregat erstellen.
`storage aggregate plex delete`	Sie können einen Plex für ein gespiegeltes Aggregat löschen.

`vserver create`	Sie können eine SVM erstellen: • Befindet sich das Root-Volume in einem Datenaggregat, das dem verbleibenden Cluster gehört Sie können keine SVM erstellen: • Befindet sich das Root-Volume in einem Datenaggregat im Eigentum des Disaster-Site-Clusters
`vserver delete`	Sie können SVMs mit Synchronisations- und synchronen Zielen löschen.
`network interface create -lif`	Sie können eine Daten-SVM-LIF sowohl für Sync-Source- als auch für Sync-Destination-SVMs erstellen.
`network interface delete -lif`	Sie können eine Daten-SVM-LIF sowohl für Sync-Source- als auch für Sync-Destination-SVMs löschen.
`volume create`	Sie können ein Volume sowohl für synchrone als auch für synchrone SVMs erstellen. • Bei einer synchronen SVM muss sich das Volume in einem Datenaggregat befinden, das dem verbleibenden Cluster gehört • Bei einer synchronen Ziel-SVM muss sich das Volume in einem Datenaggregat befinden, das dem Disaster-Site-Cluster gehört
`volume delete`	Sie können ein Volume sowohl für synchrone als auch für synchrone SVMs löschen.
`volume move`	Sie können ein Volume sowohl für synchrone als auch für synchrone SVMs verschieben. • Bei einer SVM mit synchroner Quelle muss das noch funktionsfähige Cluster das Zielaggregat sein • Bei einer SVM mit synchronem Ziel muss das Ziel-Aggregat im Disaster-Site-Cluster vorhanden sein
`snapmirror break`	Sie können eine SnapMirror Beziehung zwischen einem Quell- und Zielendpunkt einer Datensicherungsspiegelung unterbrechen.

Unterschiede bei der Umschaltung zwischen MetroCluster FC- und IP-Konfigurationen

In MetroCluster IP Konfigurationen ist der Zugriff auf die Remote-Festplatten über die Nodes des Remote-DR-Partners als iSCSI-Ziele möglich. Wenn die Remote-Nodes bei einem Switchover heruntergefahren werden, ist der Zugriff auf die Remote-Festplatten nicht möglich. Dies führt zu Unterschieden bei den MetroCluster FC-Konfigurationen:

- Gespiegelte Aggregate, die im Besitz des lokalen Clusters sind, werden herabgestuft.
- Gespiegelte Aggregate, die vom Remote-Cluster umgeschaltet wurden, werden herabgestuft.

> Wenn nicht gespiegelte Aggregate in einer MetroCluster IP-Konfiguration unterstützt werden, kann nicht auf die nicht gespiegelten Aggregate zugegriffen werden, die nicht vom Remote-Cluster umgeschaltet sind.

Änderungen am Festplattenbesitz während HA Takeover und MetroCluster Switchover in einer MetroCluster Konfiguration mit vier Nodes

Die Eigentumsrechte an Festplatten ändern sich vorübergehend automatisch während der Hochverfügbarkeit und im MetroCluster-Betrieb. Es ist hilfreich zu wissen, wie das System den Knoten verfolgt, der welche Platten besitzt.

In ONTAP wird die eindeutige System-ID eines Controller-Moduls (bezogen auf die NVRAM-Karte oder NVMEM-Platine eines Node) verwendet, um zu ermitteln, welcher Node auf einer bestimmten Festplatte besitzt. Je nach HA- oder DR-Status des Systems kann sich das Eigentum an der Festplatte vorübergehend ändern. Wenn sich das Eigentum aufgrund einer HA Übernahme oder einer DR-Umschaltung ändert, zeichnet das System auf, welcher Node der ursprüngliche (sogenannte „`Home`“) Eigentümer der Festplatte ist, sodass das System nach HA Giveback oder DR-Switchback die Eigentümerschaft zurückgeben kann. Das System verwendet die folgenden Felder, um den Festplattenbesitzer nachzuverfolgen:

- Eigentümer
- Hausbesitzer
- DR Home Inhaber

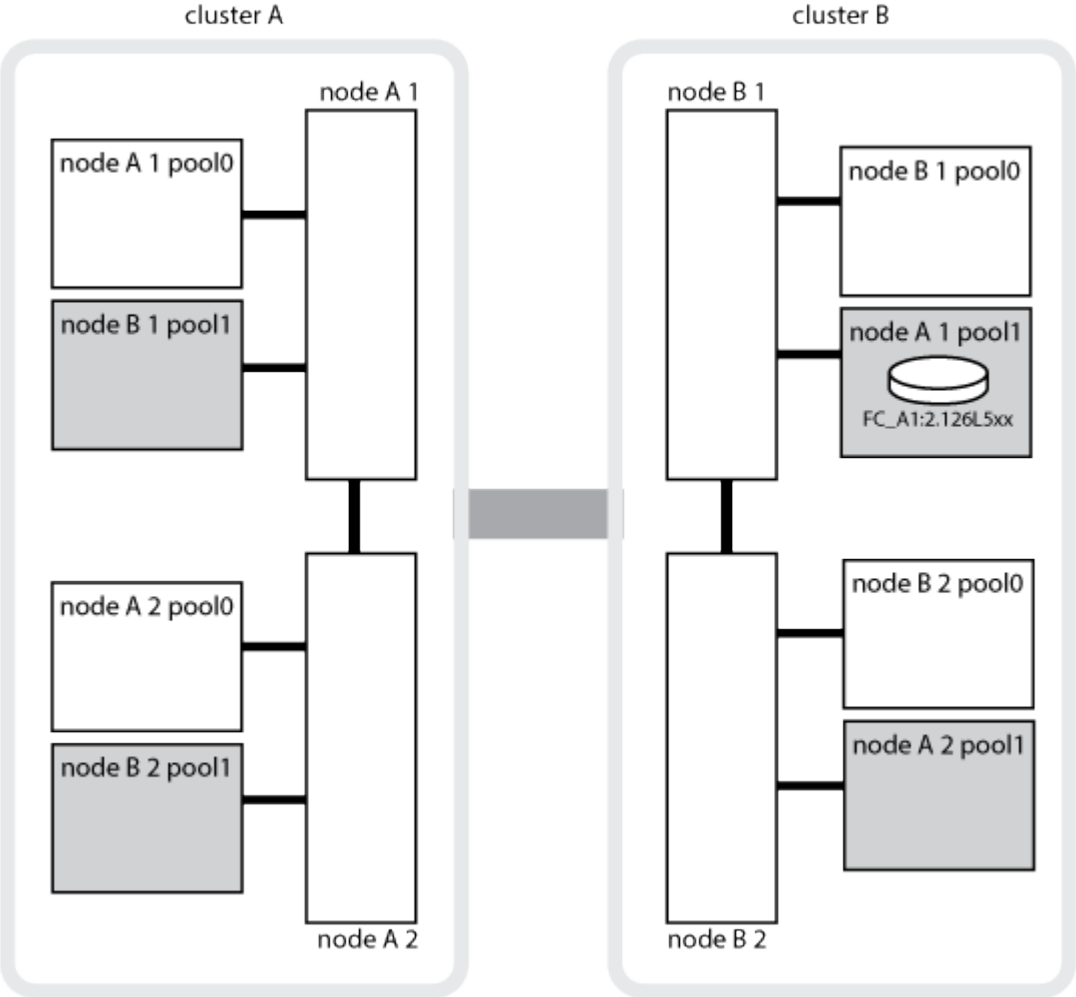
Bei der MetroCluster Konfiguration kann ein Node im Falle einer Umschaltung das Eigentum eines Aggregats übernehmen, das ursprünglich Nodes im Partner-Cluster gehörte. Solche Aggregate werden als Cluster-fremde Aggregate bezeichnet. Das Alleinstellungsmerkmal eines Cluster-fremden Aggregats besteht darin, dass es sich um ein Aggregat handelt, das derzeit dem Cluster nicht bekannt ist. Mithilfe des Felds „DR Home Owner“ wird also gezeigt, dass es sich um einen Node vom Partner-Cluster befindet. Wenn ein herkömmliches Aggregat innerhalb eines HA-Paars identifiziert wird, werden die Werte für Eigentümer und Home-Eigentümer unterschiedlich sein. Die Werte für Eigentümer und Home-Eigentümer sind jedoch für ein Cluster-fremdes Aggregat identisch. Sie können daher durch den Wert des DR-Home-Inhabers ein Cluster-fremdes Aggregat identifizieren.

Wenn sich der Zustand des Systems ändert, ändern sich die Werte der Felder, wie in der folgenden Tabelle dargestellt:

Feld	Wert während…			
	Normaler Betrieb	Lokale HA-Übernahme	MetroCluster Umschaltung	Übernahme während Switchover

Eigentümer	ID des Node, der Zugriff auf die Festplatte hat.	ID des HA-Partners, der vorübergehend auf die Festplatte zugreifen kann.	ID des DR-Partners, der vorübergehend auf die Festplatte zugreifen kann.	ID des DR-Hilfspartners, der vorübergehend Zugriff auf die Festplatte hat.
Hausbesitzer	ID des ursprünglichen Eigentümers der Festplatte innerhalb des HA-Paars.	ID des ursprünglichen Eigentümers der Festplatte innerhalb des HA-Paars.	ID des DR-Partners, der während der Umschaltung der Home Owner im HA-Paar ist.	ID des DR-Partners, der während der Umschaltung der Home Owner im HA-Paar ist.
DR Home Inhaber	Leer	Leer	ID des ursprünglichen Besitzers der Festplatte innerhalb der MetroCluster-Konfiguration.	ID des ursprünglichen Besitzers der Festplatte innerhalb der MetroCluster-Konfiguration.

Die folgende Abbildung und Tabelle zeigen ein Beispiel für Änderungen des Eigentumsrechte bei einer Platte im Disk-Pool1 von Node_A_1, die sich physisch in Cluster_B befindet



Der Status der MetroCluster	Eigentümer	Hausbesitzer	DR Home Inhaber	Hinweise
Normal, wenn alle Nodes voll funktionsfähig sind.	Node_A_1	Node_A_1	Keine Angabe	
Durch lokale HA-Übernahme hat Node_A_2 Festplatten übernommen, die zu seinem HA Partner Node_A_1 gehören.	Node_A_2	Node_A_1	Keine Angabe	
DR-Umschaltung, Node_B_1 hat Festplatten übernommen und gehört zum DR-Partner Node_A_1.	Knoten_B_1	Knoten_B_1	Node_A_1	Die ursprüngliche ID des Home-Knotens wird in das Feld „DR Home-Eigentümer“ verschoben. Nach dem Wechsel zum Aggregat oder der Reparatur kehrt das Eigentum zurück zu Node_A_1.
Bei DR-Umschaltung und lokalem HA-Takeover (doppelter Ausfall) hat Node_B_2 Festplatten übernommen, die zum HA Node_B_1 gehören.	Knoten_B_2	Knoten_B_1	Node_A_1	Nach dem Giveback geht die Eigentümerschaft zurück auf Node_B_1. Nach dem Umkehren oder Healing geht das Eigentum zurück zu Node_A_1.
Nach dem HA-Giveback und dem DR-Wechsel waren alle Nodes voll funktionsfähig.	Node_A_1	Node_A_1	Keine Angabe	

Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten

Wenn Ihre Konfiguration nicht gespiegelte Aggregate umfasst, müssen potenzielle Zugriffsprobleme nach dem Switchover berücksichtigt werden.

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.

Ist dies nicht der Fall, können Nodes am verbleibenden Standort aufgrund einer „Panik mit mehreren Festplatten“ ausfallen. Wenn Switched-over-nicht gespiegelte Aggregate offline geschaltet werden oder aufgrund des Verlusts der Verbindung zum Storage am DR-Standort aufgrund des Stromausfalls oder des Verlusts von ISLs fehlen.

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 verhandelt es Vetos. Der `metrocluster check` Befehl 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

Eine LUN sollte sich 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.

Automatisches, ungeplantes Switchover in MetroCluster FC-Konfigurationen

In MetroCluster FC-Konfigurationen können bestimmte Szenarien eine automatische, ungeplante Umschaltung (AUSO) auslösen, falls ein standortweiter Controller-Ausfall auftritt. So ist ein unterbrechungsfreier Betrieb möglich. AUSO kann auf Wunsch deaktiviert werden.

> Die automatische ungeplante Umschaltung wird in MetroCluster IP-Konfigurationen nicht unterstützt.

In einer MetroCluster FC-Konfiguration kann eine AUSO ausgelöst werden, wenn alle Nodes an einem Standort aus den folgenden Gründen ausgefallen sind:

- Schalten Sie aus
- Stromausfall
- Panik

> In einer MetroCluster FC-Konfiguration mit acht Nodes können Sie eine Option zum Auslösen eines AUSO einstellen, wenn beide Nodes eines HA-Paars ausfallen.

Da in einer MetroCluster-Konfiguration mit zwei Nodes kein lokaler HA Failover verfügbar ist, führt das System einen AUSO aus, um einen Fortsetzung des Betriebs nach einem Controller-Ausfall zu ermöglichen. Diese Funktionalität ähnelt der HA-Takeover-Fähigkeit in einem HA-Paar. In einer MetroCluster-Konfiguration mit zwei Knoten kann eine AUSO in den folgenden Szenarien ausgelöst werden:

- Node wird heruntergefahren
- Stromausfall des Node
- Node-Panic
- Neubooten des Node

Wenn ein AUSO auftritt, wird der Festplattenbesitzer für die Pool0- und Pool1-Festplatten des gestörten Knotens auf den Disaster Recovery-Partner (DR) umgestellt. Durch diese Änderung im Eigentumsrecht wird verhindert, dass die Aggregate nach der Umschaltung in einen eingeschränkten Zustand versetzt werden.

Nach der automatischen Umschaltung müssen Sie die Healing- und Switchback-Vorgänge manuell durchführen, um den Controller wieder in den normalen Betrieb zu bringen.

Hardwareunterstützte AUSO-Systeme in MetroCluster-Konfigurationen mit zwei Nodes

In einer MetroCluster-Konfiguration mit zwei Nodes überwacht der Service-Prozessor (SP) des Controller-Moduls die Konfiguration. In manchen Fällen kann der SP einen Fehler schneller erkennen als die ONTAP Software. In diesem Fall löst der SP AUSO aus. Diese Funktion wird automatisch aktiviert.

Der SP sendet und empfängt SNMP-Datenverkehr an und von seinem DR-Partner, um seinen Zustand zu überwachen.

Ändern der AUSO-Einstellung in MetroCluster FC-Konfigurationen

AUSO ist standardmäßig auf „auso-on-Cluster-Disaster“ eingestellt. Der Status kann im angezeigt werden `metrocluster show` Befehl.

> Die AUSO-Einstellung gilt nicht für MetroCluster-IP-Konfigurationen.

Sie können AUSO mit dem deaktivieren `metrocluster modify -auto-switchover-failure-domain auto-disabled` Befehl. Dieser Befehl verhindert das Auslösen von AUSO bei einem DR-standortweiten Controller-Ausfall. Sie sollte auf beiden Seiten ausgeführt werden, wenn Sie AUSO auf beiden Seiten deaktivieren möchten.

AUSO kann mit dem wieder aktiviert werden `metrocluster modify -auto-switchover-failure -domain auso-on-cluster-disaster` Befehl.

AUSO kann auch auf „`auso-on-dr-Group-Disaster`“ eingestellt werden. Dieser Befehl Advance Level löst AUSO bei HA Failover an einem Standort aus. Es sollte auf beiden Seiten mit dem laufen `metrocluster modify -auto-switchover-failure-domain auso-on-dr-group-disaster` Befehl.

Die AUSO-Einstellung während der Umschaltung

Bei einer Umschaltung wird die AUSO-Einstellung intern deaktiviert, da ein Standort nicht automatisch umgeschaltet werden kann, wenn ein Standort umgeschaltet wird.

Wiederherstellung von AUSO

Zur Wiederherstellung nach einer AUSO führen Sie dieselben Schritte aus wie bei einer geplanten Umschaltung.

"Umschaltung für Tests oder Wartung"

Mediator-gestützte automatische, ungeplante Umschaltung in MetroCluster IP-Konfigurationen

"Erfahren Sie, wie der ONTAP Mediator die automatische ungeplante Umschaltung in MetroCluster IP-Konfigurationen unterstützt".

Was geschieht während der Reparatur (MetroCluster FC-Konfigurationen)?

Bei der Reparatur von MetroCluster FC-Konfigurationen erfolgt die Resynchronisierung der gespiegelten Aggregate in einem phasenweisen Prozess, der die Nodes am reparierten Disaster Site für einen Switchback vorbereitet. Hierbei handelt es sich um ein geplantes Ereignis, wodurch Sie alle Schritte vollständig kontrollieren können, um die Ausfallzeiten zu minimieren. Die Reparatur ist ein zweistufiger Prozess, der im Storage- und im Controller-Bereich stattfindet.

Reparatur von Daten-Aggregaten

Nachdem das Problem am Disaster-Standort gelöst ist, starten Sie die Storage-Heilungsphase:

1. Überprüft, ob alle Nodes am verbleibenden Standort betriebsbereit sind.
2. Ändert den Besitz aller Pool-0-Festplatten am Disaster-Site, einschließlich Root-Aggregaten.

Während dieser Phase der Fehlerbehebung werden gespiegelte Aggregate vom RAID-Subsystem resynchronisiert, und das WAFL-Subsystem gibt die nvsave Dateien der gespiegelten Aggregate wieder, bei denen zum Zeitpunkt der Umschaltung ein Pool 1 Plex ausfällt.

Wenn einige Komponenten des Quell-Storage ausgefallen sind, meldet der Befehl die Fehler auf den entsprechenden Ebenen: Storage, Sanown oder RAID.

Wenn keine Fehler gemeldet werden, werden die Aggregate erfolgreich neu synchronisiert. Dieser Vorgang kann manchmal Stunden dauern.

"Reparieren der Konfiguration"

Fehlerbehebung im Root-Aggregat

Nach der Synchronisation der Aggregate starten Sie die Controller-Heilungsphase, indem Sie die CFO-Aggregate und Root-Aggregate an ihre jeweiligen DR-Partner geben.

"Reparieren der Konfiguration"

Was geschieht während der Reparatur (MetroCluster IP-Konfigurationen)?

Bei der Reparatur in MetroCluster IP-Konfigurationen erfolgt die Resynchronisierung der gespiegelten Aggregate in einem phasenweisen Prozess, der die Nodes am reparierten Disaster-Standort auf den Wechsel zurück vorbereitet. Hierbei handelt es sich um ein geplantes Ereignis, wodurch Sie alle Schritte vollständig kontrollieren können, um die Ausfallzeiten zu minimieren. Die Reparatur ist ein zweistufiger Prozess, der im Storage- und im Controller-Bereich stattfindet.

Unterschiede zu MetroCluster FC-Konfigurationen

In MetroCluster IP-Konfigurationen müssen Sie die Nodes im Disaster-Site-Cluster booten, bevor der Heilvorgang durchgeführt wird.

Die Nodes am Disaster-Site-Cluster müssen ausgeführt werden, damit bei der erneuten Synchronisierung von Aggregaten auf die Remote-iSCSI-Festplatten zugegriffen werden kann.

Wenn die Nodes des Disaster-Standortes nicht ausgeführt werden, schlägt der Heilvorgang fehl, da der Disaster-Node die erforderlichen Änderungen an den Festplatteneigentum nicht ausführen kann.

Reparatur von Daten-Aggregaten

Nachdem das Problem am Disaster-Standort gelöst ist, starten Sie die Storage-Heilungsphase:

1. Überprüft, ob alle Nodes am verbleibenden Standort betriebsbereit sind.
2. Ändert den Besitz aller Pool-0-Festplatten am Disaster-Site, einschließlich Root-Aggregaten.

Während dieser Phase der Fehlerbehebung werden gespiegelte Aggregate vom RAID-Subsystem resynchronisiert, und das WAFL-Subsystem gibt die nvsave Dateien der gespiegelten Aggregate wieder, bei denen zum Zeitpunkt der Umschaltung ein Pool 1 Plex ausfällt.

Wenn einige Komponenten des Quell-Storage ausgefallen sind, meldet der Befehl die Fehler auf den entsprechenden Ebenen: Storage, Sanown oder RAID.

Wenn keine Fehler gemeldet werden, werden die Aggregate erfolgreich neu synchronisiert. Dieser Vorgang kann manchmal Stunden dauern.

"Reparieren der Konfiguration"

Fehlerbehebung im Root-Aggregat

Nach der Synchronisierung der Aggregate führen Sie die Heilungsphase des Root-Aggregats durch. In MetroCluster IP-Konfigurationen bestätigt diese Phase, dass die Aggregate bereits geheilt wurden.

"Reparieren der Konfiguration"

Automatisches Heilen von Aggregaten in MetroCluster IP-Konfigurationen nach dem Switchover

Ab ONTAP 9.5 erfolgt die Reparatur während ausgehandelten Switchover-Operationen auf MetroCluster IP-Konfigurationen automatisch. Ab ONTAP 9.6 wird die automatische Reparatur nach ungeplanten Switchover unterstützt. Dadurch entfällt die Anforderung, das auszulassen `metrocluster heal` Befehle.

Automatische Reparatur nach ausgehandelter Umschaltung (beginnend mit ONTAP 9.5)

Nachdem eine ausgehandelte Umschaltung durchgeführt wurde (ein Befehl zur Umschaltung ohne die Option -Forced-on-Disaster True), vereinfacht die automatische Funktion zur Fehlerbehebung die Schritte, die erforderlich sind, um das System wieder in den normalen Betrieb zu bringen. Bei Systemen mit automatischer Fehlerbehebung tritt nach dem Switchover Folgendes auf:

- Die Knoten am Disaster-Standort bleiben verfügbar.

  Da sie sich im Umschaltzustand befinden, stellen sie keine Daten aus ihren lokalen gespiegelten Plexen

bereit.

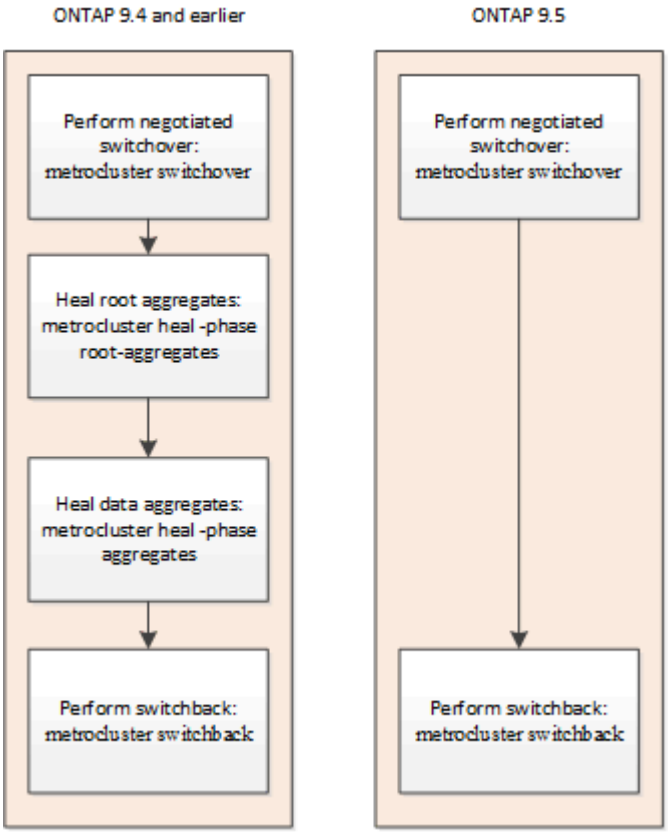
- Die Nodes des Disaster-Standorts werden in den Status „`waiting for switchback`“ verschoben.

  Sie können den Status der Disaster-Site-Nodes mit dem Befehl „MetroCluster Operation show“ bestätigen.

- Sie können den Switchback-Vorgang ausführen, ohne die Healing-Befehle eingeben zu müssen.

Diese Funktion gilt für MetroCluster IP Konfigurationen mit ONTAP 9.5 und höher. Dies gilt nicht für MetroCluster FC-Konfigurationen.

Die manuellen Healing-Befehle sind für MetroCluster IP-Konfigurationen mit ONTAP 9.4 und früher weiterhin erforderlich.



Automatische Heilung nach außerplanmäßiger Umschaltung (beginnend mit ONTAP 9.6)

MetroCluster IP-Konfigurationen ab ONTAP 9.6 unterstützen die automatische Selbstreparatur nach einer ungeplanten Umschaltung. Eine ungeplante Umschaltung ist eine, bei der Sie das ausgeben `switchover` Befehl mit dem `-forced-on-disaster true` Option.

Die automatische Reparatur nach einer ungeplanten Umschaltung wird von MetroCluster FC-Konfigurationen nicht unterstützt. Die manuellen Heilungsbefehle sind nach nicht ungeplanter Umschaltung auf MetroCluster IP-Konfigurationen mit ONTAP 9.5 und früher weiterhin erforderlich.

Bei Systemen mit ONTAP 9.6 und höher tritt nach der ungeplanten Umschaltung Folgendes auf:

- Je nach Umfang des Ausfalls können die Nodes des Disaster-Standorts ausgefallen sein.

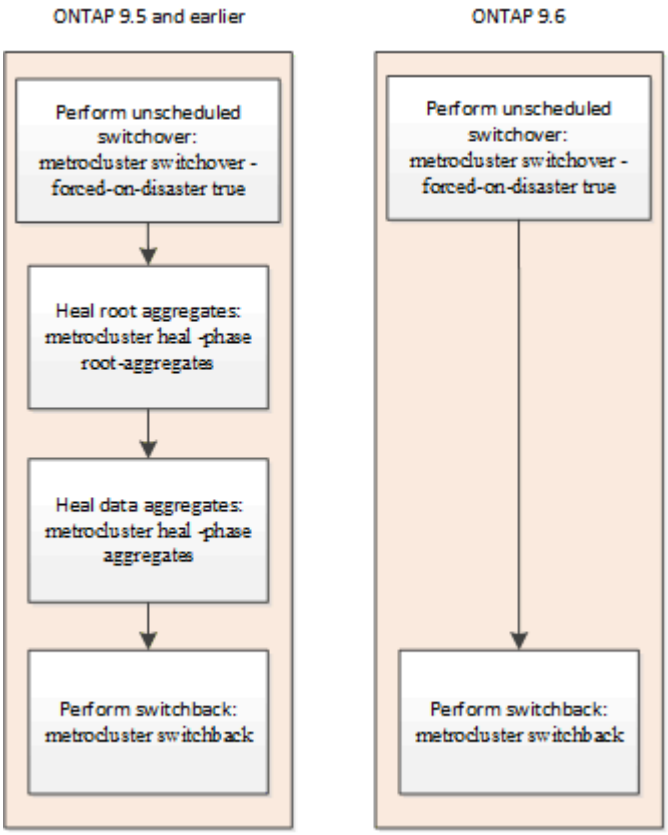
  Da sie den Umschaltzustand aufweisen, stellen sie keine Daten über ihre lokalen gespiegelten Plexe bereit, selbst wenn sie eingeschaltet sind.

- Wenn die Disaster-Standorte ausgefallen sind und nach dem Booten die Nodes des Disaster-Standorts in den Status „`waiting for switchback`“ verschoben werden.

  Wenn die Disaster-Standorte weiter genutzt wurden, werden sie sofort in den Status „`Waiting for Switchback`“ versetzt.

- Die Heilungsvorgänge werden automatisch durchgeführt.

  Sie können den Status der Disaster-Standort-Nodes bestätigen und diese Heilungsvorgänge erfolgreich durchführen, indem Sie den verwenden `metrocluster operation show` Befehl.



Wenn die automatische Reparatur fehlschlägt

Wenn der automatische Heilvorgang aus irgendeinem Grund fehlschlägt, müssen Sie den ausgeben `metrocluster heal` Befehle, die manuell wie in ONTAP-Versionen vor ONTAP 9.6 ausgeführt werden. Sie können das verwenden `metrocluster operation show` Und `metrocluster operation history show -instance` Befehle, um den Status der Reparatur zu überwachen und die Ursache eines Fehlers zu bestimmen.

Erstellen von SVMs für eine MetroCluster-Konfiguration

Sie können SVMs für eine MetroCluster-Konfiguration erstellen, um synchrones Disaster Recovery und Hochverfügbarkeit von Daten auf Clustern zu gewährleisten, die für eine MetroCluster-Konfiguration eingerichtet sind.

- Die beiden Cluster müssen sich in einer MetroCluster-Konfiguration enthalten.
- Aggregate müssen in beiden Clustern verfügbar und online sein.

- Bei Bedarf müssen IPspaces mit den gleichen Namen auf beiden Clustern erstellt werden.
- Wenn einer der Cluster, der die MetroCluster Konfiguration bildet, neu gestartet wird, ohne Umschaltung zu nutzen, dann können die Sync-Source-SVMs statt „`sTop`“ als „`sTarted`“ online geschaltet werden.

Wenn Sie eine SVM auf einem der Cluster in einer MetroCluster-Konfiguration erstellen, wird die SVM als Quell-SVM erstellt, und die Partner-SVM wird automatisch mit demselben Namen, jedoch mit dem Suffix „`-mc`“ auf dem Partner-Cluster erstellt. Enthält der SVM-Name einen Zeitraum, wird das Suffix „`-mc`“ vor dem ersten Zeitraum angewendet, z. B. SVM-MC.DNS.NAME.

In einer MetroCluster Konfiguration können Sie 64 SVMs auf einem Cluster erstellen. Eine MetroCluster Konfiguration unterstützt 128 SVMs.

1. Verwenden Sie die `vserver create` Befehl.

   Im folgenden Beispiel wird die SVM mit dem Subtyp „`sync-source`“ auf der lokalen Site und der SVM mit dem Untertyp „`sync-Destination`“ auf der Partnerseite angezeigt:

   ```
   cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -aggregate
   aggr1
   -rootvolume-security-style mixed
   [Job 196] Job succeeded:
   Vserver creation completed
   ```

   Die SVM „`vs4`“ wird auf der lokalen Website erstellt und die SVM „`vs4-mc`“ auf der Partner-Website erstellt.

2. Sie können die neu erstellten SVMs anzeigen.

   - Überprüfen Sie im lokalen Cluster den Konfigurationsstatus von SVMs:

     ```
     metrocluster vserver show
     ```

     Das folgende Beispiel zeigt den Konfigurationsstatus der Partner-SVMs:

     ```
     cluster_A::> metrocluster vserver show

                          Partner    Configuration
     Cluster     Vserver   Vserver    State
     ---------  --------  --------- -----------------
     cluster_A   vs4       vs4-mc     healthy
     cluster_B   vs1       vs1-mc     healthy
     ```

   - Überprüfen Sie in den lokalen Clustern und in den Partner-Clustern den Status der neu konfigurierten SVMs:

     ```
     vserver show command
     ```

     Im folgenden Beispiel werden der Administrations- und Betriebsstatus der SVMs angezeigt:

```
cluster_A::> vserver show

                               Admin   Operational Root
Vserver Type  Subtype         State   State       Volume     Aggregate
------- ----- -------        ------- --------    -----------
----------
vs4     data  sync-source   running   running    vs4_root   aggr1

cluster_B::> vserver show

                                 Admin   Operational  Root
Vserver Type  Subtype           State   State        Volume
Aggregate
------- ----- -------           ------  ---------    -----------
----------
vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
```

Die Erstellung einer SVM kann fehlschlagen, wenn ein Zwischenbetrieb wie die Erstellung des Root-Volumes fehlschlägt und die SVM sich im Status „`initializing`“ befindet. Sie müssen die SVM löschen und erneut erstellen.

Die SVMs für die MetroCluster-Konfiguration werden mit einer Root-Volume-Größe von 1 GB erstellt. Die SVM für die Synchronisierung hat den Status „`running`“ und die SVM für das synchrone Ziel befindet sich im Status „`stogedated`“.

Was passiert während eines Switchback

Nachdem der Disaster-Standort wiederhergestellt und die Aggregate geheilt sind, gibt der MetroCluster-Rückvermittlungsprozess den Storage- und Client-Zugriff vom Disaster Recovery-Standort auf das Home Cluster zurück.

Der `metrocluster switchback` Der Befehl gibt den primären Standort in den vollen, normalen MetroCluster-Betrieb zurück. Jegliche Konfigurationsänderungen werden an die ursprünglichen SVMs weitergegeben. Der Datenserverbetrieb wird anschließend an die synchronen Quell-SVMs am DR-Standort zurückgegeben und die mit der Synchronisierung am verbleibenden Standort ausgeführten SVMs werden deaktiviert.

Wenn SVMs auf dem verbleibenden Standort gelöscht wurden, während die MetroCluster Konfiguration sich im Switchover-Status befand, führt der Switch-Back-Prozess folgende Vorgänge aus:

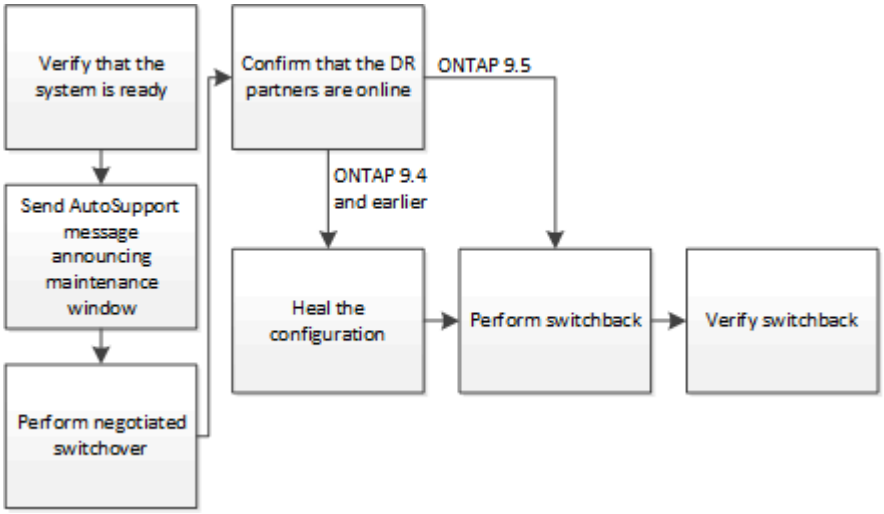
- Löscht die entsprechenden SVMs auf dem Partnerstandort (der ehemalige Disaster-Standort).
- Löscht alle Peering-Beziehungen der gelöschten SVMs.

Durchführung von Umschaltung, Healing und Switchback

Umschaltung für Tests oder Wartung

Umschaltung für Tests oder Wartung

Wenn Sie die MetroCluster Funktionalität testen oder geplante Wartungsarbeiten durchführen möchten, können Sie eine ausgehandelte Umschaltung durchführen, bei der ein Cluster ordnungsgemäß auf das Partner-Cluster umgeschaltet wird. Anschließend können Sie die Konfiguration heilen und wieder einschalten.



Ab ONTAP 9.6 können Switchover- und Switchback-Vorgänge in MetroCluster IP-Konfigurationen mit ONTAP System Manager durchgeführt werden.

Einschränkungen, wenn die MetroCluster-Konfiguration umgeschaltet wird

Wenn sich das System im Umschaltvorgang befindet, sollten bestimmte Vorgänge nicht ausgeführt werden. Informieren Sie sich über eingeschränkte Vorgänge, wenn das System umgeschaltet wird.

Eingeschränkte Vorgänge bei Umschaltung

Die folgenden Vorgänge werden nicht unterstützt, wenn sich das System in Umschaltung befindet:

- Erstellen oder Löschen von Aggregaten und Volumes
- Erstellen oder Löschen von SVMs
- Erstellen oder Löschen von LIFs
- Hinzufügen oder Entfernen von Festplatten (nur wenn Sie sie im Rahmen eines Wiederherstellungsverfahrens ersetzen)
- Durchführung von Konfigurationsänderungen an SnapMirror SVM DR

- Ändern vorhandener Broadcast-Domänen oder Erstellen neuer Broadcast-Domänen
- Ändern von Netzwerk-Subnetzen

Hardware-Austausch bei Umschaltung

Gehen Sie wie folgt vor, um die Controller-Hardware auszutauschen, wenn sich das System im Umschalten befindet:

- Wenn Sie einen Controller des gleichen Typs am Standort austauschen müssen, der sich nicht in Umschaltung befindet, gehen Sie wie unter "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"beschrieben vor.
  - Wenn Sie die Controller-Module und das Chassis austauschen müssen, während die Nodes am verbleibenden Standort umgeschaltet werden, fahren Sie beide Controller herunter, und führen Sie dann das Verfahren unter "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"aus.
- Wenn Sie einen Controller durch einen anderen Controller-Typ ersetzen müssen, befolgen Sie das Verfahren für Ihre Konfiguration in "Wählen Sie ein Controller-Upgrade-Verfahren".
  - Wenn sich Ihr System aufgrund eines Controller-Ausfalls im Umschalten befindet oder wenn bei Ihnen ein Controller-Ausfall auftritt, müssen Sie zuerst die Controller-Hardware austauschen, einen Switchback durchführen und dann ein Controller-Upgrade durchführen:
    i. Gehen Sie wie folgt "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"vor, um die Controller-Hardware zu ersetzen und den Switchback durchzuführen.
    ii. Führen Sie nach dem Austausch der Hardware ein Controller-Upgrade gemäß den Verfahren in "Wählen Sie ein Controller-Upgrade-Verfahren"durch.

Überprüfung, ob das System bereit für eine Umschaltung ist

Sie können das verwenden `-simulate` Option, um eine Vorschau der Ergebnisse eines Umschaltvorgangs anzuzeigen. Durch eine Überprüfung können Sie überprüfen, ob die meisten Voraussetzungen für einen erfolgreichen Lauf erfüllt sind, bevor Sie den Vorgang starten. Geben Sie diese Befehle von der Site aus ein, die in Betrieb bleibt:

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`
2. Simulieren Sie einen Switchover-Betrieb am Standort: `metrocluster switchover -simulate`
3. Überprüfen Sie die zurückgegebene Ausgabe.

   Der Ausgang zeigt an, ob ein Vetos einen Umschaltvorgang verhindern würde. Jedes Mal, wenn Sie einen MetroCluster-Vorgang durchführen, müssen Sie eine Reihe von Kriterien für den Erfolg des Vorgangs überprüfen. Ein „`vebis`“ ist ein Mechanismus zum Verbot der Operation, wenn ein oder mehrere der Kriterien nicht erfüllt sind. Es gibt zwei Arten von Veto: Ein “soft” Veto und ein “Hard” Veto. Sie können ein weiches Veto außer Kraft setzen, jedoch kein hartes Veto. Um beispielsweise eine ausgehandelte Umschaltung in einer MetroCluster Konfiguration mit vier Nodes durchzuführen, ist ein Kriterium, dass alle Nodes ordnungsgemäß ausgeführt werden. Angenommen, ein Node ist ausgefallen und wurde von seinem HA-Partner übernommen. Der Switchover-Vorgang wird wegen seines harten Vetos schwierig, da es ein wichtiges Kriterium ist, dass alle Knoten in Betrieb und Zustand sein müssen. Da dies ein harter Veto ist, können Sie das Veto nicht überschreiben.

   ⓘ Es ist am besten, kein Veto außer Kraft zu setzen.

Beispiel: Verifizierungsergebnisse

Das folgende Beispiel zeigt die Fehler, die bei der Simulation eines Switchover-Vorgangs auftreten:

```
cluster4::*> metrocluster switchover -simulate

[Job 126] Preparing the cluster for the switchover operation...
[Job 126] Job failed: Failed to prepare the cluster for the switchover
operation. Use the "metrocluster operation show" command to view detailed
error
information. Resolve the errors, then try the command again.
```

> Ausgehandelte Switchover- und Switchback-Funktion schlägt fehl, bis Sie alle ausgefallenen Festplatten ersetzen. Sie können Disaster Recovery durchführen, nachdem Sie die ausgefallenen Festplatten ersetzt haben. Wenn Sie die Warnung für fehlerhafte Festplatten ignorieren möchten, können Sie ein weiches Veto für die ausgehandelte Umschaltung hinzufügen und wieder zurückwechseln.

Senden einer individuellen AutoSupport Nachricht vor der ausgehandelten Umschaltung

Bevor Sie eine Umschaltung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über laufende Wartungsarbeiten zu informieren. Die ausgehandelte Umschaltung kann zu Plex- oder MetroCluster-Betriebsausfällen führen, die AutoSupport Meldungen auslösen. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei Site_A beim Cluster an
2. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

   Maintenance-Fenster in Stunden gibt die Länge des Wartungsfensters an und kann maximal 72 Stunden betragen. Wenn die Wartung vor Ablauf der Zeit abgeschlossen ist, können Sie mit dem Befehl angeben, dass der Wartungszeitraum beendet ist:`system node autosupport invoke -node * -type all -message MAINT=end`
3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Durchführen einer ausgehandelten Umschaltung

Bei einer ausgehandelten Umschaltung werden die Prozesse am Partnerstandort ordnungsgemäß heruntergefahren und dann die Betriebsvorgänge vom Kundenstandort umgestellt. Sie können eine ausgehandelte Umschaltung verwenden, um

Wartungsarbeiten an einem MetroCluster Standort durchzuführen oder die Switchover-Funktionalität zu testen.

- Alle früheren Konfigurationsänderungen müssen abgeschlossen sein, bevor Sie einen Switchback-Vorgang durchführen.

  Damit wird der Wettbewerb mit dem ausgehandelten Switchover- oder Switchback-Betrieb vermieden.

- Alle zuvor heruntergekommen Nodes müssen gestartet werden und sich in einem Cluster-Quorum befinden.

  Weitere Informationen zum Clusterquorum finden Sie im Abschnitt „`Verständnis von Quorum und epsilon`“.

  "Systemadministration"

- Das Cluster-Peering-Netzwerk muss von beiden Standorten aus verfügbar sein.
- Auf allen Nodes in der MetroCluster Konfiguration muss dieselbe Version der ONTAP Software ausgeführt werden.
- Die Option Replication.create_Data_Protection_rels.enable muss auf BEIDE Standorte in einer MetroCluster-Konfiguration auf ON gesetzt werden, bevor eine neue SnapMirror-Beziehung erstellt wird.
- Bei einer MetroCluster-Konfiguration mit zwei Nodes sollte während eines Upgrades keine neue SnapMirror Beziehung erstellt werden, wenn zwischen den Standorten unterschiedliche Versionen von ONTAP vorhanden sind.
- Bei einer MetroCluster-Konfiguration mit vier Nodes werden die nicht übereinstimmenden Versionen von ONTAP zwischen den Standorten nicht unterstützt.

Der Recovery-Standort kann ein paar Stunden dauern, bis der Wechsel wieder in Betrieb ist.

Der MetroCluster Switchover-Befehl wechselt über die Nodes in allen DR-Gruppen in der MetroCluster Konfiguration. In einer MetroCluster Konfiguration mit acht Nodes wechselt sie beispielsweise über die Nodes in beiden DR-Gruppen.

Während der Vorbereitung und der Ausführung einer ausgehandelten Umschaltung müssen keine Konfigurationsänderungen an einem Cluster vorgenommen oder Takeover- oder Giveback-Vorgänge durchgeführt werden.

Für MetroCluster FC-Konfigurationen:

- 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.
- 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.

Für MetroCluster IP-Konfigurationen:

> Bevor Sie Wartungsarbeiten durchführen, müssen Sie die Überwachung entfernen, wenn die MetroCluster-Konfiguration mit dem Tiebreaker oder Mediator Utility überwacht wird."Vor der Durchführung von Wartungsarbeiten müssen Sie den ONTAP Mediator oder den Tiebreaker Monitoring entfernen"

- 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.

    i. Verwenden Sie den befehl MetroCluster Check run, MetroCluster Check show und MetroCluster Check config-Replication show, um sicherzustellen, dass keine Konfigurationsaktualisierungen ausgeführt werden oder ausstehen. Geben Sie diese Befehle von der Site aus ein, die in Betrieb bleibt.

    ii. Implementieren Sie die Umschaltung vom Standort, der weiterhin betriebsbereit ist: `metrocluster switchover`

    Der Vorgang kann einige Minuten dauern.

    iii. Überwachen Sie den Abschluss der Umschaltung: `metrocluster operation show`

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

    iv. Wiederherstellung beliebiger SnapMirror oder SnapVault Konfigurationen

Vergewissern Sie sich, dass die SVMs ausgeführt werden und die Aggregate online sind

Nach Abschluss der Umschaltung sollten Sie sicherstellen, dass die DR-Partner Eigentum an den Festplatten haben und die Partner-SVMs online sind.

Wenn Sie den Befehl Storage Aggregate Plex show nach einer MetroCluster-Umschaltung ausführen, ist der Status von Plex0 des über das Root-Aggregat umgeschaltet unbestimmt und wird als fehlgeschlagen angezeigt. Während dieser Zeit wird die umschaltete Root nicht aktualisiert. Der tatsächliche Status dieses Plex kann nur nach der MetroCluster-Heilungsphase ermittelt werden.

Schritte

1. Überprüfen Sie, ob die Aggregate mithilfe des Storage Aggregate show-Befehls umgeschaltet wurden.

   In diesem Beispiel wurden die Aggregate umgeschaltet. Das Root-Aggregat (aggr0_b2) befindet sich in einem verschlechterten Zustand. Das Datenaggregat (b2_aggr2) befindet sich in einem gespiegelten, normalen Zustand:

```
cluster_A::*> storage aggregate show

.
.
.
mcc1-b Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b2    227.1GB   45.1GB    80% online       0 node_A_1
raid_dp,

mirror

degraded
b2_aggr1    227.1GB   200.3GB    20% online       0 node_A_1
raid_dp,

mirrored

normal
```

2. Bestätigen Sie, dass die sekundären SVMs mit dem vserver show-Befehl online geschaltet wurden.

   In diesem Beispiel wurden die zuvor inaktiv gewesen aktiven synchronen ZielSVMs am sekundären Standort aktiviert und verfügen über einen Administratorstatus:

```
cluster_A::*> vserver show
                                          Admin      Operational  Root
Name    Name
Vserver           Type  Subtype           State      State        Volume
Aggregate  Service Mapping
-----------       ----- ----------        ---------- -----------
--------- ---------- ------- -------
...
cluster_B-vs1b-mc data   sync-destination  running   running
vs1b_vol   aggr_b1   file    file
```

Heilt die Konfiguration

Reparieren Sie die Konfiguration in einer MetroCluster FC-Konfiguration

Reparieren der Konfiguration in einer MetroCluster FC-Konfiguration

Nach einer Umschaltung müssen Sie die MetroCluster Funktionen speziell mit den Heilungsoperationen wiederherstellen.

- Eine Umschaltung muss durchgeführt worden sein und der überlebende Standort muss Daten bereitstellen.
- Nodes am Disaster-Standort müssen angehalten oder deaktiviert werden.

  Sie dürfen während des Heilungsprozesses nicht vollständig gestartet werden.

- Storage am Disaster-Standort muss zugänglich sein (Shelfs werden hochgefahren, funktionieren und sind zugänglich).
- In Fabric-Attached MetroCluster-Konfigurationen müssen Inter-Switch-Links (ISLs) in Betrieb sein.
- In MetroCluster-Konfigurationen mit vier Nodes dürfen sich Nodes im verbleibenden Standort nicht im HA-Failover-Zustand befinden (alle Nodes müssen für jedes HA-Paar in Betrieb sein).

Die Reparatur muss zunächst auf den Datenaggregaten und anschließend auf den Root-Aggregaten durchgeführt werden.

Reparieren der Datenaggregate nach ausgehandelter Umschaltung

Nach Abschluss von Wartungsarbeiten oder Tests müssen die Datenaggregate repariert werden. In diesem Prozess werden die Datenaggregate neu synchronisiert und der Disaster-Standort wird auf den normalen Betrieb vorbereitet. Die Datenaggregate müssen vor dem Healing der Root-Aggregate repariert werden.

Alle Konfigurationsaktualisierungen im Remote-Cluster konnten erfolgreich auf das lokale Cluster repliziert werden. Im Rahmen dieses Verfahrens schalten Sie den Storage am Disaster Standort ein, jedoch nicht und dürfen die Controller-Module am DR-Standort nicht hochfahren.

Schritte

1. Stellen Sie sicher, dass die Umschaltung abgeschlossen wurde, indem Sie den MetroCluster Operation show-Befehl ausführen.

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. Synchronisieren Sie die Datenaggregate neu, indem Sie den Befehl MetroCluster Heal -Phase Aggregate aus dem verbleibenden Cluster ausführen.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Wenn das Heilen vetoed ist, haben Sie die Möglichkeit, den befehl MetroCluster Heal mit dem Parameter --override-vetoes erneut auszugeben. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

3. Überprüfen Sie, ob der Vorgang abgeschlossen wurde, indem Sie den Befehl „MetroCluster Operation show“ ausführen.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Überprüfen Sie den Status der Aggregate, indem Sie den Befehl „show“ für das Storage-Aggregat ausführen.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

5. Wenn Storage am Disaster Standort ausgetauscht wurde, müssen eventuell die Aggregate neu gespiegelt werden.

Heilen der Root-Aggregate nach ausgehandelter Umschaltung

Nachdem die Datenaggregate geheilt wurden, müssen Sie die Root-Aggregate heilen, um den Switchback-Betrieb zu ermöglichen.

Die Datenaggregationsphase des MetroCluster-Heilungsprozesses muss erfolgreich abgeschlossen sein.

Schritte

1. Schalten Sie die gespiegelten Aggregate zurück, indem Sie den MetroCluster Heal -Phase Root-Aggregates-Befehl ausführen.

   ```
   cluster_A::> metrocluster heal -phase root-aggregates
   [Job 137] Job succeeded: Heal Root Aggregates is successful
   ```

   Wenn das Heilen vetoed ist, haben Sie die Möglichkeit, den befehl MetroCluster Heal mit dem Parameter --override-vetoes erneut auszugeben. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

2. Bestätigen Sie den Abschluss des Heal-Vorgangs, indem Sie den Befehl „MetroCluster Operation show“ im gesunden Cluster ausführen:

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

3. Überprüfen und entfernen Sie ausgefallene Festplatten, die zum Disaster-Site gehören, indem Sie den folgenden Befehl am gesunden Standort eingeben: `disk show -broken`
4. Schalten Sie jedes Controller-Modul am Disaster-Standort aus oder starten Sie es.

   Wenn vom System die LOADER-Eingabeaufforderung angezeigt wird, führen Sie den aus `boot_ontap` Befehl.

5. Nachdem die Nodes gebootet wurden, überprüfen Sie, ob die Root-Aggregate gespiegelt wurden.

   Wenn beide Plexe vorhanden sind, erfolgt eine Neusynchronisierung automatisch, wenn die Plexe nicht synchronisiert werden. Wenn ein Plex fehlgeschlagen ist, muss dieser Plex zerstört sein und der Spiegel muss mit dem Storage Aggregat Mirror -aggregateaggregate-Name Befehl neu erstellt werden, um die Mirror-Beziehung wiederherzustellen.

Reparieren der Konfiguration in einer MetroCluster IP-Konfiguration (ONTAP 9.4 und früher)

Sie müssen die Aggregate heilen, um den Switchback-Betrieb zu ermöglichen.

> Auf MetroCluster IP-Systemen mit ONTAP 9.5 wird die Reparatur automatisch durchgeführt, und Sie können diese Aufgaben überspringen.

Vor der Durchführung des Heilverfahrens müssen die folgenden Bedingungen vorliegen:

- Eine Umschaltung muss durchgeführt worden sein und der überlebende Standort muss Daten bereitstellen.
- Storage-Shelfs am Disaster-Standort müssen hochgefahren, funktionsfähig und zugänglich sein.
- ISLs müssen verfügbar sein und in Betrieb sein.
- Nodes im verbleibenden Standort dürfen sich nicht im HA-Failover-Status befinden (beide Nodes müssen in Betrieb sein).

Diese Aufgabe bezieht sich ausschließlich auf MetroCluster IP-Konfigurationen, bei denen ONTAP Versionen vor 9.5 ausgeführt werden.

Dieses Verfahren unterscheidet sich von dem Heilverfahren für MetroCluster FC-Konfigurationen.

Schritte

1. Schalten Sie jedes Controller-Modul am Standort ein, der umgeschaltet wurde, und lassen Sie ihn vollständig booten.

   Wenn vom System die LOADER-Eingabeaufforderung angezeigt wird, führen Sie den aus `boot_ontap` Befehl.

2. Durchführen der Heilungsphase des Root-Aggregats: `metrocluster heal root-aggregates`

   ```
   cluster_A::> metrocluster heal root-aggregates
   [Job 137] Job succeeded: Heal Root-Aggregates is successful
   ```

   Wenn das Heilen vetoed ist, haben Sie die Möglichkeit, den befehl MetroCluster-Root-Aggregate heilen mit dem Parameter --override-vetoes erneut auszuführen. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

3. Synchronisieren Sie die Aggregate neu: `metrocluster heal aggregates`

   ```
   cluster_A::> metrocluster heal aggregates
   [Job 137] Job succeeded: Heal Aggregates is successful
   ```

   Wenn das Heilen vetoed ist, haben Sie die Möglichkeit, den befehl MetroCluster Heal mit dem Parameter --override-vetoes erneut auszugeben. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

4. Bestätigen Sie den Abschluss des Heal-Vorgangs, indem Sie den Befehl „MetroCluster Operation show“ im gesunden Cluster ausführen:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2017 20:54:41
   End Time: 7/29/2017 20:54:42
     Errors: -
```

Zurückwechseln

Nachdem Sie die MetroCluster-Konfiguration repariert haben, können Sie den MetroCluster-Switchback-Vorgang ausführen. Der MetroCluster Switchback-Vorgang gibt die Konfiguration wieder in den normalen Betriebsstatus zurück, wobei die Virtual Machines (SVMs) am Disaster-Standort aktiv sind und die Daten aus den lokalen Festplattenpools bereitstellen.

- Der Disaster Cluster muss erfolgreich auf den verbleibenden Cluster umgeschaltet sein.
- Mit den Daten und den Root-Aggregaten muss eine Reparatur durchgeführt worden sein.
- Die verbleibenden Cluster-Nodes dürfen sich nicht im HA-Failover-Status befinden (alle Nodes müssen für jedes HA-Paar in Betrieb sein).
- Die Controller-Module des Disaster-Site-Standorts müssen vollständig gebootet werden und nicht im HA-Übernahmemodus.
- Das Root-Aggregat muss gespiegelt werden.
- Die Inter-Switch Links (ISLs) müssen online sein.
- Alle erforderlichen Lizenzen müssen auf dem System installiert sein.

a. Vergewissern Sie sich, dass sich alle Nodes im Status aktiviert befinden: `metrocluster node show`

   Im folgenden Beispiel werden die Nodes angezeigt, die den Status aktiviert haben:

```
cluster_B::>  metrocluster node show

DR                        Configuration  DR
Group Cluster Node        State          Mirroring Mode
----- ------- ----------- -------------- ---------
--------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots
completed
              node_A_2    configured     enabled   heal roots
completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

b. Bestätigen Sie, dass die Neusynchronisierung auf allen SVMs abgeschlossen ist: `metrocluster vserver show`

c. Überprüfen Sie, ob alle automatischen LIF-Migrationen, die durch die heilenden Vorgänge durchgeführt werden, erfolgreich abgeschlossen sind: `metrocluster check lif show`

d. Führen Sie einen simulierten Umschalter durch, um zu überprüfen, ob das System bereit ist: `metrocluster switchback -simulate`

e. 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
Last Checked On: 9/13/2018 20:41:37

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

f. Führen Sie den Switchback durch, indem Sie den Befehl MetroCluster Switchback von einem beliebigen Node im verbleibenden Cluster aus ausführen: `metrocluster switchback`

g. Überprüfen Sie den Fortschritt des Umschalttaschens: `metrocluster show`

   Der Umkehrvorgang läuft noch, wenn die Ausgabe wartet auf „Zurück“ anzeigt:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang normal angezeigt wird:

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

+
Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne

über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

a. Wiederherstellung beliebiger SnapMirror oder SnapVault Konfigurationen

   In ONTAP 8.3 müssen Sie nach dem Wechsel zum MetroCluster eine verlorene SnapMirror Konfiguration manuell wiederherstellen. In ONTAP 9.0 und höher wird die Beziehung automatisch wiederhergestellt.

Überprüfen eines erfolgreichen Umschalttasches

Nach dem Wechsel zurück möchten Sie sicherstellen, dass alle Aggregate und Storage Virtual Machines (SVMs) zurück und wieder online geschaltet werden.

1. Vergewissern Sie sich, dass die Switched-Data-Aggregate zurückgeschaltet sind:

   `storage aggregate show`

   Im folgenden Beispiel ist aggr_b2 an Knoten B2 zurückgeschaltet:

   ```
   node_B_1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   ...
   aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

   mirrored,

   normal
   ```

2. Vergewissern Sie sich, dass alle SVMs mit synchronen Zielen im verbleibenden Cluster inaktiv sind (mit dem Betriebsstatus „`stopped`“):

   `vserver show -subtype sync-destination`

   ```
   node_B_1::> vserver show -subtype sync-destination
                                   Admin    Operational  Root
   Vserver       Type    Subtype    State    State        Volume
   Aggregate
   -----------   ------- ---------- -------- ----------   --------
   ----------
   ...
   cluster_A-vs1a-mc data sync-destination
                                 running    stopped    vs1a_vol   aggr_b2
   ```

Für Sync-Ziel-Aggregate in der MetroCluster-Konfiguration wurde das Suffix „`-mc`“ automatisch an ihren Namen angehängt, um sie zu identifizieren.

3. Überprüfen Sie, ob die SVMs im Disaster-Cluster mit synchronisierten Quellen betriebsbereit sind:

   `vserver show -subtype sync-source`

   ```
   node_A_1::> vserver show -subtype sync-source
                                       Admin    Operational  Root
   Vserver        Type    Subtype    State    State        Volume
   Aggregate
   -----------    ------- ---------- -------- ----------   --------
   ----------
   ...
   vs1a           data    sync-source
                                       running  running    vs1a_vol  aggr_b2
   ```

4. Vergewissern Sie sich, dass die Umkehrvorgänge mit dem erfolgreich waren `metrocluster operation show` Befehl.

Wenn die Befehlsausgabe angezeigt wird…	Dann…
Dass der Betriebszustand zurückwechseln erfolgreich ist.	Der Switch-Back-Vorgang ist abgeschlossen, und Sie können den Betrieb des Systems fortsetzen.
Dass der Betrieb des zurückkehrenden oder zurückkehrenden Agenten teilweise erfolgreich ist.	Führen Sie den vorgeschlagenen Fix aus, der in der Ausgabe des angegeben ist `metrocluster operation show` Befehl.

Sie müssen die vorherigen Abschnitte wiederholen, um den Umschalter in die entgegengesetzte Richtung auszuführen. Wenn Site_A die Umschaltung von Site_B durchgeführt hat, muss Site_B die Umschaltung von Site_A durchführen

Befehle für Umschaltung, Healing und Switchback

Zur Durchführung der MetroCluster Disaster Recovery-Prozesse gibt es bestimmte ONTAP-Befehle.

Ihr Ziel ist	Befehl
Überprüfen Sie, ob die Umschaltung fehlerfrei oder Vetos durchgeführt werden kann.	`metrocluster switchover -simulate` + auf der erweiterten Berechtigungsebene
Überprüfen Sie, ob der Wechsel fehlerfrei oder Vetos ausgeführt werden kann.	`metrocluster switchback -simulate` + auf der erweiterten Berechtigungsebene

Wechseln Sie zu den Partner-Nodes (ausgehandelte Umschaltung).	`metrocluster switchover`
Wechseln zu den Partner-Nodes (erzwungene Umschaltung).	`metrocluster switchover -forced-on-disaster true`
Reparatur von Datenaggregaten	`metrocluster heal -phase aggregates`
Reparatur des Root-Aggregats	`metrocluster heal -phase root-aggregates`
Wechseln Sie zurück zu den Home-Knoten.	`metrocluster switchback`

Verwenden Sie System Manager für Umschaltung und Switchback (nur MetroCluster IP-Konfigurationen).

Sie können die Steuerung von einem MetroCluster IP-Standort zum anderen wechseln, um Wartungsarbeiten durchzuführen oder nach einem Problem eine Wiederherstellung durchzuführen.

> Umschaltvorgänge und Switchback-Verfahren werden nur für MetroCluster IP-Konfigurationen unterstützt.

Überblick über Umschaltung und zurückwechseln

Eine Umschaltung kann in zwei Fällen erfolgen:

- **Eine geplante Umschaltung**

  Diese Umschaltung wird von einem Systemadministrator über System Manager initiiert. Mit der geplanten Umschaltung kann ein Systemadministrator eines lokalen Clusters die Kontrolle wechseln, sodass die Datenservices des Remote-Clusters vom lokalen Cluster übernommen werden. Anschließend kann ein Systemadministrator am Remote-Cluster-Standort Wartungsarbeiten am Remote-Cluster durchführen.

- **Eine ungeplante Umschaltung**

  In manchen Fällen initiiert ONTAP automatisch ein Switchover, wenn ein MetroCluster Cluster ausfällt oder die Verbindungen zwischen den Clustern ausfallen, sodass der noch laufende Cluster die Verantwortung für die Datenhandhabung des ausgefallen Clusters übernimmt.

  Wenn ONTAP den Status eines der Cluster nicht ermitteln kann, initiiert der Systemadministrator des Standorts, der gerade arbeitet, die Umschaltung, um die Verantwortung für die Datenverarbeitung am anderen Standort zu übernehmen.

Bei jedem Switch-Verfahren wird die Datenpflege mithilfe eines *switchback*-Prozesses an das Cluster zurückgegeben.

Der Umschaltvorgang und der Rückkehrprozess sind abhängig von Ihrer ONTAP-Version:

- Verwenden Sie System Manager in ONTAP 9.6 oder 9.7 für Umschaltung und Switchback
- Verwenden Sie System Manager in ONTAP 9.8 oder höher für die Umschaltung und den Wechsel zurück

Verwenden Sie System Manager in ONTAP 9.6 oder 9.7 für Umschaltung und Switchback

Schritte

1. Melden Sie sich in ONTAP 9.6 oder 9.7 beim System Manager an.
2. Klicken Sie auf **(Zurück zur klassischen Version)**.
3. Klicken Sie auf **Konfiguration > MetroCluster**.

   System Manager überprüft, ob eine ausgehandelte Umschaltung möglich ist.

4. Führen Sie einen der folgenden Teilschritte durch, wenn der Validierungsprozess abgeschlossen ist:
   a. Wenn die Validierung fehlschlägt, Standort B jedoch aktiv ist, ist ein Fehler aufgetreten. Beispielsweise könnte ein Problem mit einem Subsystem auftreten, oder NVRAM-Spiegelung wird unter Umständen nicht synchronisiert.
      i. Beheben Sie das Problem, das den Fehler verursacht, klicken Sie auf **Schließen** und starten Sie dann erneut bei Schritt 2.
      ii. Beenden Sie die Knoten von Standort B, klicken Sie auf **Schließen**, und führen Sie dann die Schritte unter "Durchführung einer ungeplanten Umschaltung"aus.
   b. Wenn die Validierung fehlschlägt und Standort B ausgefallen ist, liegt höchstwahrscheinlich ein Verbindungsproblem vor. Überprüfen Sie, ob Standort B ausgefallen ist, und führen Sie die Schritte in "Durchführung einer ungeplanten Umschaltung"aus.
5. Klicken Sie auf **Umschaltung von Standort B zu Standort A**, um den Switchover-Prozess zu starten.
6. Klicken Sie auf **Wechseln Sie zum neuen Erlebnis**.

Verwenden Sie System Manager in ONTAP 9.8 oder höher für die Umschaltung und den Wechsel zurück

Durchführen einer geplanten Umschaltung (ONTAP 9.8 oder höher)

Schritte

1. Melden Sie sich unter ONTAP 9.8 oder höher beim System Manager an.
2. Wählen Sie **Dashboard**. Im Abschnitt **MetroCluster** werden die beiden Cluster mit einer Verbindung angezeigt.
3. Klicken Sie im lokalen Cluster (links dargestellt) auf , und wählen Sie **Umschalten der Remote-Datenservices auf ⋮ den lokalen Standort**.

   Nachdem die Umschaltanforderung validiert wurde, wird die Steuerung vom Remote-Standort an den lokalen Standort übertragen. Der lokale Standort führt Datenserviceanfragen für beide Cluster aus.

   Das Remote Cluster wird neu gebootet, die Storage-Komponenten sind jedoch nicht aktiv, und das Cluster verarbeitet keine Datenanfragen. Es steht nun für die geplante Wartung zur Verfügung.

Das Remote-Cluster sollte erst für die Datenpflege verwendet werden, wenn Sie einen Switchback durchführen.

Durchführung einer ungeplanten Umschaltung (ONTAP 9.8 oder höher)

Eine ungeplante Umschaltung kann automatisch von ONTAP initiiert werden. Wenn ONTAP nicht feststellen kann, ob ein Switchback erforderlich ist, so initiiert der Systemadministrator des noch aktiven MetroCluster Standorts die Umschaltung mit folgenden Schritten:

Schritte

1. Melden Sie sich unter ONTAP 9.8 oder höher beim System Manager an.
2. Wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** wird die Verbindung zwischen den beiden Clustern mit einem "X" dargestellt. Dies bedeutet, dass eine Verbindung nicht erkannt werden kann und dass entweder die Verbindungen oder das Cluster ausgefallen sind.

3. Klicken Sie im lokalen Cluster (links dargestellt) auf , und wählen Sie **Umschalten der Remote-Datenservices auf ⋮ den lokalen Standort**.

   Falls die Umschaltung mit einem Fehler fehlschlägt, klicken Sie auf den Link „View Details“ in der Fehlermeldung und bestätigen Sie die ungeplante Umschaltung.

   Nachdem die Umschaltanforderung validiert wurde, wird die Steuerung vom Remote-Standort an den lokalen Standort übertragen. Der lokale Standort führt Datenserviceanfragen für beide Cluster aus.

   Das Cluster muss repariert werden, bevor es wieder online geschaltet wird.

Nachdem das Remote-Cluster online gestellt wurde, sollte es erst dann für die Datenpflege verwendet werden, wenn Sie ein Switchback durchführen.

Durchführen eines Switchback (ONTAP 9.8 oder höher)

Bevor Sie beginnen

Wenn das Remote-Cluster aufgrund geplanter Wartungsarbeiten oder aufgrund eines Ausfalls ausfällt, sollte es nun betriebsbereit sein und auf den Switchback warten.

Schritte

1. Melden Sie sich auf dem lokalen Cluster in ONTAP 9.8 oder höher bei System Manager an.
2. Wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** werden die beiden Cluster angezeigt.

3. Klicken Sie im lokalen Cluster (links dargestellt) auf ⋮, und wählen Sie **Kontrolle zurücknehmen**.

   Die Daten werden zuerst *healed*, um zu überprüfen, ob die Daten zwischen beiden Clustern synchronisiert und gespiegelt werden.

4. Wenn die Datenheilung abgeschlossen ist, klicken Sie auf ⋮, und wählen Sie **Switchback initiieren** aus.

   Nach Abschluss der zurückschalttaFunktionen sind beide Cluster aktiv und warten Datenanfragen. Zudem werden die Daten zwischen den Clustern gespiegelt und synchronisiert.

Monitoring der MetroCluster-Konfiguration

Mit ONTAP MetroCluster Befehlen und Active IQ Unified Manager (früher OnCommand Unified Manager) lässt sich der Zustand verschiedener Software-Komponenten und der Status von MetroCluster Vorgängen überwachen.

Überprüfen der MetroCluster-Konfiguration

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

Über diese Aufgabe

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

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

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

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

2. Zeigen Sie detailliertere Ergebnisse der letzten Zeit an `metrocluster check run` Befehl:

   ```
   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

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

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

```
cluster_A::> metrocluster check aggregate show

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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
                                                 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.
```

Befehle zum Prüfen und Überwachen der MetroCluster-Konfiguration

Es gibt bestimmte ONTAP Befehle zur Überwachung der MetroCluster Konfiguration und zum Prüfen der MetroCluster Vorgänge.

Befehle zum Prüfen von MetroCluster-Vorgängen

Ihr Ziel ist	Befehl

Überprüfen Sie die MetroCluster Vorgänge. **Hinweis:** dieser Befehl sollte nicht als einziger Befehl für die Systemvalidierung vor dem DR-Betrieb verwendet werden.	`metrocluster check run`
Sehen Sie sich die Ergebnisse der letzten Überprüfung der MetroCluster-Vorgänge an.	`metrocluster show`
Zeigen Sie die Ergebnisse der Überprüfung der Konfigurationsreplikation zwischen den Standorten an.	`metrocluster check config-replication show metrocluster check config-replication show-aggregate-eligibility`
Zeigen Sie die Ergebnisse der Überprüfung der Node-Konfiguration an.	`metrocluster check node show`
Zeigen Sie die Ergebnisse der Überprüfung auf Aggregatkonfiguration an.	`metrocluster check aggregate show`
Sehen Sie sich die Fehler der LIF-Platzierung in der MetroCluster Konfiguration an.	`metrocluster check lif show`

Befehle für das Monitoring des MetroCluster Interconnect

Ihr Ziel ist	Befehl
Zeigt den Status und Informationen zur HA- und DR-Spiegelung für die MetroCluster-Nodes im Cluster an.	`metrocluster interconnect mirror show`

Befehle für das Monitoring von MetroCluster SVMs

Ihr Ziel ist	Befehl
Sie können alle SVMs an beiden Standorten in der MetroCluster Konfiguration anzeigen.	`metrocluster vserver show`

Überwachen der Konfiguration über MetroCluster Tiebreaker oder ONTAP Mediator

Siehe "Unterschiede zwischen ONTAP Mediator und MetroCluster Tiebreaker" Informationen über die Unterschiede zwischen diesen beiden Methoden zur Überwachung der MetroCluster-Konfiguration und zum Initiieren einer automatischen Umschaltung

Über die folgenden Links können Sie Tiebreaker oder Mediator installieren und konfigurieren:

- "MetroCluster Tiebreaker Software installieren und konfigurieren"
- "Vorbereiten der Installation von ONTAP Mediator"

Wie die NetApp MetroCluster Tiebreaker Software Ausfälle erkennt

Sie wird auf einem Linux-Host ausgeführt. Sie benötigen die Tiebreaker Software nur, wenn zwei Cluster und der Konnektivitätsstatus zwischen ihnen von einem dritten Standort aus überwacht werden soll. Wenn dann die Verbindung zwischen den Standorten ausfällt, kann jeder Partner in einem Cluster zwischen einem ISL-Fehler und einem Standortausfall unterscheiden.

Nachdem Sie die Tiebreaker Software auf einem Linux-Host installiert haben, können Sie die Cluster in einer MetroCluster-Konfiguration konfigurieren, um auf Notfälle zu überwachen.

So erkennt die Tiebreaker Software Konnektivitätsausfälle zwischen Standorten

Die MetroCluster Tiebreaker Software benachrichtigt Sie, wenn alle Verbindungen zwischen den Standorten verloren gehen.

Arten von Netzwerkpfaden

Je nach Konfiguration gibt es drei Typen von Netzwerkpfaden zwischen den beiden Clustern in einer MetroCluster Konfiguration:

- **FC-Netzwerk (in Fabric-Attached MetroCluster-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten FC Switch Fabrics. Jede Switch-Fabric verfügt über zwei FC-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei FC-Switches, eine von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige IP-Switches FC-Konnektivität (NV Interconnect und FCP Initiator) verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

- **Intercluster Peering-Netzwerk**

  Dieser Netzwerktyp besteht aus einem redundanten IP-Netzwerkpfad zwischen den beiden Clustern. Das Cluster-Peering-Netzwerk bietet die Konnektivität, die zur Spiegelung der Konfiguration der Storage Virtual Machine (SVM) erforderlich ist. Die Konfiguration aller SVMs auf einem Cluster wird vom Partner-Cluster gespiegelt.

- **IP-Netzwerk (in MetroCluster IP-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten IP Switch-Netzwerken. Jedes Netzwerk verfügt über zwei IP-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei IP-Switches, einer von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige FC-Switches verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

Monitoring der Konnektivität zwischen Standorten

Die Tiebreaker Software ruft regelmäßig den Status der Konnektivität zwischen Standorten von den Nodes ab. Wenn die NV-Interconnect-Konnektivität verloren geht und das Intercluster-Peering nicht auf Pings reagiert, gehen die Cluster davon aus, dass die Sites isoliert sind und die Tiebreaker Software eine Warnung als „AllLinksSevered“ auslöst. Wenn ein Cluster den Status „AllLinksSevered“ identifiziert und der andere Cluster nicht über das Netzwerk erreichbar ist, löst die Tiebreaker Software eine Warnung als „Disaster“ aus.

Wie die Tiebreaker Software Standortausfällen erkennt

Die NetApp MetroCluster Tiebreaker Software überprüft die Erreichbarkeit der Nodes in einer MetroCluster Konfiguration und des Clusters, um zu ermitteln, ob ein Standortausfall aufgetreten ist. Über die Tiebreaker

Software wird auch unter bestimmten Bedingungen eine Warnmeldung ausgelöst.

Komponenten, die über die Tiebreaker Software überwacht werden

Die Tiebreaker Software überwacht jeden Controller in der MetroCluster-Konfiguration, indem redundante Verbindungen über mehrere Pfade zu einer Node-Management-LIF und zur Cluster-Management-LIF erstellt werden, die beide im IP-Netzwerk gehostet werden.

Die Tiebreaker Software überwacht folgende Komponenten in der MetroCluster Konfiguration:

- Nodes über lokale Node-Schnittstellen
- Ein Cluster über die vom Cluster vorgegebenen Schnittstellen durchführen
- Überlebendes Cluster, um zu ermitteln, ob Verbindung zum Disaster-Standort vorhanden ist (NV Interconnect, Storage und Cluster-Peering)

Wenn es einen Verlust der Verbindung zwischen der Tiebreaker Software und allen Nodes im Cluster und dem Cluster selbst gibt, wird das Cluster durch die Tiebreaker Software als „`nicht erreichbar`“ deklariert. Es dauert etwa drei bis fünf Sekunden, einen Verbindungsfehler zu erkennen. Wenn ein Cluster über die Tiebreaker Software nicht erreichbar ist, muss das verbleibende Cluster (das Cluster, das noch erreichbar ist) angeben, dass alle Links zum Partner-Cluster getrennt werden, bevor die Tiebreaker Software eine Meldung auslöst.

> Alle Links werden getrennt, wenn das verbliebene Cluster nicht mehr über FC (NV Interconnect und Storage) und Intercluster-Peering mit dem Cluster am Disaster-Standort kommunizieren kann.

Ausfallszenarien, während denen Tiebreaker Software eine Warnmeldung auslöst

Die Tiebreaker Software löst eine Warnmeldung aus, wenn das Cluster (alle Nodes) an der Disaster Site ausgefallen ist oder nicht erreichbar ist und das Cluster auf der überlebenden Site den Status „AllLinksSevered“ anzeigt.

Die Tiebreaker Software löst keine Warnmeldung (oder der Alarm wird über ein Vetos ausgelöst) in den folgenden Szenarien aus:

- Wenn in einer MetroCluster Konfiguration mit acht Nodes ein HA-Paar am Disaster-Standort ausfällt
- In einem Cluster, in dem alle Knoten am Katastrophenstandort ausgefallen sind, ein HA-Paar am überlebenden Standort ausgefallen und das Cluster auf der überlebenden Site weist den Status „AllLinksSevered“ auf

  Die Tiebreaker Software löst eine Warnmeldung aus, jedoch vetoes ONTAP diese Warnmeldung aus. In dieser Situation ist auch ein manuelles Switchover vetoed vetoed

- In jedem Szenario, in dem die Tiebreaker Software mindestens einen Node oder die Cluster-Schnittstelle am Disaster-Standort erreichen kann, kann der verbleibende Standort über FC (NV Interconnect und Storage) oder Intercluster Peering einen Node am Disaster-Standort erreichen

Wie der ONTAP Mediator die automatische ungeplante Umschaltung unterstützt

"Erfahren Sie, wie der ONTAP Mediator die automatische ungeplante Umschaltung in MetroCluster IP-Konfigurationen unterstützt".

Überwachen und Schützen der Konsistenz des Filesystems mithilfe von NVFAIL

Der `-nvfail` Parameter von `volume modify` Mit dem Befehl kann ONTAP Inkonsistenzen im nichtflüchtigen RAM (NVRAM) erkennen, wenn das System gebootet oder nach einem Switchover-Vorgang gestartet wird. Sie werden außerdem gewarnt und schützt das System vor Datenzugriff und -Änderungen, bis das Volume manuell wiederhergestellt werden kann.

Wenn ONTAP Probleme erkennt, werden Datenbank- oder Filesysteminstanzen nicht mehr reagiert oder heruntergefahren. ONTAP sendet dann Fehlermeldungen an die Konsole, um Sie zu benachrichtigen, den Status der Datenbank oder des Dateisystems zu überprüfen. Sie können NVFAIL aktivieren, um Datenbankadministratoren zu warnen, dass NVRAM-Inkonsistenzen zwischen geclusterten Nodes auftreten, die die Gültigkeit von Datenbanken beeinträchtigen können.

Nach dem Verlust von NVRAM-Daten während des Failover oder der Boot-Recovery können NFS-Clients erst dann auf Daten von einem der Nodes zugreifen, wenn der Status „NV-Fehler“ beseitigt wurde. CIFS-Clients sind nicht betroffen.

Auswirkungen von NV-Fehler auf den Zugriff auf NFS-Volumes oder LUNs

Der NV-Fehler-Status wird festgelegt, wenn ONTAP beim Booten, bei einem MetroCluster-Switchover oder während eines HA-Takeover-Vorgangs NVRAM-Fehler erkennt, wenn die Option NVFAIL auf dem Volume festgelegt ist. Wenn beim Start keine Fehler erkannt werden, wird der Dateidienst normal gestartet. Wenn jedoch NVRAM-Fehler erkannt oder die NVFAIL-Verarbeitung bei einem Disaster Switchover durchgesetzt wird, verhindert ONTAP, dass Datenbankinstanzen auf diese reagieren.

Wenn Sie die Option NVFAIL aktivieren, findet während des Bootup eines der in der folgenden Tabelle beschriebenen Prozesse statt:

Wenn…	Dann…
ONTAP erkennt keine NVRAM-Fehler	Der Fileservice wird ordnungsgemäß gestartet.

ONTAP erkennt NVRAM-Fehler	• ONTAP gibt einen veralteten Fehler beim Dateihandle (ESTALE) an NFS-Clients zurück, die versuchen, auf die Datenbank zuzugreifen, da die Applikation nicht mehr reagiert, abstürzt oder heruntergefahren werden kann. ONTAP sendet dann eine Fehlermeldung an die Systemkonsole und die Log-Datei. • Beim Neustart der Anwendung stehen CIFS-Clients Dateien zur Verfügung, selbst wenn Sie nicht überprüft haben, ob sie gültig sind. Bei NFS-Clients können Dateien erst nach dem Zurücksetzen des nicht mehr zugänglich sein `in-nvfailed-state` Option auf dem betroffenen Volumen.
Wenn einer der folgenden Parameter verwendet wird: • `dr-force-nvfail` Die Volume-Option ist festgelegt • `force-nvfail-all` Die Option Switchover ist festgelegt.	Sie können die Einstellung aufheben `dr-force-nvfail` Option nach der Umschaltung, falls der Administrator nicht damit rechnet, die NVFAIL-Verarbeitung für mögliche zukünftige Disaster-Switchover-Operationen zu erzwingen. Bei NFS-Clients können Dateien erst nach dem Zurücksetzen des nicht mehr zugänglich sein `in-nvfailed-state` Option auf dem betroffenen Volumen. Verwenden der `force-nvfail-all` Option verursacht das `dr-force-nvfail` Option für alle DR-Volumes, die während der Disaster Switchover verarbeitet werden, ist aktiviert.
ONTAP erkennt NVRAM-Fehler auf einem Volume, das LUNs enthält	LUNs in diesem Volume werden in den Offline-Modus versetzt. Der `in-nvfailed-state` Option auf dem Volume muss gelöscht werden, und das NV-Fehler-Attribut auf den LUNs muss gelöscht werden, indem jede LUN im betroffenen Volume online geschaltet wird. Sie können die Schritte durchführen, um die Integrität der LUNs zu überprüfen und die LUN nach Bedarf aus einer Snapshot Kopie oder einem Backup wiederherzustellen. Nachdem alle LUNs im Volume wiederhergestellt sind, der `in-nvfailed-state` Die Option auf dem betroffenen Volume wird gelöscht.

Befehle für das Monitoring von Datenverlusten

Wenn Sie die Option NVFAIL aktivieren, erhalten Sie eine Benachrichtigung, wenn ein Systemabsturz aufgrund von NVRAM-Inkonsistenzen oder einer MetroCluster-Umschaltung auftritt.

Standardmäßig ist der NVFAIL-Parameter nicht aktiviert.

Ihr Ziel ist	Befehl
Erstellen Sie ein neues Volume mit aktiviertem NVFAIL	`volume create -nvfail on`
Aktivieren Sie NVFAIL auf einem vorhandenen Volume	`volume modify` **Hinweis:** Sie stellen das ein `-nvfail` Option „ein“, um NVFAIL auf dem erstellten Volume zu aktivieren.
Zeigt an, ob NVFAIL derzeit für ein angegebenes Volume aktiviert ist	`volume show` **Hinweis:** Sie stellen das ein `-fields` Parameter in „nvfail“ zum Anzeigen des NV-Fehler-Attributs für ein angegebenes Volume.

Verwandte Informationen

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

Zugriff auf Volumes im Status „NV-Fehler“ nach einer Umschaltung

Nach einer Umschaltung müssen Sie den NV-Fehler-Status löschen, indem Sie den zurücksetzen `-in -nvfailed-state` Parameter von `volume modify` Befehl, um die Einschränkung von Clients für den Zugriff auf Daten zu entfernen.

Bevor Sie beginnen

Die Datenbank oder das Dateisystem dürfen nicht ausgeführt werden oder es darf versucht werden, auf das betroffene Volume zuzugreifen.

Über diese Aufgabe

Einstellung `-in-nvfailed-state` Für Parameter ist die Berechtigung auf erweiterter Ebene erforderlich.

Schritt

1. Stellen Sie das Volume mithilfe des Befehls Volume modify wieder her, mit dem Parameter -in-nvfailed -State auf false gesetzt.

Nachdem Sie fertig sind

Anweisungen zur Überprüfung der Gültigkeit von Datenbankdateien finden Sie in der Dokumentation für Ihre spezifische Datenbanksoftware.

Wenn Ihre Datenbank LUNs verwendet, überprüfen Sie die Schritte, um nach einem NVRAM-Fehler den Host Zugriff auf die LUNs zu ermöglichen.

Verwandte Informationen

"Überwachen und Schützen der Systemkonsistenz der Dateien mit NVFAIL"

Die Wiederherstellung von LUNs in NV-Fehler-Status nach dem Switchover erfolgt

Nach einer Umschaltung hat der Host nicht mehr Zugriff auf Daten auf den LUNs, die sich im Status „NV-Fehler“ befinden. Sie müssen eine Reihe von Aktionen durchführen, bevor die Datenbank Zugriff auf die LUNs hat.

Bevor Sie beginnen

Die Datenbank darf nicht ausgeführt werden.

Schritte

1. Löschen Sie den NV-Fehler-Status auf dem Volume „Auswirkungen“, das die LUNs hostet, indem Sie das zurücksetzen `-in-nvfailed-state` Parameter von `volume modify` Befehl.
2. Versetzen Sie die betroffenen LUNs in den Online-Modus.
3. Untersuchen Sie die LUNs auf Dateninkonsistenzen und beheben Sie sie.

   Dies könnte Host-basierte Wiederherstellung oder Recovery umfassen, die auf dem Storage Controller mit SnapRestore durchgeführt wird.

4. Versetzen Sie die Datenbankapplikation online, nachdem Sie die LUNs wiederhergestellt haben.

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen
"Technischer Bericht 4375 zu NetApp MetroCluster für ONTAP 9.3"	• Eine technische Übersicht über Konfiguration und Betrieb von MetroCluster • Best Practices für die Konfiguration von MetroCluster.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von MetroCluster IP"	• MetroCluster IP Architektur • Verkabelung der Konfiguration • Konfigurieren der MetroCluster in ONTAP

"Installation und Konfiguration der MetroCluster Tiebreaker 1.21 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

Warten der MetroCluster-Komponenten

Weitere Informationen zur MetroCluster-Wartung

Erfahren Sie, wie Sie MetroCluster-Wartungsaufgaben vorbereiten und das richtige Wartungsverfahren für Ihre Konfiguration auswählen.

Vorbereitung auf Wartungsaufgaben

Lesen Sie die Informationen in "Vorbereitung auf die MetroCluster-Wartung"durch, bevor Sie Wartungsmaßnahmen durchführen.

> Sie müssen die Konsolenprotokollierung aktivieren und ONTAP Mediator oder Tiebreaker Monitoring entfernen, bevor Sie Wartungsaufgaben durchführen.

Wartungsverfahren für verschiedene Arten von MetroCluster Konfigurationen

- Wenn Sie über eine MetroCluster-IP-Konfiguration verfügen, lesen Sie die Verfahren in "Wartungsverfahren für MetroCluster IP-Konfigurationen".
- Wenn Sie über eine MetroCluster FC-Konfiguration verfügen, lesen Sie die Verfahren in "Wartungsverfahren für MetroCluster FC-Konfigurationen".
- Wenn Sie das Verfahren im Abschnitt für Ihre Konfiguration nicht finden können, lesen Sie die Verfahren unter "Wartungsverfahren für alle MetroCluster Konfigurationen".

Alle anderen Wartungsverfahren

Die folgende Tabelle enthält Links zu Verfahren im Zusammenhang mit der MetroCluster-Wartung, die sich nicht in den drei oben aufgeführten Abschnitten befinden:

Komponente	MetroCluster Typ (FC oder IP)	Aufgabe	Verfahren
ONTAP Software	Beides	ONTAP-Software-Upgrade	"Upgrade, Zurücksetzen oder Downgrade"

Controller-Modul	Beides	FRU-Ersatz (einschließlich Controller-Module, PCIe-Karten, FC-VI-Karte usw.) Das Verschieben eines Storage-Controller-Moduls oder einer NVRAM-Karte zu den MetroCluster Storage-Systemen wird nicht unterstützt.	"Dokumentation zu ONTAP Hardwaresystemen"
Upgrades und Erweiterungen	"MetroCluster Upgrade und Erweiterung"	Übergang von FC- zu IP-Konnektivität	"Umstellung von MetroCluster FC auf MetroCluster IP"
Festplatten-Shelf	FC	Alle anderen Shelf-Wartungsarbeiten Die Standardverfahren können verwendet werden.	"Aufrechterhaltung der Festplatten-Shelfs DS460C DS224C und DS212C"
IP	Alle Shelf-Wartungsarbeiten Die Standardverfahren können verwendet werden. Wenn Sie Shelfs für ein nicht gespiegeltes Aggregat hinzufügen, lesen Sie "Überlegungen bei der Verwendung von nicht gespiegelten Aggregaten"	"Aufrechterhaltung der Festplatten-Shelfs DS460C DS224C und DS212C"	Beides

Vorbereitung auf die MetroCluster-Wartung

Aktivieren Sie die Konsolenprotokollierung, bevor Sie Wartungsaufgaben durchführen

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie Wartungsaufgaben durchführen.

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und vor der Durchführung von Wartungsmaßnahmen die folgenden Aktionen durchzuführen:

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Vor der Durchführung von Wartungsarbeiten müssen Sie den ONTAP Mediator oder den Tiebreaker Monitoring entfernen

Bevor Sie Wartungsarbeiten durchführen, müssen Sie die Überwachung entfernen, wenn die MetroCluster-Konfiguration mit dem Tiebreaker oder Mediator Utility überwacht wird.

Zu den Wartungsarbeiten gehören ein Upgrade der Controller-Plattform, ein Upgrade der ONTAP und ein ausgehandeltes Switchover und Switchback.

Schritte

1. Sammeln Sie die Ausgabe für den folgenden Befehl:

   ```
   storage iscsi-initiator show
   ```

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

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

3. Nach Abschluss der Wartung der MetroCluster-Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen" Im Abschnitt *MetroCluster Tiebreaker Installation and Configuration*.
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" im Abschnitt *MetroCluster IP-Installation und -Konfiguration*.
Applikationen von Drittanbietern	Siehe Produktdokumentation.

MetroCluster-Fehlerszenarien und Recovery

Sie sollten sich bewusst sein, wie die MetroCluster Konfiguration auf unterschiedliche Ausfallereignisse reagiert.

Weitere Informationen zur Wiederherstellung nach Knotenausfällen finden Sie im Abschnitt „Auswahl des richtigen Wiederherstellungsverfahrens“ "Nach einem Ausfall wiederherstellen".

Ereignis	Auswirkungen	Recovery
Ausfall eines Single Node	Ein Failover wird ausgelöst.	Die Konfiguration ist durch eine lokale Übernahme wiederhergestellt. RAID ist nicht beeinträchtigt. Überprüfen Sie die Systemmeldungen und ersetzen Sie ggf. fehlerhafte FRUs. "Dokumentation zu ONTAP Hardwaresystemen"
Zwei Nodes fallen an einem Standort aus	Zwei Nodes funktionieren nur, wenn die automatisierte Umschaltung in der MetroCluster Tiebreaker Software aktiviert ist.	Bei nicht aktiviertem automatisierten Switchover in der MetroCluster Tiebreaker Software ist eine manuelle, ungeplante Umschaltung (USO) nicht möglich. "Dokumentation zu ONTAP Hardwaresystemen"

Fehler der MetroCluster-IP-Schnittstelle eines Ports	Das System ist beeinträchtigt. Zusätzlicher Port-Ausfall hat Auswirkungen auf die HA-Spiegelung.	Der zweite Port wird verwendet. Die Systemzustandsüberwachung generiert eine Meldung, wenn die physische Verbindung zum Port beschädigt ist. Überprüfen Sie die Systemmeldungen und ersetzen Sie ggf. fehlerhafte FRUs. "Dokumentation zu ONTAP Hardwaresystemen"
Fehler der MetroCluster-IP-Schnittstelle beider Ports	DIE HA-Funktion ist beeinträchtigt. Die Synchronisierung der RAID SyncMirror des Nodes wird unterbrochen.	Sofortige manuelle Wiederherstellung ist erforderlich, da kein HA Takeover vorhanden ist. Überprüfen Sie die Systemmeldungen und ersetzen Sie ggf. fehlerhafte FRUs. "Dokumentation zu ONTAP Hardwaresystemen"
Ausfall eines MetroCluster IP-Switch	Keine Auswirkungen. Redundanz wird über das zweite Netzwerk bereitgestellt.	Tauschen Sie den defekten Schalter ggf. aus. "Austauschen eines IP-Switches"
Ausfall von zwei MetroCluster IP-Switches im selben Netzwerk	Keine Auswirkungen. Redundanz wird über das zweite Netzwerk bereitgestellt.	Tauschen Sie den defekten Schalter ggf. aus. "Austauschen eines IP-Switches"
Ausfall von zwei MetroCluster IP-Switchen an einem Standort	Die Synchronisierung der RAID SyncMirror des Nodes wird unterbrochen. DIE HA-Funktion wird beeinträchtigt und das Cluster geht nicht mehr durch Quorum.	Tauschen Sie den defekten Schalter ggf. aus. "Austauschen eines IP-Switches"
Ausfall von zwei MetroCluster IP Switches, die sich an verschiedenen Standorten befinden und nicht im gleichen Netzwerk (diagonal Ausfall)	Die Synchronisierung der RAID SyncMirror des Nodes wird unterbrochen.	Die Synchronisierung der RAID SyncMirror des Nodes wird unterbrochen. Cluster- und HA-Funktionen sind nicht beeinträchtigt. Tauschen Sie den defekten Schalter ggf. aus. "Austauschen eines IP-Switches"

Mit dem Interoperabilitäts-Matrix-Tool finden Sie MetroCluster Informationen

Wenn Sie die MetroCluster-Konfiguration einrichten, können Sie mit dem Interoperabilitäts-Tool sicherstellen, dass Sie unterstützte Software- und

Hardwareversionen verwenden.

"NetApp Interoperabilitäts-Matrix-Tool"

Nachdem Sie die Interoperabilitäts-Matrix geöffnet haben, können Sie im Feld „Storage Solution“ Ihre MetroCluster Lösung auswählen.

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.

Wartungsverfahren für MetroCluster FC-Konfigurationen

Ändern Sie eine Switch- oder ATTO Bridge-IP-Adresse für die Statusüberwachung

Nachdem Sie die IP-Adressen von MetroCluster FC-Back-End-Switches und ATTO-Bridges geändert haben, müssen Sie die alten IP-Adressen für die Integritätsüberwachung durch die neuen Werte ersetzen.

- Ändern Sie eine Switch-IP-Adresse
- Ändern Sie eine ATTO Bridge-IP-Adresse

Ändern Sie eine Switch-IP-Adresse

Ersetzen Sie die alte IP-Adresse für die Statusüberwachung eines MetroCluster FC-Back-End-Switches.

Bevor Sie beginnen

Informationen zum Ändern der IP-Adresse auf dem Switch finden Sie in der Dokumentation des Switch-Anbieters für Ihr Switch-Modell, bevor Sie die IP-Adresse für die Integritätsüberwachung ändern.

Schritte

1. Führen Sie die aus `::> storage switch show` Und notieren Sie sich in der Ausgabe die Switches, die Fehler melden.
2. Entfernen Sie die Switch-Einträge mit alten IP-Adressen:

   ```
   ::> storage switch remove -name switch_name
   ```

3. Fügen Sie die Switches mit neuen IP-Adressen hinzu:

   ```
   ::> storage switch add -name switch_name -address new_IP_address -managed-by
   in-band
   ```

4. Überprüfen Sie die neuen IP-Adressen, und vergewissern Sie sich, dass keine Fehler vorliegen:

   ```
   ::> storage switch show
   ```

5. Aktualisieren Sie bei Bedarf die Einträge:

   ```
   ::> set advanced
   ```

```
::*> storage switch refresh

::*> set admin
```

Ändern Sie eine ATTO Bridge-IP-Adresse

Ersetzen Sie die alte IP-Adresse der Integritätsüberwachung einer ATTO Bridge.

Schritte

1. Führen Sie die aus `::> storage bridge show` Beachte in der Ausgabe und die ATTO-Bridges, die Fehler melden.
2. Entfernen Sie die ATTO Bridge-Einträge mit alten IP-Adressen:

   ```
   ::> storage bridge remove -name ATTO_bridge_name
   ```

3. Fügen Sie die ATTO-Bridges mit neuen IP-Adressen hinzu:

   ```
   ::> storage bridge add -name ATTO_bridge_name -address new_IP_address -managed
   -by in-band
   ```

4. Überprüfen Sie die neuen IP-Adressen, und vergewissern Sie sich, dass keine Fehler vorliegen:

   ```
   ::> storage bridge show
   ```

5. Aktualisieren Sie bei Bedarf die Einträge:

   ```
   ::> set advanced

   ::*> storage bridge refresh

   ::*> set admin
   ```

FC-to-SAS-Bridge-Wartung

Unterstützung für FibreBridge 7600N-Brücken in MetroCluster-Konfigurationen

Die FibreBridge 7600N wird auf ONTAP 9.5 und höher als Ersatz für die FibreBridge 7500N oder 6500N Bridge unterstützt oder beim Hinzufügen von neuem Speicher zur MetroCluster-Konfiguration. Die Zoning-Anforderungen und Einschränkungen für die Verwendung der FC-Ports der Bridge entsprechen denen der FibreBridge 7500N-Bridge.

"NetApp Interoperabilitäts-Matrix-Tool"

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

Anwendungsfall	Änderungen beim Zoning erforderlich?	Einschränkungen	Verfahren

Austausch einer einzelnen FibreBridge 7500N-Brücke durch eine einzelne FibreBridge 7600N-Brücke	Nein	Die FibreBridge 7600N-Brücke muss genau wie die FibreBridge 7500N-Brücke konfiguriert sein.	"Hot-Swap einer FibreBridge 7500N mit einer 7600N-Brücke"
Austausch einer einzelnen FibreBridge 6500N-Brücke durch eine einzige FibreBridge 7600N-Brücke	Nein	Die FibreBridge 7600N-Brücke muss genau wie die FibreBridge 6500N-Brücke konfiguriert sein.	"Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke"
Hinzufügen von neuem Speicher durch Hinzufügen eines neuen FibreBridge 7600N-Brückenpaares	Ja. Sie müssen für jeden der FC-Ports der neuen Brücken Speicherzonen hinzufügen.	Sie müssen über verfügbare Ports an der FC Switch-Fabric (in einer Fabric-Attached MetroCluster-Konfiguration) oder auf den Storage Controllern (in einer Stretch-MetroCluster-Konfiguration) verfügen.jedes FibreBridge-Paar 7500N oder 7600N unterstützt bis zu vier Stacks.	"Hot-Adding eines Stacks mit SAS-Platten-Shelves und Brücken zu einem MetroCluster System"

Unterstützung für FibreBridge 7500N-Brücken in MetroCluster-Konfigurationen

Die FibreBridge 7500N Bridge wird als Ersatz für die FibreBridge 6500N Bridge oder für beim Hinzufügen von neuem Speicher zur MetroCluster-Konfiguration unterstützt. Die unterstützten Konfigurationen weisen Zoning-Anforderungen und Einschränkungen in Bezug auf die Verwendung der FC-Ports der Bridge sowie der Beschränkungen für Stack und Storage-Shelf auf.

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

Anwendungsfall	Änderungen beim Zoning erforderlich?	Einschränkungen	Verfahren
Austausch einer einzelnen FibreBridge 6500N-Brücke durch eine einzelne FibreBridge 7500N-Brücke	Nein	Die FibreBridge 7500N-Bridge muss über einen einzelnen FC-Port und eine Verbindung zu einem einzelnen Stack genau so konfiguriert sein wie die FibreBridge 6500N Bridge. Der zweite FC-Port auf der FibreBridge 7500N darf nicht verwendet werden.	"Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke"

Anwendungsfall	Änderungen beim Zoning erforderlich?	Einschränkungen	Verfahren
Konsolidierung mehrerer Stacks durch Ersetzen mehrerer FibreBridge 6500N-Paare durch ein einziges Paar FibreBridge 7500N-Brücken	Ja.	In diesem Fall können Sie die FibreBridge 6500N-Brücken außer Betrieb nehmen und durch ein einziges Paar FibreBridge 7500N-Brücken ersetzen.jedes Paar FibreBridge 7500N oder 7600N unterstützt bis zu vier Stapel. Am Ende des Verfahrens müssen sowohl die obere als auch die untere Seite der Stapel an die entsprechenden Anschlüsse der FibreBridge 7500N angeschlossen werden.	"Austausch von zwei FibreBridge 6500N-Brücken durch 7600N- oder 7500N-Brücken"
Hinzufügen von neuem Speicher durch das Hinzufügen eines neuen FibreBridge 7500N-Brückenpaares	Ja. Sie müssen für jeden der FC-Ports der neuen Brücken Speicherzonen hinzufügen.	Sie müssen über verfügbare Ports an der FC Switch-Fabric (in einer Fabric-Attached MetroCluster-Konfiguration) oder auf den Storage Controllern (in einer Stretch-MetroCluster-Konfiguration) verfügen.jedes FibreBridge-Paar 7500N oder 7600N unterstützt bis zu vier Stacks.	"Hot-Adding eines Stacks mit SAS-Platten-Shelves und Brücken zu einem MetroCluster System"

Aktivieren des IP-Portzugriffs auf der FibreBridge 7600N-Brücke, falls erforderlich

Wenn Sie eine ONTAP-Version vor 9.5 verwenden oder anderweitig planen, Out-of-Band-Zugriff auf die FibreBridge 7600N-Brücke über Telnet oder andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) zu nutzen, können Sie die Zugriffsservices über den Konsolen-Port aktivieren.

Im Gegensatz zur ATTO FibreBridge 7500N Bridge wird die FibreBridge 7600N Bridge mit deaktivierten IP-Port-Protokollen und -Diensten ausgeliefert.

Ab ONTAP 9.5 wird *in-Band-Management* der Brücken unterstützt. Das bedeutet, dass die Brücken über die FC-Verbindung zur Bridge von der ONTAP-CLI konfiguriert und überwacht werden können. Physischer Zugang zur Bridge über die Bridge-Ethernet-Ports ist nicht erforderlich und die Bridge-Benutzeroberflächen sind nicht erforderlich.

Ab ONTAP 9.8 wird *in-Band-Management* der Bridges standardmäßig unterstützt und out-of-Band SNMP-

Management ist veraltet.

Diese Aufgabe ist erforderlich, wenn Sie zur Verwaltung der Brücken * nicht* verwenden. In diesem Fall müssen Sie die Bridge über den Ethernet-Management-Port konfigurieren.

Schritte

1. Greifen Sie auf die Konsolenschnittstelle der Bridge zu, indem Sie ein serielles Kabel an den seriellen Port der FibreBridge 7600N anschließen.
2. Aktivieren Sie die Zugriffsservices über die Konsole, und speichern Sie die Konfiguration:

   ```
   set closeport none

   saveconfiguration
   ```

   Der `set closeport none` Befehl aktiviert alle Zugriffsservices auf der Bridge.

3. Deaktivieren Sie ggf. einen Dienst, indem Sie den ausstellen `set closeport` Und den Befehl ggf. wiederholen, bis alle gewünschten Dienste deaktiviert sind:

   ```
   set closeport service
   ```

   Der `set closeport` Durch den Befehl wird ein einzelner Dienst gleichzeitig deaktiviert.

   `service` Folgende Optionen stehen zur Verfügung:

   - expressnav
   - ftp
   - icmp
   - quicknav
   - snmp
   - telnet

     Sie können mithilfe der überprüfen, ob ein bestimmtes Protokoll aktiviert oder deaktiviert ist `get closeport` Befehl.

4. Wenn Sie SNMP aktivieren, müssen Sie auch den Befehl Set SNMP Enabled eingeben:

   ```
   set SNMP enabled
   ```

   SNMP ist das einzige Protokoll, das einen separaten Enable-Befehl erfordert.

5. Konfiguration speichern:

   ```
   saveconfiguration
   ```

Firmware auf einer FibreBridge-Bridge aktualisieren

Das Verfahren zum Aktualisieren der Bridge-Firmware hängt von Ihrem Bridge-Modell und der ONTAP-Version ab.

Über diese Aufgabe

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Firmware-Aktualisierung auf FibreBridge 7600N oder 7500N-Bridges für Konfigurationen mit ONTAP 9.4 und höher

Möglicherweise müssen Sie die Firmware auf Ihren FibreBridge-Bridges aktualisieren, um sicherzustellen, dass Sie über die neuesten Funktionen verfügen oder mögliche Probleme beheben können. Dieses Verfahren sollte für FibreBridge 7600N- oder 7500N-Brücken bei Konfigurationen mit ONTAP 9.4 und höher angewendet werden.

- Die MetroCluster Konfiguration muss ordnungsgemäß ausgeführt werden.
- Alle FibreBridge-Brücken in der MetroCluster-Konfiguration müssen in Betrieb sein.
- Alle Storage-Pfade müssen verfügbar sein.
- Sie benötigen das Administratorkennwort und Zugriff auf einen HTTP-, FTP- oder TFTP-Server (Trivial File Transfer Protocol).
- Sie müssen eine unterstützte Firmware-Version verwenden.

  "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.

- Sie können diese Aufgabe nur bei Bridges FibreBridge 7600N oder 7500N in Konfigurationen mit ONTAP 9.4 oder höher verwenden.
- Sie müssen diese Aufgabe auf jeder FibreBridge-Brücke in der MetroCluster-Konfiguration ausführen, damit alle Brücken dieselbe Firmware-Version ausführen.

Diese Prozedur ist unterbrechungsfrei und dauert etwa 30 Minuten.

Ab ONTAP 9.8 ersetzt der `system bridge` Befehl den `storage bridge`. Im Folgenden wird der Befehl angezeigt `system bridge`. Wenn Sie jedoch eine Version vor ONTAP 9.8 ausführen, sollten Sie den Befehl verwenden `storage bridge`.

Schritte

1. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt:

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

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

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

2. Gehen Sie zur Seite ATTO FibreBridge und wählen Sie die passende Firmware für Ihre Bridge aus.

   "ATTO FibreBridge Firmware-Download-Seite"

3. Überprüfen Sie die Vorsichtsprüfung/MustRead- und Endbenutzervereinbarung, und klicken Sie auf das Kontrollkästchen, um die Annahme anzuzeigen und fortzufahren.
4. Platzieren Sie die Firmware-Datei an einem Netzwerkspeicherort, der für die Controller-Module netzwerkgerecht wird.

   Sie können die Befehle in den verbleibenden Schritten von der Konsole eines der beiden Controller-Module aus eingeben.

5. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   Sie müssen mit „`y`“ antworten, wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*>) anzuzeigen.

6. Aktualisieren Sie die Bridge-Firmware.

   Ab ONTAP 9.16.1 können Sie Anmeldeinformationen verwenden, um die Bridge-Firmware zu aktualisieren, wenn sie vom Server zum Herunterladen des Firmware-Pakets benötigt werden.

Wenn Anmeldedaten nicht erforderlich sind:

a. Aktualisieren Sie die Bridge-Firmware:

```
system bridge firmware update -bridge <name> -uri <URL-of-firmware-
package>
```

Beispiel

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD
```

Wenn Anmeldeinformationen erforderlich sind:

a. Aktualisieren Sie die Bridge-Firmware, und geben Sie den erforderlichen Benutzernamen an:

```
system bridge firmware update -bridge <name> -uri <URL-of-
firmware-package> -username <name>
```

b. Geben Sie das Passwort ein, wenn Sie in der Ausgabe dazu aufgefordert werden, wie im folgenden Beispiel gezeigt:

Beispiel

```
cluster_A> system bridge firmware update -bridge bridge_A_1a -uri
http://192.168.132.97/firmware.ZBD -username abc

(system bridge)

Enter the password:

[Job 70] Job is queued: System bridge firmware update job.
```

7. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

8. Vergewissern Sie sich, dass die Firmware-Aktualisierung abgeschlossen ist:

   ```
   job show -name "<job_name>"
   ```

   Das folgende Beispiel zeigt, dass der Job „`sSystem Bridge Firmware Update`“ noch ausgeführt wird:

```
cluster_A> job show -name "system bridge firmware update"
Owning

Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
2246   job-name
                            cluster_A
                                       node_A_1
                                                      Running
Description: System bridge firmware update job
```

Nach etwa 10 Minuten ist die neue Firmware vollständig installiert und der Auftragsstatus wird erfolgreich sein:

```
cluster_A> job show -name "system bridge firmware update"

                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
2246   System bridge firmware update
                            cluster_A
                                       node_A_1
                                                      Success
Description: System bridge firmware update job
```

9. Führen Sie die Schritte aus, ob die bandinterne Verwaltung aktiviert ist und welche Version von ONTAP Ihr System ausgeführt wird:

   - Wenn Sie ONTAP 9.4 ausführen, wird die bandinterne Verwaltung nicht unterstützt, und der Befehl muss von der Bridge-Konsole ausgegeben werden:

     i. Führen Sie die aus `flashimages` Befehl an der Konsole der Bridge und vergewissern Sie sich, dass die korrekten Firmware-Versionen angezeigt werden.

     > Das Beispiel zeigt, dass das primäre Flash-Image das neue Firmware-Image anzeigt, während das sekundäre Flash-Image das alte Image anzeigt.

     ```
     flashimages

      ;Type Version
     ;=====================================================
     Primary 3.16 001H
     Secondary 3.15 002S
     Ready.
     ```

a. Starten Sie die Bridge neu, indem Sie den ausführen `firmwarerestart` Befehl von der Bridge aus.
   - Wenn Sie ONTAP 9.5 oder höher ausführen, wird das bandinterne Management unterstützt, und der Befehl kann an der Cluster-Eingabeaufforderung ausgegeben werden:

b. Führen Sie den `system bridge run-cli -name <bridge_name> -command FlashImages` Befehl aus.

> Das Beispiel zeigt, dass das primäre Flash-Image das neue Firmware-Image anzeigt, während das sekundäre Flash-Image das alte Image anzeigt.

```
cluster_A> system bridge run-cli -name ATTO_7500N_IB_1 -command
FlashImages

[Job 2257]

;Type         Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.


[Job 2257] Job succeeded.
```

a. Falls erforderlich, starten Sie die Bridge neu:

```
system bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart
```

> Ab ATTO Firmware Version 2.95 wird die Bridge automatisch neu gestartet und dieser Schritt ist nicht erforderlich.

10. Überprüfen Sie, ob die Bridge ordnungsgemäß neu gestartet wurde:

```
sysconfig
```

Das System sollte für Multipath High Availability (beide Controller haben Zugriff über die Brücken zu den Platten-Shelfs in jedem Stack) verkabelt werden.

```
cluster_A> node run -node cluster_A-01 -command sysconfig
NetApp Release 9.6P8: Sat May 23 16:20:55 EDT 2020
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-
02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

11. Überprüfen Sie, ob die FibreBridge-Firmware aktualisiert wurde:

    `system bridge show -fields fw-version,symbolic-name`

    ```
    cluster_A> system bridge show -fields fw-version,symbolic-name
    name fw-version symbolic-name
    ---------------- ---------------- -------------
    ATTO_20000010affeaffe 3.10 A06X bridge_A_1a
    ATTO_20000010affeffae 3.10 A06X bridge_A_1b
    ATTO_20000010affeafff 3.10 A06X bridge_A_2a
    ATTO_20000010affeaffa 3.10 A06X bridge_A_2b
    4 entries were displayed.
    ```

12. Überprüfen Sie, ob die Partitionen in der Bridge-Eingabeaufforderung aktualisiert wurden:

    `flashimages`

    Das primäre Flash-Image zeigt das neue Firmware-Image an, während das sekundäre Flash-Image das alte Image anzeigt.

    ```
    Ready.
    flashimages

    ;Type         Version
    ;=====================================================
       Primary    3.16 001H
     Secondary    3.15 002S

     Ready.
    ```

13. Wiederholen Sie die Schritte 5 bis 10, um sicherzustellen, dass beide Flash-Images auf dieselbe Version aktualisiert werden.
14. Vergewissern Sie sich, dass beide Flash-Images auf dieselbe Version aktualisiert wurden.

    `flashimages`

    Die Ausgabe sollte für beide Partitionen dieselbe Version anzeigen.

```
Ready.
flashimages

;Type         Version
;=====================================================
   Primary    3.16 001H
 Secondary    3.16 001H

 Ready.
```

15. Wiederholen Sie die Schritte 5 bis 13 auf der nächsten Brücke, bis alle Brücken in der MetroCluster-Konfiguration aktualisiert wurden.

Austauschen einer einzelnen FC-to-SAS-Bridge

Sie können eine Bridge unterbrechungsfrei durch dieselbe Modellbrücke oder durch eine neue Modellbrücke ersetzen.

Bevor Sie beginnen

Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

Über diese Aufgabe

Diese Prozedur ist unterbrechungsfrei und dauert etwa 60 Minuten.

Bei diesem Verfahren wird über die Bridge-CLI eine Bridge konfiguriert und verwaltet, und die Bridge-Firmware und das ATTO Quicknav-Dienstprogramm aktualisiert, um den Bridge Ethernet Management 1-Port zu konfigurieren. Sie können andere Schnittstellen verwenden, wenn sie die Anforderungen erfüllen.

"Anforderungen für die Verwendung anderer Schnittstellen zur Konfiguration und Verwaltung von FibreBridge-Brücken"

Verwandte Informationen

"Austausch von zwei FibreBridge 6500N-Brücken durch 7600N- oder 7500N-Brücken"

Überprüfung der Storage-Konnektivität

Vor dem Austausch von Brücken sollten Sie die Verbindung zu Bridge und Storage überprüfen. Wenn Sie sich die Befehlsausgabe vertraut machen, können Sie die Konnektivität nach Konfigurationsänderungen nachträglich überprüfen.

Über diese Aufgabe

Sie können diese Befehle von der Admin-Eingabeaufforderung eines der Controller-Module in der MetroCluster-Konfiguration am Standort, der gewartet wird, ausgeben.

Schritte

1. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:

   ```
   run local sysconfig -v
   ```

In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
```

```
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Hot-Swap-durchführen einer Bridge mit einer Ersatzbrücke desselben Modells

Sie können eine fehlerhafte Bridge durch eine andere Brücke desselben Modells im laufenden Betrieb austauschen.

Über diese Aufgabe

Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den entsprechenden Schritten angegeben.

> 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. Wenn auf die alte Brücke zugegriffen werden kann, können Sie die Konfigurationsinformationen abrufen.

Wenn…	Dann…
Sie verwenden IP-Management	Stellen Sie über eine Telnet-Verbindung eine Verbindung mit der alten Bridge her, und kopieren Sie die Ausgabe der Bridge-Konfiguration.

• Sie verwenden in-Band-Management*	Verwenden Sie die ONTAP CLI, um die Konfigurationsinformationen mit den folgenden Befehlen abzurufen:
	
	`storage bridge run-cli -name` *`bridge-name`* `-command "info"`
	
	`storage bridge run-cli -name` *`bridge-name`* `-command "sasportlist"`

   a. Geben Sie den Befehl ein:

   `storage bridge run-cli -name bridge_A1 -command "info"`

   ```
   info
   ```

```
Device Status         = Good
Unsaved Changes       = None
Device                = "FibreBridge 7500N"
Serial Number         = FB7500N100000
Device Version        = 3.10
Board Revision        = 7
Build Number          = 007A
Build Type            = Release
Build Date            = "Aug 20 2019" 11:01:24
Flash Revision        = 0.02
Firmware Version      = 3.10
BCE Version (FPGA 1)  = 15
BAU Version (FPGA 2)  = 33
User-defined name     = "bridgeA1"
World Wide Name       = 20 00 00 10 86 A1 C7 00
MB of RAM Installed   = 512
FC1 Node Name         = 20 00 00 10 86 A1 C7 00
FC1 Port Name         = 21 00 00 10 86 A1 C7 00
FC1 Data Rate         = 16Gb
FC1 Connection Mode   = ptp
FC1 FW Revision       = 11.4.337.0
FC2 Node Name         = 20 00 00 10 86 A1 C7 00
FC2 Port Name         = 22 00 00 10 86 A1 C7 00
FC2 Data Rate         = 16Gb
FC2 Connection Mode   = ptp
FC2 FW Revision       = 11.4.337.0
SAS FW Revision       = 3.09.52
MP1 IP Address        = 10.10.10.10
MP1 IP Subnet Mask    = 255.255.255.0
MP1 IP Gateway        = 10.10.10.1
MP1 IP DHCP           = disabled
MP1 MAC Address       = 00-10-86-A1-C7-00
MP2 IP Address        = 0.0.0.0 (disabled)
MP2 IP Subnet Mask    = 0.0.0.0
MP2 IP Gateway        = 0.0.0.0
MP2 IP DHCP           = enabled
MP2 MAC Address       = 00-10-86-A1-C7-01
SNMP                  = enabled
SNMP Community String = public
PS A Status           = Up
PS B Status           = Up
Active Configuration  = NetApp

Ready.
```

b. Geben Sie den Befehl ein:

```
storage bridge run-cli -name bridge_A1 -command "sasportlist"
```

```
SASPortList

;Connector      PHY     Link            Speed   SAS Address
;==============================================================
Device  A       1       Up              6Gb     5001086000a1c700
Device  A       2       Up              6Gb     5001086000a1c700
Device  A       3       Up              6Gb     5001086000a1c700
Device  A       4       Up              6Gb     5001086000a1c700
Device  B       1       Disabled        12Gb    5001086000a1c704
Device  B       2       Disabled        12Gb    5001086000a1c704
Device  B       3       Disabled        12Gb    5001086000a1c704
Device  B       4       Disabled        12Gb    5001086000a1c704
Device  C       1       Disabled        12Gb    5001086000a1c708
Device  C       2       Disabled        12Gb    5001086000a1c708
Device  C       3       Disabled        12Gb    5001086000a1c708
Device  C       4       Disabled        12Gb    5001086000a1c708
Device  D       1       Disabled        12Gb    5001086000a1c70c
Device  D       2       Disabled        12Gb    5001086000a1c70c
Device  D       3       Disabled        12Gb    5001086000a1c70c
Device  D       4       Disabled        12Gb    5001086000a1c70c
```

2. Wenn sich die Bridge in einer Fabric-Attached MetroCluster-Konfiguration befindet, deaktivieren Sie alle Switch-Ports, die mit dem Bridge-FC-Port oder -Ports verbunden sind.
3. Entfernen Sie von der ONTAP-Cluster-Eingabeaufforderung die Bridge, die gerade gewartet wird, aus dem Systemzustandsüberwachungs-Monitoring:
   a. Entfernen Sie die Brücke:
      `storage bridge remove -name bridge-name`
   b. Zeigen Sie die Liste der überwachten Brücken an und bestätigen Sie, dass die entfernte Brücke nicht vorhanden ist:
      `storage bridge show`
4. Richtig gemahlen.
5. Schalten Sie die ATTO-Brücke aus, und entfernen Sie die an die Brücke angeschlossenen Stromkabel.
6. Ziehen Sie die Kabel ab, die mit der alten Brücke verbunden sind.

   Notieren Sie sich den Anschluss, an den jedes Kabel angeschlossen war.

7. Entfernen Sie die alte Brücke vom Rack.
8. Die neue Brücke in das Rack einbauen.
9. Schließen Sie das Netzkabel wieder an, und wenn Sie für den IP-Zugriff auf die Bridge konfigurieren, ist ein abgeschirmtes Ethernet-Kabel vorhanden.

> Sie dürfen die SAS- oder FC-Kabel derzeit nicht wieder anschließen.

10. Schließen Sie die Bridge an eine Stromquelle an, und schalten Sie sie dann ein.

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

11. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

    Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.

12. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

    In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

    Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

13. Konfigurieren Sie die Bridge.

    Wenn Sie die Konfigurationsinformationen von der alten Bridge abgerufen haben, konfigurieren Sie die neue Bridge mit den Informationen.

    Notieren Sie sich den von Ihnen bestimmen Benutzernamen und das Kennwort.

    Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihr Bridge-Modell enthält die aktuellsten Informationen zu verfügbaren Befehlen und deren Verwendung.

    > Konfigurieren Sie die Zeitsynchronisierung auf ATTO FibreBridge 7600N oder 7500N nicht. Die Zeitsynchronisierung für ATTO FibreBridge 7600N oder 7500N ist auf die Cluster-Zeit eingestellt, nachdem die Brücke von ONTAP erkannt wurde. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

    a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

       Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle Verbindung mit der FibreBridge.

       Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

       ```
       set ipaddress mp1 _ip-address
       ```

       ```
       set ipsubnetmask mp1 subnet-mask
       ```

       ```
       set ipgateway mp1 x.x.x.x
       ```

```
set ipdhcp mp1 disabled

set ethernetspeed mp1 1000
```

b. Konfigurieren Sie den Brückennamen.

   Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

   Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

   - Bridge_A_1a
   - Bridge_A_1b
   - Bridge_B_1a
   - Bridge_B_1b

     Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set bridgename bridgename
```

c. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:

```
set SNMP enabled
```

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

14. Konfigurieren Sie die Bridge-FC-Ports.

    a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

       Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

       - Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
       - Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.

       > Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch von dem Switch unterstützt wird, an den der Bridge-Port angeschlossen wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

       Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set FCDataRate port-number port-speed
```

    b. Wenn Sie eine FibreBridge 7500N konfigurieren, konfigurieren Sie den Verbindungsmodus, den der Port für „ptp“ verwendet.

       > Die Einstellung FCConnMode ist nicht erforderlich, wenn Sie eine FibreBridge 7600N-Bridge konfigurieren.

Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set FCConnMode port-number ptp
```

c. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, müssen Sie den FC2-Port konfigurieren oder deaktivieren.
   - Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
   - Wenn Sie den zweiten Port nicht verwenden, müssen Sie den Port deaktivieren:

     ```
     FCPortDisable port-number
     ```

d. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, deaktivieren Sie die nicht verwendeten SAS-Ports:

   ```
   SASPortDisable sas-port
   ```

   > SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren. Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein.

15. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration.

    a. Überprüfen Sie in der Eingabeaufforderung des Controllers den Status der Brücken: `storage bridge show`

       Der Ausgang zeigt an, welche Brücke nicht gesichert ist.

    b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:

       ```
       info
       ```

       Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.

    c. Wenn Ethernet-Port MP1 aktiviert ist, führen Sie den folgenden Befehl aus:

       ```
       set EthernetPort mp1 disabled
       ```

       > Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.

    d. Die Konfiguration der Bridge speichern.

       Sie müssen die folgenden Befehle ausführen:

       ```
       SaveConfiguration
       ```

       ```
       FirmwareRestart
       ```

    Sie werden aufgefordert, die Bridge neu zu starten.

16. Schließen Sie die FC-Kabel an dieselben Ports an der neuen Bridge an.

17. Aktualisieren Sie die FibreBridge-Firmware auf jeder Bridge.

    Wenn die neue Bridge vom gleichen Typ wie die Partner Bridge ist, aktualisieren Sie auf dieselbe Firmware wie die Partner Bridge. Falls sich die neue Brücke von einem anderen Typ der Partnerbrücke unterscheidet, aktualisieren Sie auf die neueste Firmware, die von der Bridge und Version von ONTAP unterstützt wird. Siehe "Firmware auf einer FibreBridge-Bridge aktualisieren"

18. Schließen Sie die SAS-Kabel wieder an die gleichen Ports der neuen Bridge an.

    Sie müssen die Kabel austauschen, die die Brücke mit der oberen oder unteren Seite des Regalstapels verbinden. Für die FibreBridge 7600N- und 7500N-Brücken sind Mini-SAS-Kabel für diese Verbindungen erforderlich.

    > Warten Sie mindestens 10 Sekunden, bevor Sie den Anschluss anschließen. Die SAS-Kabelanschlüsse sind codiert. Wenn sie sich korrekt in einen SAS-Port orientieren, klicken sie auf ihren Platz und die Festplatten-Shelf-SAS-Port LNK-LED leuchtet grün. Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche. Bei Controllern kann die Ausrichtung der SAS-Ports je nach Plattformmodell variieren. Daher variiert die korrekte Ausrichtung des SAS-Kabelsteckers.

19. Stellen Sie sicher, dass jede Bridge alle Festplattenlaufwerke und Festplatten-Shelfs sehen kann, mit denen die Bridge verbunden ist.

Wenn Sie den…	Dann…
ATTO ExpressNAV GUI	a. Geben Sie in einem unterstützten Webbrowser die IP-Adresse der Bridge in das Browserfenster ein. Sie werden auf die ATTO FibreBridge Homepage gebracht, die einen Link hat. b. Klicken Sie auf den Link, und geben Sie dann Ihren Benutzernamen und das Passwort ein, das Sie beim Konfigurieren der Bridge festgelegt haben. Die ATTO FibreBridge-Statusseite wird mit einem Menü links angezeigt. c. Klicken Sie im Menü auf **Erweitert**. d. Anzeigen der angeschlossenen Geräte: `sastargets` e. Klicken Sie Auf **Absenden**.
Serieller Anschluss	Anzeigen der angeschlossenen Geräte: `sastargets`

    Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Die Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können.

Wenn die abgeschnittene Textantwort zu Beginn der Ausgabe angezeigt wird, können Sie Telnet verwenden, um eine Verbindung zur Bridge herzustellen, und dann die gesamte Ausgabe über anzeigen `sastargets` Befehl.

Die folgende Ausgabe zeigt, dass 10 Festplatten angeschlossen sind:

```
Tgt VendorID ProductID        Type SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK 3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK 3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK 3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK 3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK 3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK 3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK 3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK 3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK 3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK 3QP1FXW600009940VERQ
```

20. Überprüfen Sie, ob in der Befehlsausgabe angezeigt wird, dass die Bridge mit allen entsprechenden Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Sie den Schritt 19Vorgang für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie die SAS-Kabel auf lose Kabel, oder korrigieren Sie die SAS-Verkabelung, indem Sie wiederholenSchritt 18. b. Wiederholen.Schritt 19

21. Wenn sich die Bridge in einer Fabric-Attached MetroCluster-Konfiguration befindet, aktivieren Sie den FC-Switch-Port, den Sie zu Beginn dieses Verfahrens deaktiviert haben.

    Dies sollte der Port sein, der mit der Brücke verbunden ist.

22. Überprüfen Sie über die Systemkonsole beider Controller-Module, ob alle Controller-Module über die neue Bridge auf die Festplatten-Shelfs zugreifen können (d. h. dass das System für Multipath HA verkabelt ist):

    ```
    run local sysconfig
    ```

    Es kann bis zu einer Minute dauern, bis das System die Erkennung abgeschlossen hat.

    Wenn die Ausgabe Multipath HA nicht angibt, müssen Sie die SAS- und FC-Verkabelung korrigieren, da nicht alle Festplattenlaufwerke über die neue Bridge zugänglich sind.

    Die folgende Ausgabe gibt an, dass das System für Multipath HA verkabelt ist:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

> Wenn das System nicht als Multipath HA verkabelt ist, kann der Neustart einer Bridge zum Verlust des Zugriffs auf die Festplatten und zu einer Panik mehrerer Festplatten führen.

23. Wenn ONTAP 9.4 oder früher ausgeführt wird, vergewissern Sie sich, dass die Bridge für SNMP konfiguriert ist.

    Wenn Sie die Bridge-CLI verwenden, führen Sie den folgenden Befehl aus:

    ```
    get snmp
    ```

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

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

ONTAP-Version	Befehl
9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
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 bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP-Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „`Status`“ „`ok`“ lautet und weitere Informationen, 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::>
```

25. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
    a. Überprüfen Sie, ob das System multipathed ist:
       `node run -node node-name sysconfig -a`
    b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:
       `system health alert show`
    c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
       `metrocluster show`
    d. Führen Sie eine MetroCluster-Prüfung durch:
       `metrocluster check run`
    e. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
       `metrocluster check show`
    f. Überprüfen Sie, ob auf den Switches Zustandswarnmeldungen angezeigt werden (falls vorhanden):
       `storage switch show`
    g. Nutzen Sie Config Advisor.

       "NetApp Downloads: Config Advisor"

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

Verwandte Informationen

"In-Band-Management der FC-to-SAS-Bridges"

Hot-Swap einer FibreBridge 7500N mit einer 7600N-Brücke

Sie können eine FibreBridge 7500N-Bridge im laufenden Betrieb durch eine 7600N-Brücke austauschen.

Über diese Aufgabe

Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den entsprechenden Schritten angegeben.

> 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. Wenn sich die Bridge in einer Fabric-Attached MetroCluster-Konfiguration befindet, deaktivieren Sie alle Switch-Ports, die mit dem Bridge-FC-Port oder -Ports verbunden sind.
2. Entfernen Sie von der ONTAP-Cluster-Eingabeaufforderung die Bridge, die gerade gewartet wird, aus dem Systemzustandsüberwachungs-Monitoring:
   a. Entfernen Sie die Brücke:
      `storage bridge remove -name` *`bridge-name`*
   b. Zeigen Sie die Liste der überwachten Brücken an und bestätigen Sie, dass die entfernte Brücke nicht vorhanden ist:
      `storage bridge show`
3. Richtig gemahlen.
4. Entfernen Sie die an der Bridge angeschlossenen Netzkabel, um die Bridge herunterzufahren.
5. Ziehen Sie die Kabel ab, die mit der alten Brücke verbunden sind.

   Notieren Sie sich den Anschluss, an den jedes Kabel angeschlossen war.
6. Entfernen Sie die alte Brücke vom Rack.
7. Die neue Brücke in das Rack einbauen.
8. Schließen Sie das Netzkabel und das abgeschirmte Ethernet-Kabel wieder an.

   > Sie dürfen die SAS- oder FC-Kabel derzeit nicht wieder anschließen.
9. Schließen Sie die Bridge an eine Stromquelle an, und schalten Sie sie dann ein.

   Die LED „Bridge Ready“ kann bis zu 30 Sekunden in Anspruch nehmen, was darauf hinweist, dass die Bridge ihre Selbsttestsequenz beim Einschalten abgeschlossen hat.
10. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

    Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.
11. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

    Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.
12. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede

Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

13. Konfigurieren Sie die Brücken.

    Notieren Sie sich den von Ihnen bestimmen Benutzernamen und das Kennwort.

    Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihr Bridge-Modell enthält die aktuellsten Informationen zu verfügbaren Befehlen und deren Verwendung.

    > Konfigurieren Sie die Zeitsynchronisierung auf FibreBridge 7600N nicht. Die Zeitsynchronisierung für FibreBridge 7600N ist nach dem Entdeckung der Brücke durch ONTAP auf die Cluster-Zeit eingestellt. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

    a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

       Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle Verbindung mit der FibreBridge.

       Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

       ```
       set ipaddress mp1 ip-address

       set ipsubnetmask mp1 subnet-mask

       set ipgateway mp1 x.x.x.x

       set ipdhcp mp1 disabled

       set ethernetspeed mp1 1000
       ```

    b. Konfigurieren Sie den Brückennamen.

       Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

       Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

       - Bridge_A_1a
       - Bridge_A_1b
       - Bridge_B_1a
       - Bridge_B_1b

         Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set bridgename bridgename
```

a. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:
```
set SNMP enabled
```

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

14. Konfigurieren Sie die Bridge-FC-Ports.

a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

- Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
- Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.

> Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch vom FC-Port des Controller-Moduls oder vom Switch unterstützt wird, mit dem der Bridge-Port verbunden wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set FCDataRate port-number port-speed
```

b. Sie müssen den FC2-Port konfigurieren oder deaktivieren.

- Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
- Wenn Sie den zweiten Port nicht verwenden, müssen Sie den nicht verwendeten Port deaktivieren:

```
FCPortDisable port-number
```

Im folgenden Beispiel wird die Deaktivierung von FC-Port 2 gezeigt:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

c. Deaktivieren Sie die nicht verwendeten SAS-Ports:

```
SASPortDisable sas-port
```

> SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren.

Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein. Im

folgenden Beispiel wird die Deaktivierung von SAS Port B. gezeigt Sie müssen die SAS-Ports C und D ähnlich deaktivieren:

```
SASPortDisable b

SAS Port B has been disabled.
```

15. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration.

    a. Überprüfen Sie in der Eingabeaufforderung des Controllers den Status der Brücken:

    ```
    storage bridge show
    ```

    Der Ausgang zeigt an, welche Brücke nicht gesichert ist.

    b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:

    ```
    info
    ```

    Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.

    c. Wenn Ethernet-Port MP1 aktiviert ist, führen Sie den folgenden Befehl aus:

    ```
    set EthernetPort mp1 disabled
    ```

    > Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.

    d. Die Konfiguration der Bridge speichern.

    Sie müssen die folgenden Befehle ausführen: +

    ```
    SaveConfiguration

    FirmwareRestart
    ```

    Sie werden aufgefordert, die Bridge neu zu starten.

16. Schließen Sie die FC-Kabel an dieselben Ports an der neuen Bridge an.
17. Aktualisieren Sie die FibreBridge-Firmware auf jeder Bridge.

    "Aktualisieren Sie die Firmware auf einer FibreBridge-Bridge"

18. Verbinden Sie die SAS-Kabel wieder mit denselben Ports an der neuen Bridge.

> Warten Sie mindestens 10 Sekunden, bevor Sie den Anschluss anschließen. Die SAS-Kabelanschlüsse sind codiert. Wenn sie sich korrekt in einen SAS-Port orientieren, klicken sie auf ihren Platz und die Festplatten-Shelf-SAS-Port LNK-LED leuchtet grün. Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche. Bei Controllern kann die Ausrichtung der SAS-Ports je nach Plattformmodell variieren. Daher variiert die korrekte Ausrichtung des SAS-Kabelsteckers.

19. Überprüfen Sie, ob jede Bridge alle Festplattenlaufwerke und Platten-Shelfs, mit denen die Bridge verbunden ist, sehen kann:

    ```
    sastargets
    ```

    Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Die Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können.

    Die folgende Ausgabe zeigt, dass 10 Festplatten angeschlossen sind:

    ```
    Tgt VendorID ProductID        Type        SerialNumber
      0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
      1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
      2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
      3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
      4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
      5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
      6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
      7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
      8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
      9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
    ```

20. Überprüfen Sie, ob in der Befehlsausgabe angezeigt wird, dass die Bridge mit allen entsprechenden Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Sie den vorherigen Schritt für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie die SAS-Kabel auf lose Kabel, oder korrigieren Sie die SAS-Verkabelung, indem Sie wiederholenSchritt 18. b. Wiederholen Sie den vorherigen Schritt.

21. Wenn sich die Bridge in einer Fabric-Attached MetroCluster-Konfiguration befindet, aktivieren Sie den FC-Switch-Port, den Sie zu Beginn dieses Verfahrens deaktiviert haben.

    Dies sollte der Port sein, der mit der Brücke verbunden ist.

22. Überprüfen Sie über die Systemkonsole beider Controller-Module, ob alle Controller-Module über die neue Bridge auf die Festplatten-Shelfs zugreifen können (d. h. dass das System für Multipath HA verkabelt ist):

```
run local sysconfig
```

> Es kann bis zu einer Minute dauern, bis das System die Erkennung abgeschlossen hat.

Wenn die Ausgabe Multipath HA nicht angibt, müssen Sie die SAS- und FC-Verkabelung korrigieren, da nicht alle Festplattenlaufwerke über die neue Bridge zugänglich sind.

Die folgende Ausgabe gibt an, dass das System für Multipath HA verkabelt ist:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

> Wenn das System nicht als Multipath HA verkabelt ist, kann der Neustart einer Bridge zum Verlust des Zugriffs auf die Festplatten und zu einer Panik mehrerer Festplatten führen.

23. Wenn ONTAP 9.4 oder früher ausgeführt wird, vergewissern Sie sich, dass die Bridge für SNMP konfiguriert ist.

    Wenn Sie die Bridge-CLI verwenden, führen Sie den folgenden Befehl aus:

    ```
    get snmp
    ```

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

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

ONTAP-Version	Befehl
9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
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 bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP-Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „`Status`“ „`ok`“ lautet und weitere Informationen, 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::>
```

25. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
    a. Überprüfen Sie, ob das System multipathed ist:
       `node run -node node-name sysconfig -a`
    b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:
       `system health alert show`
    c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
       `metrocluster show`
    d. Führen Sie eine MetroCluster-Prüfung durch:
       `metrocluster check run`
    e. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an: +

       `metrocluster check show`

    f. Überprüfen Sie, ob auf den Switches Zustandswarnmeldungen angezeigt werden (falls vorhanden):
       `storage switch show`
    g. Nutzen Sie Config Advisor.

       "NetApp Downloads: Config Advisor"

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

Verwandte Informationen

"In-Band-Management der FC-to-SAS-Bridges"

Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke

Sie können eine FibreBridge 6500N-Bridge im laufenden Betrieb durch eine FibreBridge 7600N- oder 7500N-Bridge austauschen, um eine fehlerhafte Bridge zu ersetzen oder Ihre Bridge in einer Fabric-Attached-Konfiguration oder einer MetroCluster-Bridge-Verbindung zu aktualisieren.

Über diese Aufgabe

- Dieses Verfahren dient zum Hot-Swap einer einzelnen FibreBridge 6500N-Bridge mit einer einzigen FibreBridge 7600N oder 7500N-Brücke.
- Wenn Sie eine FibreBridge 6500N-Bridge im laufenden Betrieb durch eine FibreBridge 7600N- oder 7500N-Bridge austauschen, müssen Sie nur einen FC-Port und einen SAS-Port auf der FibreBridge 7600N oder 7500N verwenden.
- Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den entsprechenden Schritten angegeben.

> Wenn Sie beide FibreBridge 6500N-Brücken Hot-Swap in ein Paar einsetzen, müssen Sie das verwenden "Konsolidierung Mehrerer Storage Stacks" Verfahren für Zoning-Anweisungen. Durch den Austausch beider FibreBridge 6500N-Brücken auf der Brücke können Sie die zusätzlichen Ports auf der FibreBridge 7600N oder 7500N-Brücke nutzen.

> 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. Führen Sie einen der folgenden Schritte aus:
   - Wenn sich die fehlerhafte Bridge in einer Fabric-Attached MetroCluster-Konfiguration befindet, deaktivieren Sie den Switch-Port, der mit dem Bridge-FC-Port verbunden ist.
   - Wenn sich die ausgefallene Bridge in einer Stretch-MetroCluster-Konfiguration befindet, verwenden Sie einen der verfügbaren FC-Ports.
2. Entfernen Sie von der ONTAP-Cluster-Eingabeaufforderung die Bridge, die gerade gewartet wird, aus dem Systemzustandsüberwachungs-Monitoring:
   a. Entfernen Sie die Brücke:

      ```
      storage bridge remove -name bridge-name
      ```

   b. Zeigen Sie die Liste der überwachten Brücken an und bestätigen Sie, dass die entfernte Brücke nicht vorhanden ist:

      ```
      storage bridge show
      ```

3. Richtig gemahlen.
4. Schalten Sie den Netzschalter der Brücke aus.
5. Trennen Sie die Kabel vom Shelf an die FibreBridge 6500N-Bridge-Ports und die Netzkabel.

   Beachten Sie die Anschlüsse, mit denen jedes Kabel verbunden war.

6. Entfernen Sie die FibreBridge 6500N-Brücke, die Sie aus dem Rack ersetzen müssen.

7. Setzen Sie die neue FibreBridge 7600N oder 7500N in das Rack ein.
8. Schließen Sie das Netzkabel und gegebenenfalls das abgeschirmte Ethernet-Kabel wieder an.

   Schließen Sie derzeit nicht die SAS- oder FC-Kabel wieder an.

9. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

   Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.

10. Wenn Sie die IP-Verwaltung konfigurieren, schließen Sie den Ethernet-Management-1-Port an jeder Bridge über ein Ethernet-Kabel an das Netzwerk an.

    In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

    Der Ethernet Management 1 Port ermöglicht es Ihnen, schnell die Bridge-Firmware (über ATTO ExpressNAV oder FTP Management-Schnittstellen) herunterzuladen und Core-Dateien und Extrahieren von Logs abzurufen.

11. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

    In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

    Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

12. Konfigurieren Sie die Bridge.

    Wenn Sie die Konfigurationsinformationen von der alten Bridge abgerufen haben, konfigurieren Sie die neue Bridge mit den Informationen.

    Notieren Sie sich den von Ihnen bestimmen Benutzernamen und das Kennwort.

    Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihr Bridge-Modell enthält die aktuellsten Informationen zu verfügbaren Befehlen und deren Verwendung.

    Konfigurieren Sie die Zeitsynchronisierung auf ATTO FibreBridge 7600N oder 7500N nicht. Die Zeitsynchronisierung für ATTO FibreBridge 7600N oder 7500N ist auf die Cluster-Zeit eingestellt, nachdem die Brücke von ONTAP erkannt wurde. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

    a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

       Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle

Verbindung mit der FibreBridge.

Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

```
set ipaddress mp1 ip-address

set ipsubnetmask mp1 subnet-mask

set ipgateway mp1 x.x.x.x

set ipdhcp mp1 disabled

set ethernetspeed mp1 1000
```

b. Konfigurieren Sie den Brückennamen.

Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

- Bridge_A_1a
- Bridge_A_1b
- Bridge_B_1a
- Bridge_B_1b

Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set bridgename bridgename
```

a. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:
`set SNMP enabled`

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

13. Konfigurieren Sie die Bridge-FC-Ports.

a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

- Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
- Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.
- Die FibreBridge 6500N unterstützt bis zu 8, 4 oder 2 Gbit/s.

> Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch von dem Switch unterstützt wird, an den der Bridge-Port angeschlossen wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set FCDataRate port-number port-speed
```

b. Wenn Sie eine FibreBridge 7500N oder 6500N-Bridge konfigurieren, konfigurieren Sie den Verbindungsmodus, den der Port für ptp verwendet.

> Die Einstellung FCConnMode ist nicht erforderlich, wenn Sie eine FibreBridge 7600N-Bridge konfigurieren.

Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

```
set FCConnMode port-number ptp
```

c. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, müssen Sie den FC2-Port konfigurieren oder deaktivieren.
   - Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
   - Wenn Sie den zweiten Port nicht verwenden, müssen Sie den Port deaktivieren:

     ```
     FCPortDisable port-number
     ```

d. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, deaktivieren Sie die nicht verwendeten SAS-Ports:

```
SASPortDisable sas-port
```

> SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren. Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein.

14. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration.

a. Überprüfen Sie in der Eingabeaufforderung des Controllers den Status der Brücken:

```
storage bridge show
```

Der Ausgang zeigt an, welche Brücke nicht gesichert ist.

b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:

```
info
```

Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.

c. Wenn Ethernet-Port MP1 aktiviert ist, führen Sie den folgenden Befehl aus:

```
set EthernetPort mp1 disabled
```

> Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.

d. Die Konfiguration der Bridge speichern.

   Sie müssen die folgenden Befehle ausführen:

   ```
   SaveConfiguration
   ```

   ```
   FirmwareRestart
   ```

Sie werden aufgefordert, die Bridge neu zu starten.

15. Schalten Sie die Funktionsüberwachung für die FibreBridge 7600N oder 7500N ein.
16. Schließen Sie die FC-Kabel an die Fibre-Channel-1-Ports der neuen Bridge an.

    Sie müssen den FC-Port mit demselben Switch oder Controller-Port verkabeln, mit dem auch die FibreBridge 6500N Bridge verbunden war.

17. Aktualisieren Sie die FibreBridge-Firmware auf jeder Bridge.

    Wenn die neue Bridge vom gleichen Typ wie die Partner Bridge ist, aktualisieren Sie auf dieselbe Firmware wie die Partner Bridge. Wenn die neue Bridge einen anderen Typ als die Partner-Bridge hat, aktualisieren Sie auf die neueste Firmware und Version von ONTAP, die von der Bridge unterstützt wird.

    "Aktualisieren Sie die Firmware auf einer FibreBridge-Bridge"

18. Schließen Sie die SAS-Kabel wieder an die SAS A-Ports der neuen Bridge an.

    Der SAS-Port muss mit demselben Shelf-Port verbunden sein, mit dem die FibreBridge 6500N-Bridge verbunden war.

    > Erzwingen Sie keinen Anschluss in einen Port. Die Mini-SAS-Kabel sind codiert; wenn sie korrekt in einen SAS-Port ausgerichtet sind, klickt das SAS-Kabel an ihre Stelle und die Festplatten-Shelf-SAS-Port LNK LED leuchtet grün. Bei Festplatten-Shelfs setzen Sie einen SAS-Kabelanschluss ein, wobei die Zuglasche (auf der Unterseite des Connectors) nach unten ausgerichtet ist.bei Controllern kann die Ausrichtung der SAS-Ports je nach Plattformmodell variieren.Daher ist die richtige Ausrichtung des SAS-Kabelsteckers unterschiedlich.

19. Überprüfen Sie, ob die Bridge alle Festplattenlaufwerke und Platten-Shelfs erkennt, mit denen sie verbunden ist.

Wenn Sie den…	Dann…

ATTO ExpressNAV GUI	a. Geben Sie in einem unterstützten Webbrowser die IP-Adresse der Bridge in das Browserfenster ein. Sie werden auf die ATTO FibreBridge Homepage gebracht, die einen Link hat. b. Klicken Sie auf den Link, und geben Sie dann Ihren Benutzernamen und das Passwort ein, das Sie beim Konfigurieren der Bridge festgelegt haben. Die ATTO FibreBridge-Statusseite wird mit einem Menü links angezeigt. c. Klicken Sie im Menü auf **Erweitert**. d. Geben Sie den folgenden Befehl ein und klicken Sie dann auf **Senden**, um die Liste der für die Bridge sichtbaren Laufwerke anzuzeigen: `sastargets`
Serieller Anschluss	Zeigen Sie die Liste der für die Bridge sichtbaren Festplatten an: `sastargets`

Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können. Die folgende Ausgabe zeigt beispielsweise, dass 10 Festplatten verbunden sind:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

Wenn der Text “response cuted” am Anfang der Ausgabe erscheint, können Sie Telnet verwenden, um auf die Brücke zuzugreifen und den gleichen Befehl eingeben, um alle Ausgaben zu sehen.

20. Überprüfen Sie, ob in der Befehlsausgabe angezeigt wird, dass die Bridge mit allen notwendigen Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Sie den vorherigen Schritt für jede verbleibende Brücke.

Nicht richtig	a. Überprüfen Sie die SAS-Kabel auf lose Kabel, oder korrigieren Sie die SAS-Verkabelung, indem Sie wiederholenSchritt 18. b. Wiederholen Sie den vorherigen Schritt für jede verbleibende Brücke.

21. Aktivieren Sie den FC-Switch-Port, der mit der Bridge verbunden ist, wieder.
22. Überprüfen Sie an der Systemkonsole beider Controller, ob alle Controller über die neue Brücke auf die Festplatten-Shelfs zugreifen können (dass das System für Multipath HA verkabelt ist):

    `run local sysconfig`

    Es kann bis zu einer Minute dauern, bis das System die Erkennung abgeschlossen hat.

    Beispielsweise zeigt die folgende Ausgabe, dass das System für Multipath HA verkabelt ist:

    ```
    NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
    System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
    System Serial Number: 700000123123 (node_A_1); partner Serial Number:
    700000456456 (node_A_2)
    System Rev: B0
    System Storage Configuration: Multi-Path HA
    System ACP Connectivity: NA
    ```

    Wenn in der Befehlsausgabe angegeben wird, dass die Konfiguration Mixed-Path oder Single Path HA ist, müssen Sie die SAS- und FC-Verkabelung korrigieren, da nicht alle Festplattenlaufwerke über die neue Bridge zugänglich sind.

    Wenn das System nicht als Multipath HA verkabelt ist, kann der Neustart einer Bridge zum Verlust des Zugriffs auf die Festplatten und zu einer Panik mehrerer Festplatten führen.

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

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

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

    b. Überprüfen Sie, ob die Bridge hinzugefügt wurde und richtig konfiguriert ist:
    `storage bridge show`

    Es kann bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP-Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert

in der Spalte „`Status`“ „`ok`“ lautet und weitere Informationen, 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::>
```

24. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
    a. Prüfen Sie, ob das System multipathed ist:

       `node run -node node-name sysconfig -a`

    b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:
       `system health alert show`
    c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

       `metrocluster show`

    d. Durchführen einer MetroCluster-Prüfung:

       `metrocluster check run`

    e. Ergebnisse der MetroCluster-Prüfung anzeigen:

       `metrocluster check show`

    f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

       `storage switch show`

    g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

25. Nach dem Austausch des Teils senden Sie das fehlerhafte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe "Teilerückgabe Austausch" Seite für weitere Informationen.

Verwandte Informationen

"In-Band-Management der FC-to-SAS-Bridges"

Austausch von zwei FibreBridge 6500N-Brücken durch 7600N- oder 7500N-Brücken

Um die zusätzlichen FC2-Anschlüsse der FibreBridge 7600N oder 7500N-Brücken zu nutzen und die Rack-Auslastung zu verringern, können Sie 6500N-Brücken unterbrechungsfrei ersetzen und bis zu vier Speicher-Stacks hinter einem einzigen FibreBridge 7600N- oder 7500N-Paar konsolidieren.

Bevor Sie beginnen

Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

Über diese Aufgabe

Sie sollten dieses Verfahren verwenden, wenn:

- Sie ersetzen ein Paar FibreBridge 6500N-Brücken durch FibreBridge 7600N oder 7500N-Brücken.

  Nach dem Austausch müssen beide Brücken im Paar das gleiche Modell sein.

- Sie haben zuvor eine einzelne FibreBridge 6500N durch eine 7600N- oder 7500N-Brücke ersetzt und ersetzen nun die zweite Brücke im Paar.
- Sie verfügen über zwei Bridges aus FibreBridge 7600N oder 7500N mit verfügbaren SAS-Ports und Sie konsolidieren SAS-Storage-Stacks, die derzeit über FibreBridge 6500N-Brücken verbunden sind.

Dieser Vorgang läuft unterbrechungsfrei ab und dauert ungefähr zwei Stunden.

Verwandte Informationen

"Austauschen einer einzelnen FC-to-SAS-Bridge"

Überprüfung der Storage-Konnektivität

Vor dem Austausch von Brücken sollten Sie die Verbindung zu Bridge und Storage überprüfen. Wenn Sie sich die Befehlsausgabe vertraut machen, können Sie die Konnektivität nach Konfigurationsänderungen nachträglich überprüfen.

Sie können diese Befehle von der Admin-Eingabeaufforderung eines der Controller-Module in der MetroCluster-Konfiguration am Standort, der gewartet wird, ausgeben.

1. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:

   ```
   run local sysconfig -v
   ```

In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
```

```
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Hot-Swap FibreBridge 6500N-Brücken, um ein Paar FibreBridge 7600N oder 7500N-Brücken zu bilden

Um eine oder zwei FibreBridge 6500N Hot-Swap durchzuführen, um eine Konfiguration mit zwei FibreBridge 7600N oder 7500N Brücken zu erstellen, müssen Sie die Brücken nacheinander austauschen und den korrekten Kabelvorgang befolgen. Die neue Verkabelung unterscheidet sich von der ursprünglichen Verkabelung.

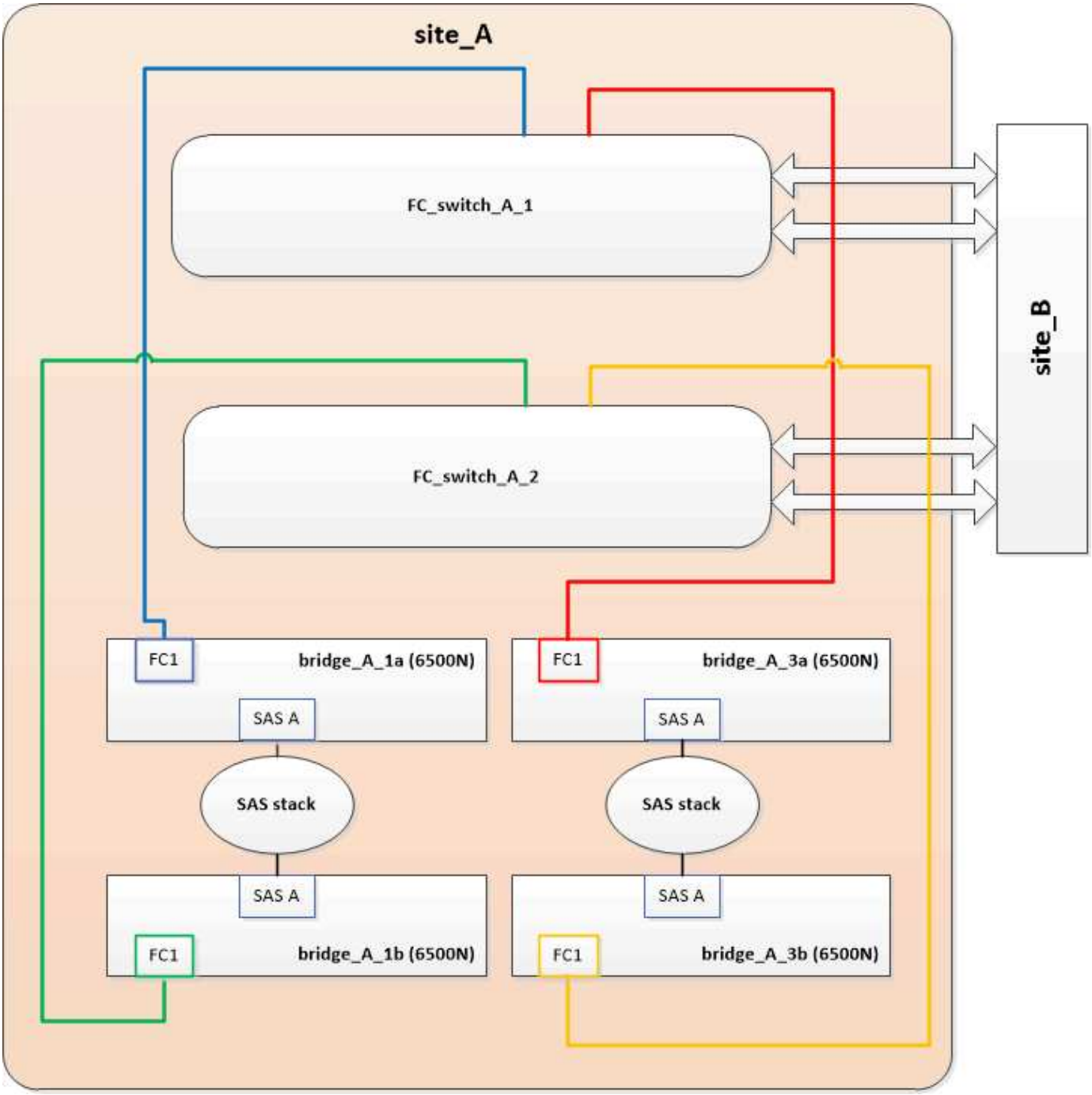
Über diese Aufgabe

Sie können dieses Verfahren auch verwenden, wenn die folgenden Bedingungen erfüllt sind:

- Sie ersetzen ein Paar FibreBridge 6500N-Brücken, die beide mit demselben SAS-Speicher verbunden sind.
- Sie haben zuvor eine FibreBridge 6500N-Brücke im Paar ersetzt, und Ihr Speicherstapel ist mit einer FibreBridge 6500N-Brücke und einer FibreBridge 7600N oder 7500N-Brücke konfiguriert.

  In diesem Fall sollten Sie mit dem folgenden Schritt beginnen, um die untere FibreBridge 6500N-Brücke mit einer FibreBridge 7600N oder 7500N Hot-Swap zu starten.

Das folgende Diagramm zeigt ein Beispiel für die Erstkonfiguration, in der vier FibreBridge 6500N-Brücken zwei SAS-Storage-Stacks verbinden:



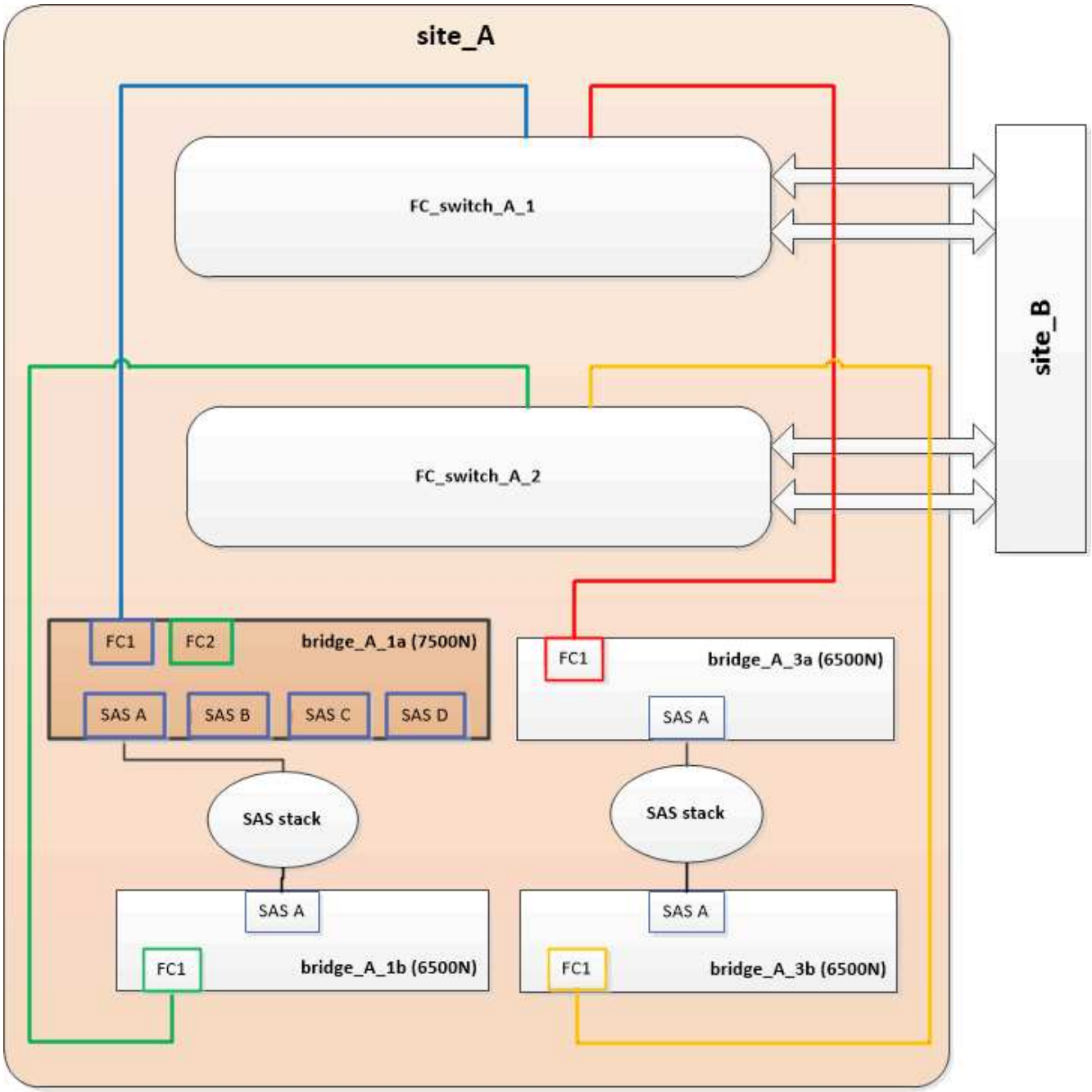
Schritte

1. Gemäß den folgenden Richtlinien tauschen Sie die obere FibreBridge 6500N Bridge unter Verwendung des Verfahrens in mit einer FibreBridge 7600N oder 7500N aus "Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke":

    - Verbinden Sie den Anschluss FibreBridge 7600N oder 7500N Bridge FC1 mit dem Switch oder Controller.

      Dies ist die gleiche Verbindung, die zum Anschluss FibreBridge 6500N Bridge FC1 hergestellt wurde.

    - Schließen Sie den Anschluss FibreBridge 7600N oder 7500N Bridge FC2 derzeit nicht an. Das folgende Diagramm zeigt, dass Bridge_A_1a ersetzt wurde und nun eine FibreBridge 7600N oder 7500N-Brücke ist:



2. Überprüfen Sie die Verbindung zu den mit der Bridge verbundenen Festplatten und die Tatsache, dass die neue FibreBridge 7500N in der Konfiguration sichtbar ist:

```
run local sysconfig -v
```

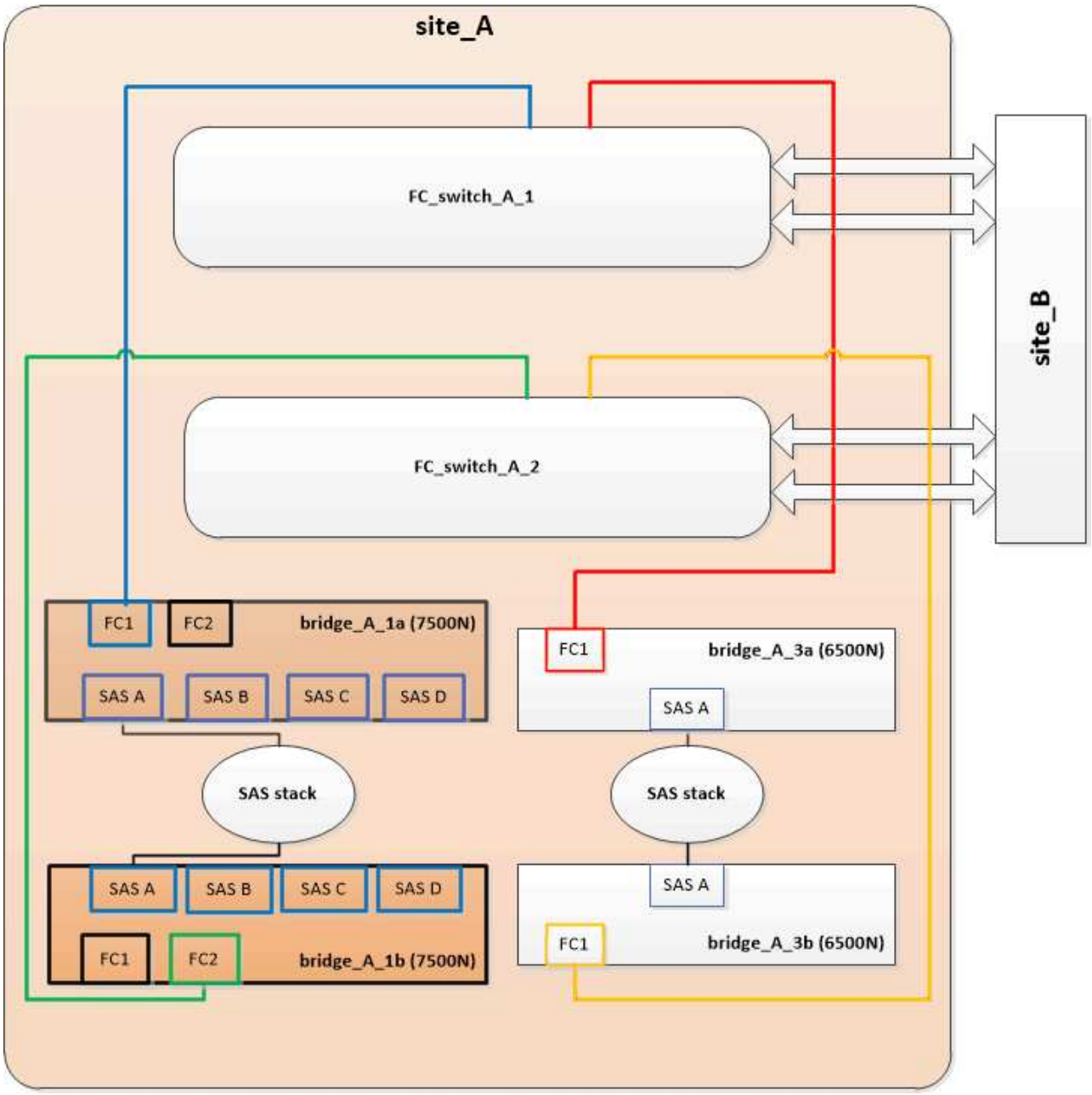
```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
```

```
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104**<===**
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

3. Gemäß den folgenden Richtlinien tauschen Sie die untere FibreBridge 6500N-Brücke mit einer FibreBridge 7600N oder 7500N unter Verwendung des Verfahrens in im laufenden Betrieb aus "Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke":
   - Verbinden Sie den Anschluss FibreBridge 7600N oder 7500N Bridge FC2 mit dem Switch oder Controller.

     Dies ist die gleiche Verbindung, die zum Anschluss FibreBridge 6500N Bridge FC1 hergestellt wurde.

   - Schließen Sie den Anschluss FibreBridge 7600N oder 7500N Bridge FC1 derzeit nicht an.



4. Überprüfen Sie die Verbindung zu den mit der Bridge verbundenen Festplatten:

   ```
   run local sysconfig -v
   ```

   In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
```

```
IOM3 B: 0200
          .
          .
          .
```

Verkabelung der Bridge-SAS-Ports bei Storage-Konsolidierung hinter FibreBridge 7600N- oder 7500N-Bridges

Wenn Sie mehrere SAS Storage Stacks hinter einem einzigen FibreBridge 7600N- oder 7500N-Paar mit verfügbaren SAS-Ports konsolidieren, müssen Sie die oberen und unteren SAS-Kabel auf die neuen Brücken bringen.

Über diese Aufgabe

Die FibreBridge 6500N Bridge SAS-Ports verwenden QSFP-Anschlüsse. Die SAS-Ports FibreBridge 7600N oder 7500N verwenden Mini-SAS-Anschlüsse.

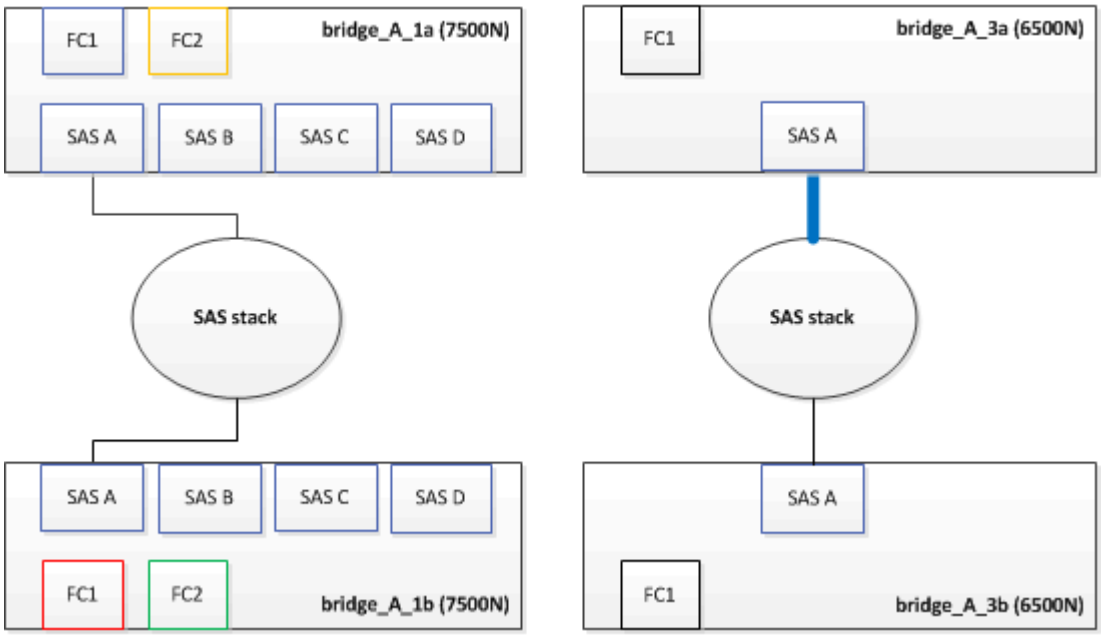
> Wenn Sie ein SAS-Kabel in den falschen Port stecken, müssen Sie das Kabel von einem SAS-Port entfernen und mindestens 120 Sekunden warten, bevor Sie das Kabel an einen anderen SAS-Port anschließen. Wenn Sie dies nicht tun, erkennt das System nicht, dass das Kabel auf einen anderen Port verschoben wurde.

> Warten Sie mindestens 10 Sekunden, bevor Sie den Anschluss anschließen. Die SAS-Kabelanschlüsse sind codiert. Wenn sie sich korrekt in einen SAS-Port orientieren, klicken sie auf ihren Platz und die Festplatten-Shelf-SAS-Port LNK-LED leuchtet grün. Bei Festplatten-Shelfs stecken Sie einen SAS-Kabelanschluss mit nach unten (auf der Unterseite des Connectors) gerichteter Zuglasche.

Schritte

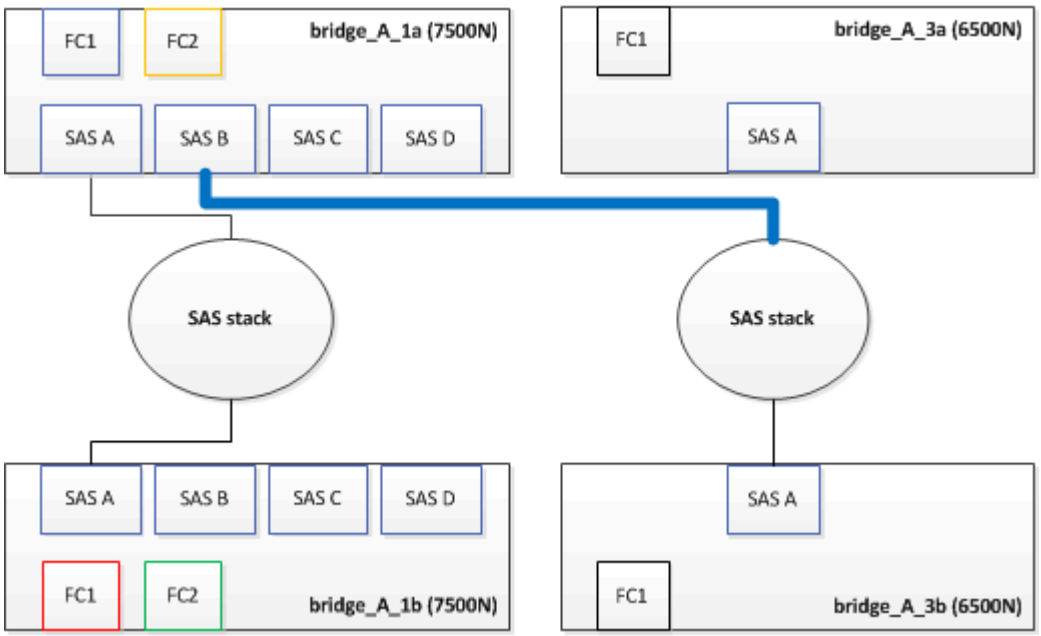
1. Entfernen Sie das Kabel, das den SAS A-Port der oberen FibreBridge 6500N-Bridge mit dem oberen SAS-Shelf verbindet. Achten Sie darauf, den SAS-Port am Storage-Shelf zu notieren, mit dem er verbunden ist.

   Das Kabel wird im folgenden Beispiel blau angezeigt:



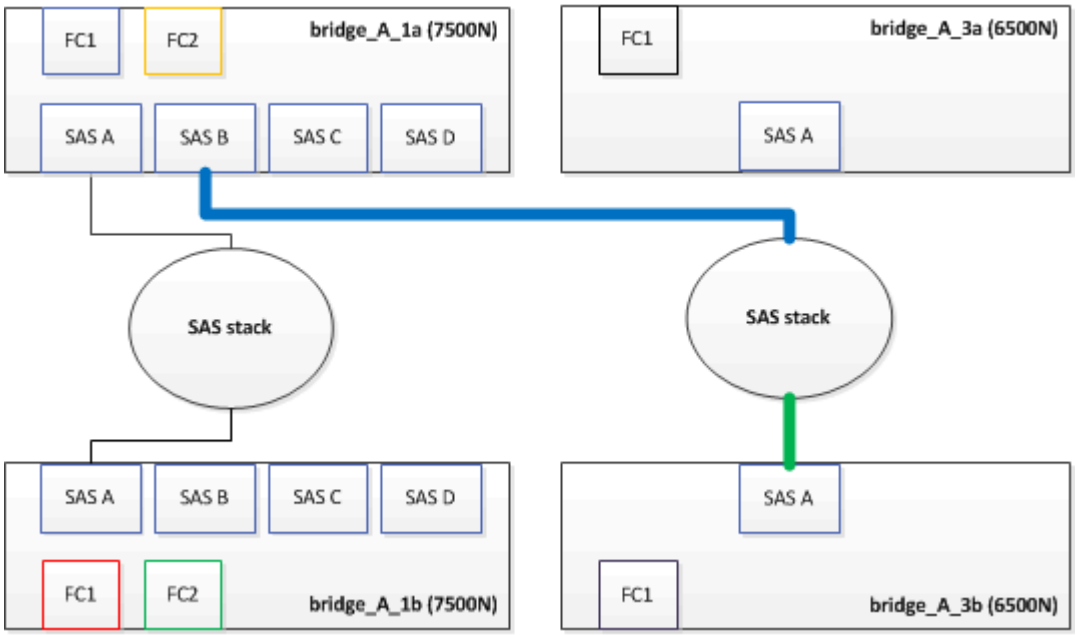
2. Verbinden Sie mithilfe eines Kabels mit einem Mini-SAS-Anschluss denselben SAS-Port am Storage Shelf mit dem SAS B-Port der oberen FibreBridge 7600N oder 7500N-Brücke.

   Das Kabel wird im folgenden Beispiel blau angezeigt:



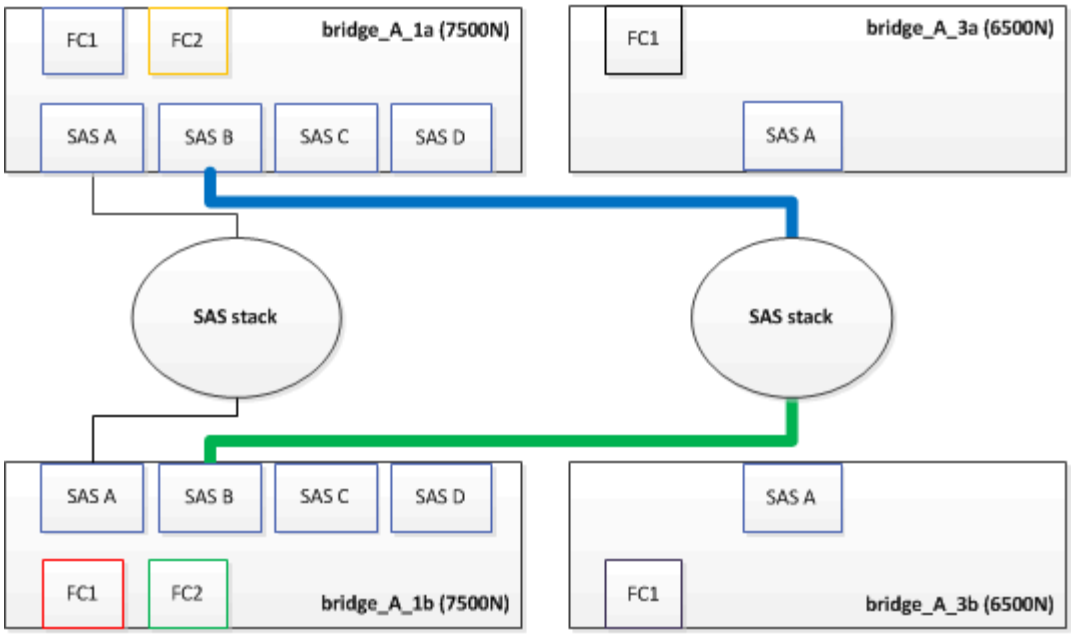
3. Entfernen Sie das Kabel, das den SAS A-Port der unteren FibreBridge 6500N-Bridge mit dem oberen SAS-Shelf verbindet. Achten Sie darauf, den SAS-Port am Storage-Shelf zu notieren, mit dem er verbunden ist.

   Das Kabel wird im folgenden Beispiel grün angezeigt:



4. Verbinden Sie mithilfe eines Kabels mit einem Mini-SAS-Anschluss denselben SAS-Port am Storage Shelf mit dem SAS B-Port der unteren FibreBridge 7600N oder 7500N-Brücke.

   Das Kabel wird im folgenden Beispiel grün angezeigt:



5. Überprüfen Sie die Verbindung zu den mit der Bridge verbundenen Festplatten:

   ```
   run local sysconfig -v
   ```

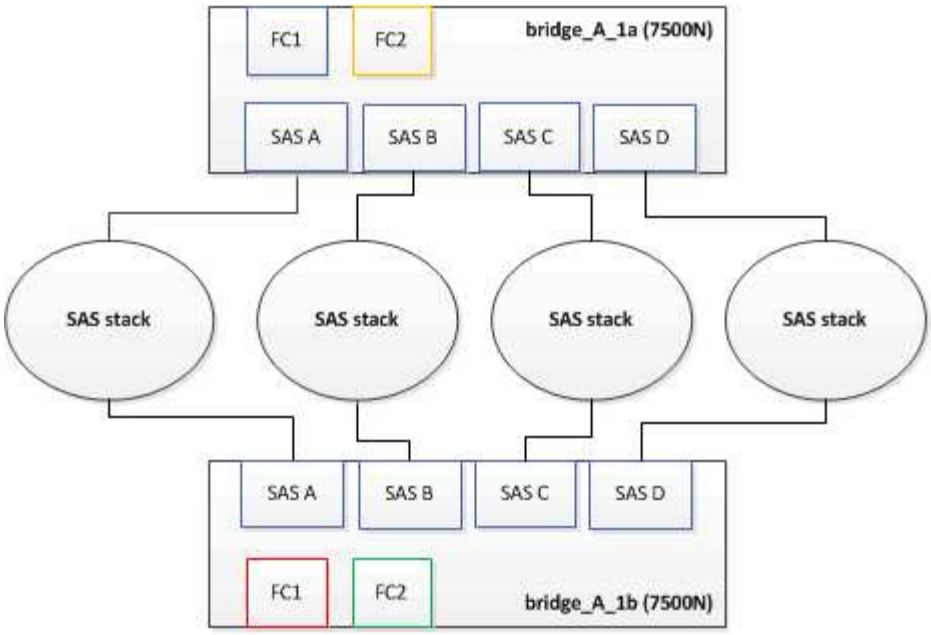
   In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
   System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
   System Serial Number: 940001025465 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   be multi-path HA**
   .
   .
   .
   slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
   Initiator port**
           Firmware rev:      7.5.0
           Flash rev:         0.0.0
           Host Port Id:      0x60100
           FC Node Name:      5:00a:098201:bae312
           FC Port Name:      5:00a:098201:bae312
           SFP Vendor:        FINISAR CORP.
           SFP Part Number:   FTLF8529P3BCVAN1
           SFP Serial Number: URQ0R1R
           SFP Capabilities:  4, 8 or 16 Gbit
           Link Data Rate:    16 Gbit
           Switch Port:       brcd6505-fcs40:1
   ```

```
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

6. Entfernen Sie die alten FibreBridge 6500N-Brücken, die nicht mehr mit dem SAS-Speicher verbunden sind.
7. Warten Sie zwei Minuten, bis das System die Änderungen erkennt.
8. Wenn das System nicht ordnungsgemäß verkabelt war, entfernen Sie das Kabel, korrigieren Sie die Verkabelung und schließen Sie dann das korrekte Kabel wieder an.
9. Wiederholen Sie bei Bedarf die vorherigen Schritte, um bis zu zwei weitere SAS-Stacks hinter den neuen FibreBridge 7600N oder 7500N-Brücken zu bewegen, und zwar mit den SAS-Ports C und dann D.

   Jeder SAS-Stack muss mit demselben SAS-Port an der oberen und unteren Brücke verbunden sein. Wenn zum Beispiel die obere Verbindung des Stacks mit dem oberen Bridge-SAS B-Port verbunden ist, muss die untere Verbindung mit dem SAS B-Port der unteren Brücke verbunden sein.



Zoning wird aktualisiert, wenn eine Konfiguration FibreBridge 7600N oder 7500N-Brücken hinzugefügt wird

Das Zoning muss geändert werden, wenn Sie FibreBridge 6500N-Bridges durch FibreBridge 7600N oder 7500N-Brücken ersetzen und beide FC-Ports auf den FibreBridge 7600N oder 7500N-Bridges verwenden. Die erforderlichen Änderungen hängen davon ab, ob Sie eine ONTAP-Version vor 9.1 oder 9.1 und höher ausführen.

Aktualisieren des Zoning beim Hinzufügen von FibreBridge 7500N-Bridges zu einer Konfiguration (vor ONTAP 9.1)

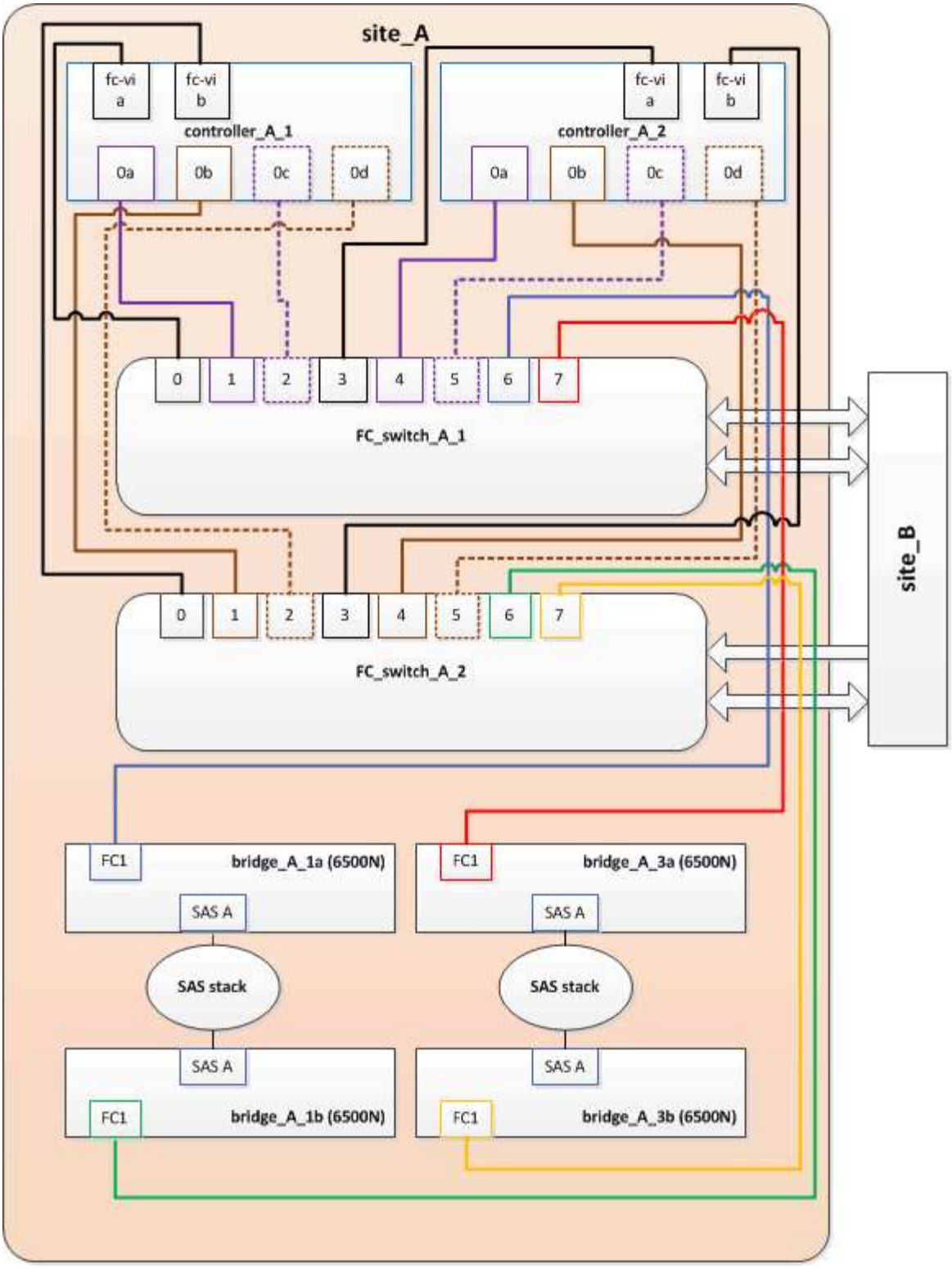
Das Zoning muss geändert werden, wenn Sie FibreBridge 6500N-Brücken durch FibreBridge 7500N-Brücken ersetzen und beide FC-Ports auf den FibreBridge 7500N verwenden. Jede Zone kann nicht mehr als vier Initiator-Ports enthalten. Das Zoning, das Sie verwenden, hängt davon ab, ob Sie ONTAP vor Version 9.1 oder 9.1 und höher ausführen

Über diese Aufgabe

Das spezifische Zoning in dieser Aufgabe gilt für Versionen von ONTAP vor Version 9.1.

Die Änderungen beim Zoning sind erforderlich, um Probleme mit ONTAP zu vermeiden, die erfordern, dass nicht mehr als vier FC-Initiator-Ports einen Pfad zu einer Festplatte haben können. Nach Neuordnung zur Konsolidierung der Shelves würde das vorhandene Zoning dazu führen, dass jede Festplatte über acht FC-Ports erreichbar ist. Sie müssen das Zoning ändern, um die Initiator-Ports in jeder Zone auf vier zu reduzieren.

Das folgende Diagramm zeigt das Zoning vor den Änderungen an Site_A:



Schritte

1. Aktualisieren Sie die Speicherzonen für die FC-Switches, indem Sie die Hälfte der Initiator-Ports aus jeder vorhandenen Zone entfernen und neue Zonen für die FibreBridge 7500N FC2-Ports erstellen.

   Die Zonen für die neuen FC2-Ports enthalten die Initiator-Ports, die aus den vorhandenen Zonen entfernt wurden. In den Diagrammen werden diese Zonen mit gestrichelten Linien dargestellt.

   Informationen zu den Zoning-Befehlen finden Sie in den FC-Switch-Abschnitten des "Installation und Konfiguration von Fabric-Attached MetroCluster" Oder "Installation und Konfiguration von Stretch

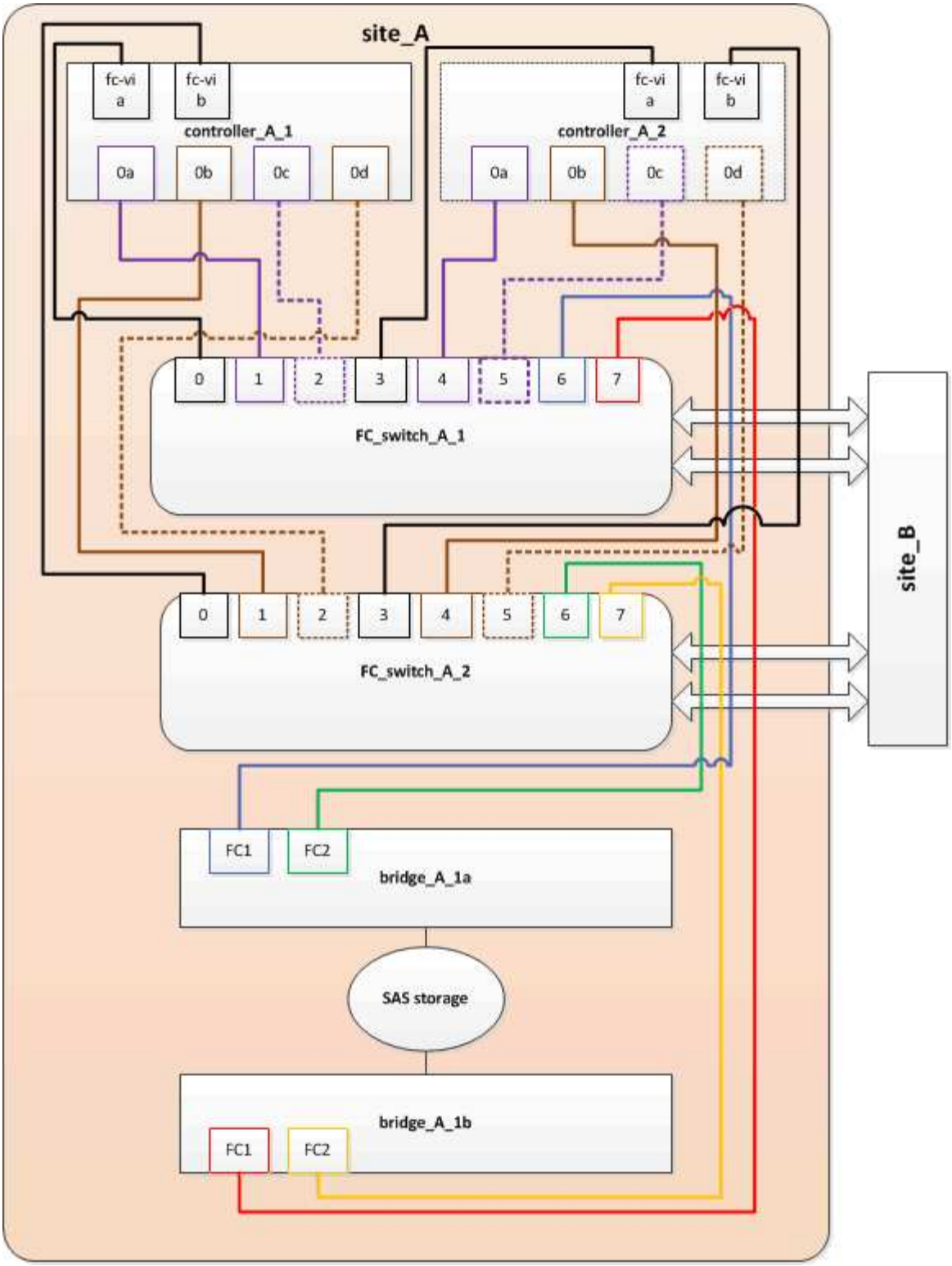
MetroCluster".

Die folgenden Beispiele zeigen die Storage-Zonen und die Ports in jeder Zone vor und nach der Konsolidierung. Die Ports werden durch *Domain, Port*-Paare identifiziert.

- Domäne 5 besteht aus Switch FC_Switch_A_1.
- Domäne 6 besteht aus Switch FC_Switch_A_2.
- Domäne 7 besteht aus Switch FC_Switch_B_1.
- Domäne 8 besteht aus Switch FC_Switch_B_2.

Vor oder nach der Konsolidierung	Zone	Domänen und Ports	Farben in Diagrammen (die Diagramme zeigen nur Standort A an)
Zonen vor der Konsolidierung. An den vier FibreBridge 6500N-Brücken gibt es für jeden FC-Port eine Zone.	STOR_A_1A-FC1	5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,6	Lila + gestrichelt lila + blau
STOR_A_1B-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,6	Braun + gestrichelt braun + grün	STOR_A_2A-FC1
5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,7	Violett + gestrichelt lila + rot	STOR_A_2B-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,7
Braun + gestrichelt braun + orange	Zonen nach der Konsolidierung. An den beiden FibreBridge 7500N-Brücken gibt es eine Zone für jeden FC-Port.	STOR_A_1A-FC1	7,1; 7,4; 5,1; 5,4; 5,6
Violett + blau	STOR_A_1B-FC1	7,2; 7,5; 5,2; 5,5; 5,7	Violett + rot gestrichelt
STOR_A_1A-FC2	8,1; 8,4; 6,1; 6,4; 6,6	Braun + grün	STOR_A_1B-FC2

Das folgende Diagramm zeigt das Zoning von Site_A nach der Konsolidierung:



Aktualisieren des Zoning beim Hinzufügen von FibreBridge 7600N oder 7500N-Bridges zu einer Konfiguration (ONTAP 9.1 und höher)

Das Zoning muss geändert werden, wenn Sie FibreBridge 6500N-Bridges durch FibreBridge 7600N oder 7500N-Brücken ersetzen und beide FC-Ports auf den FibreBridge 7600N oder 7500N-Bridges verwenden. Jede Zone kann nicht mehr als vier Initiator-Ports enthalten.

Über diese Aufgabe

- Diese Aufgabe gilt für ONTAP 9.1 und höher.
- FibreBridge 7600N-Brücken werden in ONTAP 9.6 und höher unterstützt.
- Das spezifische Zoning in dieser Aufgabe gilt für ONTAP 9.1 und höher.
- Die Änderungen beim Zoning sind erforderlich, um Probleme mit ONTAP zu vermeiden, die erfordern, dass nicht mehr als vier FC-Initiator-Ports einen Pfad zu einer Festplatte haben können.

  Nach Neuordnung zur Konsolidierung der Shelves würde das vorhandene Zoning dazu führen, dass jede Festplatte über acht FC-Ports erreichbar ist. Sie müssen das Zoning ändern, um die Initiator-Ports in jeder Zone auf vier zu reduzieren.

Schritt

1. Aktualisieren Sie die Speicherzonen für die FC-Switches, indem Sie die Hälfte der Initiator-Ports aus jeder vorhandenen Zone entfernen und neue Zonen für die FibreBridge 7600N- oder 7500N-FC2-Ports erstellen.

   Die Zonen für die neuen FC2-Ports enthalten die Initiator-Ports, die aus den vorhandenen Zonen entfernt wurden.

   Informationen finden Sie im Abschnitt zum FC-Switch von "Installation und Konfiguration von Fabric-Attached MetroCluster" Weitere Informationen zu den Zoning-Befehlen.

Verkabelung des zweiten Bridge-FC-Ports beim Hinzufügen von FibreBridge 7600N- oder 7500N-Bridges zu einer Konfiguration

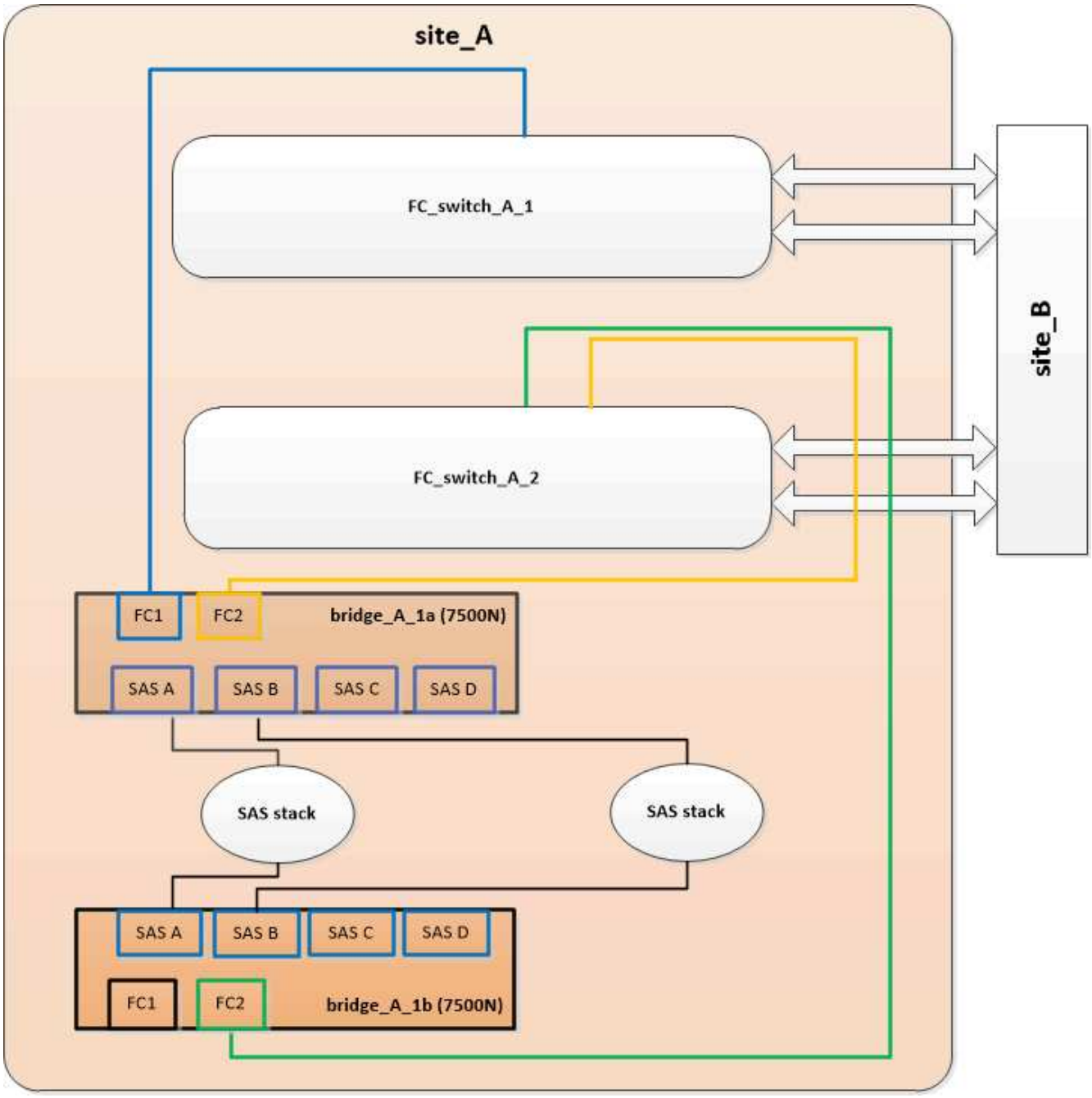
Um mehrere Pfade zu den Speicherstapeln bereitzustellen, können Sie den zweiten FC-Port an jeder FibreBridge 7600N oder 7500N-Brücke verkabeln, wenn Sie der Konfiguration die FibreBridge 7600N oder 7500N-Brücke hinzugefügt haben.

Bevor Sie beginnen

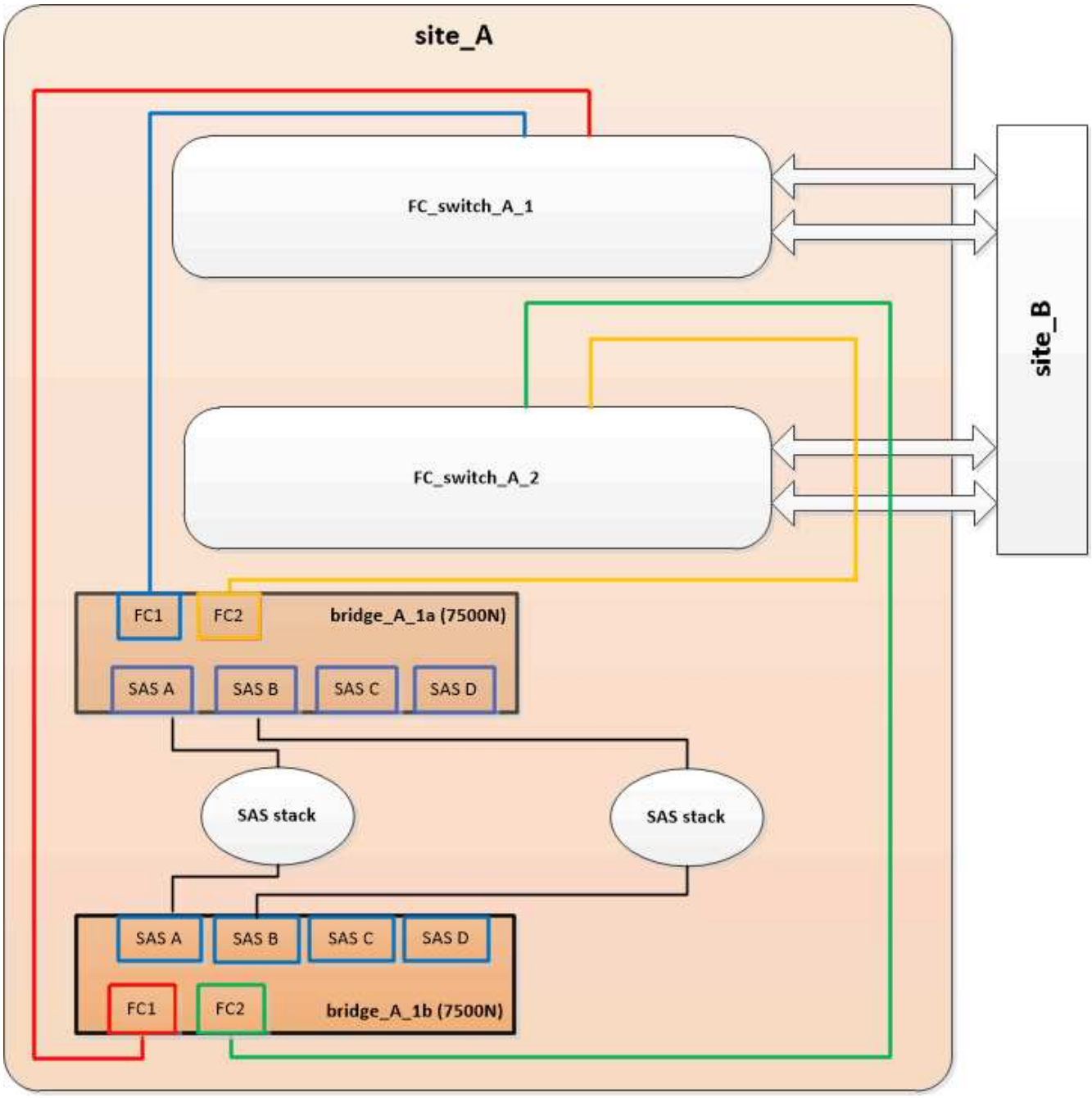
Das Zoning muss angepasst werden, um Zonen für die zweiten FC-Ports bereitzustellen.

Schritte

1. Schließen Sie den FC2-Port der oberen Brücke an den richtigen Port an FC_Switch_A_2 an.



2. Schließen Sie den FC1-Port der unteren Brücke an den richtigen Port an FC_Switch_A_1 an.



3. Überprüfen Sie die Verbindung zu den mit der Bridge verbundenen Festplatten:

   ```
   run local sysconfig -v
   ```

   In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
   System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
   System Serial Number: 940001025465 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   ```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Deaktivieren nicht verwendeter SAS-Ports an den FC-to-SAS-Bridges

Nachdem Sie die Verkabelung geändert haben, sollten Sie alle nicht verwendeten SAS-Ports in den FC-zu-SAS-Bridges deaktivieren, um Warnmeldungen zur Systemzustandsüberwachung zu den nicht verwendeten Ports zu vermeiden.

Schritte

1. Nicht genutzte SAS-Ports auf der oberen FC-to-SAS-Bridge deaktivieren:

   a. Melden Sie sich bei der Bridge-CLI an.

   b. Deaktivieren Sie alle nicht verwendeten Ports.

   > Wenn Sie eine ATTO 7500N-Bridge konfiguriert haben, sind standardmäßig alle SAS-Ports (A bis D) aktiviert, und Sie müssen die nicht verwendeten SAS-Ports deaktivieren:
   >
   > `SASPortDisable` *`sas port`*

   Wenn SAS-Ports A und B verwendet werden, müssen die SAS-Ports C und D deaktiviert werden. Im folgenden Beispiel sind die nicht verwendeten SAS-Ports C und D deaktiviert:

   ```
   Ready. *
   SASPortDisable C

   SAS Port C has been disabled.

   Ready. *
   SASPortDisable D

   SAS Port D has been disabled.

   Ready. *
   ```

   c. Bridge-Konfiguration speichern:
   `SaveConfiguration`

   Im folgenden Beispiel wird gezeigt, dass die SAS-Ports C und D deaktiviert wurden. Beachten Sie, dass das Sternchen nicht mehr angezeigt wird, was darauf hinweist, dass die Konfiguration gespeichert wurde.

   ```
   Ready. *
   SaveConfiguration

   Ready.
   ```

2. Wiederholen Sie den vorherigen Schritt auf der unteren FC-zu-SAS-Brücke.

Anforderungen für die Verwendung anderer Schnittstellen zur Konfiguration und Verwaltung von FibreBridge-Brücken

Sie können die Kombination aus seriellem Port, Telnet und FTP verwenden, um die FibreBridge-Brücken anstelle der empfohlenen Verwaltungsschnittstellen zu verwalten. Das System muss die Anforderungen für die jeweilige Schnittstelle erfüllen, bevor Sie die Brücken installieren.

Sie können einen seriellen Port oder Telnet verwenden, um die Bridge- und Ethernet-Management-1-Ports zu konfigurieren und die Bridge zu verwalten. Sie können FTP verwenden, um die Bridge-Firmware zu aktualisieren.

> Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihre Modellbrücke enthält weitere Informationen zu Management-Schnittstellen.

Sie können auf dieses Dokument auf der ATTO-Website zugreifen, indem Sie den Link auf der ATTO FibreBridge-Beschreibungsseite verwenden.

Serieller Port

Bei der Verwendung des seriellen Ports zur Konfiguration und Verwaltung einer Bridge und zur Konfiguration des Ethernet Management 1-Ports muss das System die folgenden Anforderungen erfüllen:

- Ein serielles Kabel (das vom seriellen Bridge-Port an einen seriellen COM-Port (serieller Anschluss) des Computers, den Sie für die Einrichtung verwenden, angeschlossen wird)

  Der serielle Bridge-Port ist RJ-45 und verfügt über die gleiche Anschlussbuchse wie die Controller.

- Ein Terminalemulationsprogramm wie Hyperterminal, Teraterm oder PuTTY zum Zugriff auf die Konsole

  Das Terminalprogramm sollte in der Lage sein, Bildschirmausgabe in eine Datei zu protokollieren.

Telnet

Wenn Sie Telnet verwenden, um eine Bridge zu konfigurieren und zu verwalten, muss Ihr System die folgenden Anforderungen erfüllen:

- Ein serielles Kabel (das vom seriellen Bridge-Port an einen seriellen COM-Port (serieller Anschluss) des Computers, den Sie für die Einrichtung verwenden, angeschlossen wird)

  Der serielle Bridge-Port ist RJ-45 und verfügt über die gleiche Anschlussbuchse wie die Controller.

- (Empfohlen) Ein nicht standardmäßiger Benutzername und ein Kennwort (für den Zugriff auf die Bridge)
- Ein Terminalemulationsprogramm wie Hyperterminal, Teraterm oder PuTTY zum Zugriff auf die Konsole

  Das Terminalprogramm sollte in der Lage sein, Bildschirmausgabe in eine Datei zu protokollieren.

- Eine IP-Adresse, eine Subnetzmaske und Gateway-Informationen für den Ethernet-Management-1-Port auf jeder Bridge

FTP

Wenn Sie FTP verwenden, um die Bridge-Firmware zu aktualisieren, muss Ihr System die folgenden

Anforderungen erfüllen:

- Ein Standard-Ethernet-Kabel (das über den Bridge Ethernet Management 1-Port mit Ihrem Netzwerk verbunden wird)
- (Empfohlen) Ein nicht standardmäßiger Benutzername und ein Kennwort (für den Zugriff auf die Bridge)

Hot-Ersetzen eines fehlerhaften Netzteilmoduls

Wenn sich der Status eines Netzteilmoduls auf die Bridge ändert, können Sie das Netzteilmodul entfernen und installieren.

Sie können den Status eines Netzteilmoduls über die LEDs auf der Bridge anzeigen. Sie können den Status der Stromversorgungsmodule auch über die ExpressNAV GUI und die Bridge-CLI, über serielle Schnittstelle oder per Telnet anzeigen.

- Dieser Vorgang läuft unterbrechungsfrei (unterbrechungsfrei) und dauert etwa 15 Minuten.
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

> Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihre Modellbrücke enthält weitere Informationen zu Management-Schnittstellen.

Sie können auf diesen und andere Inhalte auf der ATTO-Website zugreifen, indem Sie den Link auf der ATTO FibreBridge-Beschreibungsseite verwenden.

In-Band-Management der FC-to-SAS-Bridges

Ab ONTAP 9.5 mit FibreBridge 7500N oder 7600N Bridges wird das in-Band-Management der Brücken als Alternative zum IP-Management der Brücken unterstützt. Ab ONTAP 9.8 ist das Out-of-Band-Management veraltet.

> **Über diese Aufgabe**
>
> 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.

Bei Verwendung der in-Band-Verwaltung können die Brücken über die FC-Verbindung zur Bridge von der ONTAP-CLI verwaltet und überwacht werden. Der physische Zugriff auf die Bridge über die Bridge-Ethernet-Ports ist nicht erforderlich, wodurch die Sicherheitslücke der Bridge verringert wird.

Die Verfügbarkeit der in-Band-Verwaltung der Brücken hängt von der Version von ONTAP ab:

- Ab ONTAP 9.8 werden Brücken standardmäßig über in-Band-Verbindungen verwaltet und die Out-of-Band-Verwaltung der Brücken über SNMP ist veraltet.
- ONTAP 9.5 bis 9.7: Entweder in-Band-Management oder Out-of-Band-SNMP-Management wird unterstützt.
- Vor ONTAP 9.5 wird nur bandexterne SNMP-Verwaltung unterstützt.

Bridge-CLI-Befehle können über die ONTAP-Schnittstelle ausgegeben werden `storage bridge run-cli -name` *`bridge-name`* `-command` *`bridge-command-name`* Befehl über die ONTAP-Schnittstelle.

Die Verwendung von in-Band-Management mit deaktiviertem IP-Zugriff wird empfohlen, um die Sicherheit durch Beschränkung der physischen Konnektivität der Bridge zu verbessern.

Verwandte Informationen

"Hot-Swap-durchführen einer Bridge mit einer Ersatzbrücke desselben Modells"

"Hot-Swap einer FibreBridge 7500N mit einer 7600N-Brücke"

"Hot-Swap einer FibreBridge 6500N-Bridge mit FibreBridge 7600N oder 7500N-Brücke"

"Hot-Adding eines Stacks mit SAS-Platten-Shelfs und Bridges"

Verwalten einer FibreBridge-Brücke von ONTAP aus

Ab ONTAP 9.5 können Sie die ONTAP-CLI verwenden, um FibreBridge-Befehle an die Bridge zu übergeben und die Ergebnisse dieser Befehle anzuzeigen.

Über diese Aufgabe

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. Führen Sie den entsprechenden FiberBridge-Befehl im aus `storage bridge run-cli` Befehl:

   `storage bridge run-cli -name` *`bridge-name`* `-command` *`"command-text"`*

   Mit dem folgenden Befehl wird die FibreBridge ausgeführt `SASPortDisable` Befehl von der ONTAP-Eingabeaufforderung zum Deaktivieren von SAS-Port b auf der Bridge:

   ```
   cluster_A::> storage bridge run-cli -name "SASPortDisable b"

   SAS Port B has been disabled.
   Ready
   cluster_A::>
   ```

Sichern oder Entricken der FibreBridge-Brücke

Um potenziell unsichere Ethernet-Protokolle auf einer Bridge einfach zu deaktivieren, können Sie ab ONTAP 9.5 die Bridge sichern. Dadurch werden die Ethernet-Ports der Bridge deaktiviert. Sie können auch den Ethernet-Zugriff erneut aktivieren.

- Durch das Sichern der Brücke werden Telnet und andere IP-Port-Protokolle und -Dienste (FTP, ExpressNAV, ICMP oder Quicknav) auf der Brücke deaktiviert.
- Bei diesem Verfahren wird die Out-of-Band-Verwaltung mithilfe der ONTAP-Eingabeaufforderung verwendet, die ab ONTAP 9.5 verfügbar ist.

  Sie können die Befehle aus der Bridge-CLI ausgeben, wenn Sie keine Out-of-Band-Verwaltung

verwenden.

- Der **`unsecurebridge`** Mit dem Befehl können die Ethernet-Ports erneut aktiviert werden.
- In ONTAP 9.7 und früher, Ausführen der **`securebridge`** Durch den Befehl auf der ATTO FibreBridge wird der Bridge-Status auf dem Partner-Cluster möglicherweise nicht korrekt aktualisiert. Führen Sie in diesem Fall den aus **`securebridge`** Befehl aus dem Partner-Cluster.

> 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. Sichern Sie die Bridge an der ONTAP-Eingabeaufforderung des Clusters mit der Bridge oder unsichern Sie sie.

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   securebridge
   ```

   Mit dem folgenden Befehl wird Bridge_A_1 aufgehoben:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   unsecurebridge
   ```

2. Speichern Sie in der ONTAP-Eingabeaufforderung des Clusters, der die Bridge enthält, die Bridge-Konfiguration:

   `storage bridge run-cli -bridge *bridge-name* -command saveconfiguration`

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. Starten Sie an der ONTAP-Eingabeaufforderung des Clusters, das die Bridge enthält, die Firmware der Bridge neu:

   `storage bridge run-cli -bridge *bridge-name* -command firmwarerestart`

   Mit dem folgenden Befehl wird Bridge_A_1 gesichert:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   firmwarerestart
   ```

Wartung und Austausch von FC-Switches

Upgrade oder Downgrade der Firmware auf einem Brocade FC-Switch

Zum Upgrade oder Downgrade der Firmware auf einem Brocade FC-Switch müssen Sie den Switch mit den spezifischen Brocade Befehlen deaktivieren, die Firmware-Änderung durchführen und überprüfen sowie den Switch neu starten und wieder aktivieren.

Über diese Aufgabe

Vergewissern Sie sich, dass Sie die folgenden Aufgaben für Ihre Konfiguration überprüft und ausgeführt haben:

- Sie haben die Firmware-Dateien.
- Das System ist ordnungsgemäß verkabelt.
- Es sind alle Pfade zu den Storage Shelfs verfügbar.
- Die Platten-Shelf Stacks sind stabil.
- Die FC-Switch-Fabric ist in einem ordnungsgemäßen Zustand.
- Im System sind keine fehlerhaften Komponenten vorhanden.
- Das System funktioniert normal.
- Sie haben das Admin-Passwort und Zugriff auf einen FTP- oder SCP-Server.
- Die Konsolenprotokollierung ist aktiviert.

  "Aktivieren Sie die Konsolenprotokollierung"

Die Switch-Fabric wird während eines Firmware-Upgrades oder Downgrades deaktiviert, wobei die MetroCluster-Konfiguration den Betrieb über die zweite Fabric fortsetzt.

Ab Fabric OS 9.0 wird SNMPv2 auf Brocade-Switches nicht unterstützt. Wenn Sie ein Upgrade auf Fabric OS 9.0.1 oder höher durchführen, müssen Sie SNMPv3 für die Statusüberwachung verwenden. Weitere Informationen finden Sie unter "Konfigurieren von SNMPv3 in einer MetroCluster-Konfiguration".

Wenn Sie ein Upgrade auf Fabric OS V 9.2.x oder höher durchführen, müssen Sie ein Brocade TruFOS-Zertifikat installiert haben. Weitere Informationen finden Sie unter"Upgrade-Handbuch für Brocade Fabric OS Software, 9.2.x".

Diese Aufgabe muss nacheinander an jeder Switch-Fabric ausgeführt werden, damit alle Switches dieselbe Firmware-Version ausführen.

> Dieser Vorgang läuft unterbrechungsfrei ab und dauert etwa eine Stunde.

Schritte

1. Melden Sie sich bei jedem der Switches in der Fabric an.

   Die Beispiele in den folgenden Schritten verwenden den Schalter `FC_switch_A_1`.

2. Deaktivieren Sie jeden der Switches in der Fabric:

   `switchCfgPersistentDisable`

Wenn dieser Befehl nicht verfügbar ist, führen Sie den aus `switchDisable` Befehl.

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

3. Laden Sie die gewünschte Firmware-Version herunter:

   `firmwareDownload`

   Wenn Sie zur Eingabe des Dateinamens aufgefordert werden, müssen Sie das Unterverzeichnis oder den relativen Pfad zur Firmware-Datei angeben.

   Sie können die ausführen `firmwareDownload` Befehl gleichzeitig auf beiden Switches, aber Sie müssen der Firmware das Herunterladen und Commit ermöglichen, bevor Sie mit dem nächsten Schritt fortfahren.

```
FC_switch_A_1:admin> firmwaredownload
Server Name or IP Address: 10.64.203.188
User Name: test
File Name: v7.3.1b
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP, 5-HTTP) [1]: 2
Password:
Server IP: 10.64.203.188, Protocol IPv4
Checking system settings for firmwaredownload...
System settings check passed.
```

4. Vergewissern Sie sich, dass die Firmware heruntergeladen und auf beiden Partitionen gesetzt wurde:

   `firmwareShow`

   Das folgende Beispiel zeigt, dass der Firmware-Download abgeschlossen ist, wenn beide Bilder aktualisiert werden:

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. Starten Sie die Switches neu:

   `reboot`

   Nach Abschluss des Firmware-Downloads führen einige Firmware-Versionen automatisch einen haReboot-Vorgang durch. Der Neustart in diesem Schritt ist auch dann erforderlich, wenn der haReboot durchgeführt wurde.

```
FC_switch_A_1:admin> reboot
```

6. Prüfen Sie, ob die neue Firmware auf eine mittlere Firmware-Ebene oder auf eine endgültige angegebene Version gehört.

   Wenn der Download auf die mittlere Firmware-Ebene erfolgt, führen Sie die beiden vorherigen Schritte aus, bis das angegebene Release installiert ist.

7. Aktivieren Sie die Switches:

   `switchCfgPersistentEnable`

   Wenn dieser Befehl nicht verfügbar ist, sollte sich der Schalter im befinden `enabled` Status nach dem `reboot` Befehl wird ausgeführt.

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. Vergewissern Sie sich, dass die Switches online sind und alle Geräte ordnungsgemäß angemeldet sind:

   `switchShow`

```
FC_switch_A_1:admin> switchShow
```

9. Stellen Sie sicher, dass die Informationen zur Puffernutzung für eine Portgruppe oder alle Portgruppen im Switch ordnungsgemäß angezeigt werden:

   `portbuffershow`

```
FC_switch_A_1:admin> portbuffershow
```

10. Überprüfen Sie, ob die aktuelle Konfiguration eines Ports ordnungsgemäß angezeigt wird:

    `portcfgshow`

```
FC_switch_A_1:admin> portcfgshow
```

    Überprüfen Sie die Porteinstellungen, z. B. Geschwindigkeit, Modus, Trunking, Verschlüsselung, Und Komprimierung in der Inter-Switch Link-Ausgabe (ISL). Vergewissern Sie sich, dass die Porteinstellungen vom Firmware-Download nicht betroffen waren.

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

    a. Überprüfen Sie, ob das System multipathed ist:
       `node run -node node-name sysconfig -a`

    b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:

```
system health alert show
```

c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
```
metrocluster show
```

d. Führen Sie eine MetroCluster-Prüfung durch:
```
metrocluster check run
```

e. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
```
metrocluster check show
```

f. Überprüfen Sie, ob auf den Switches Zustandswarnmeldungen angezeigt werden (falls vorhanden):
```
storage switch show
```

g. Nutzen Sie Config Advisor.

   "NetApp Downloads: Config Advisor"

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

12. Warten Sie 15 Minuten, bevor Sie diesen Vorgang für das zweite Switch-Fabric wiederholen.

Upgrade oder Downgrade der Firmware auf einem Cisco FC Switch

Zum Upgrade oder Downgrade der Firmware auf einem Cisco FC-Switch müssen Sie den Switch mit den Cisco-spezifischen Befehlen deaktivieren, das Upgrade durchführen und überprüfen sowie den Switch neu starten und wieder aktivieren.

Über diese Aufgabe

Vergewissern Sie sich, dass Sie die folgenden Aufgaben für Ihre Konfiguration überprüft und ausgeführt haben:

- Das System ist ordnungsgemäß verkabelt.
- Es sind alle Pfade zu den Storage Shelfs verfügbar.
- Die Platten-Shelf Stacks sind stabil.
- Die FC-Switch-Fabric ist in einem ordnungsgemäßen Zustand.
- Alle Komponenten im System sind in gutem Zustand.
- Das System funktioniert normal.
- Sie haben das Admin-Passwort und Zugriff auf einen FTP- oder SCP-Server.
- Die Konsolenprotokollierung ist aktiviert.

  "Aktivieren Sie die Konsolenprotokollierung"

Die Switch-Fabric wird während des Firmware-Upgrades oder Downgrades deaktiviert und die MetroCluster-Konfiguration basiert auf der zweiten Fabric, um den Betrieb fortzusetzen.

Sie müssen diese Aufgabe nacheinander an jeder Switch-Fabric wiederholen, um sicherzustellen, dass alle Switches dieselbe Firmware-Version verwenden.

Sie müssen über die Firmware-Dateien verfügen.

Dieser Vorgang läuft unterbrechungsfrei ab und dauert etwa eine Stunde.

Schritte

1. Melden Sie sich bei jedem der Switches in der Fabric an.

   In den Beispielen werden die Switches FC_Switch_A_1 und FC_Switch_B_1 genannt.

2. Bestimmen Sie, ob auf jedem Switch genügend Speicherplatz im Bootflash-Verzeichnis vorhanden ist:

   `dir bootflash`

   Wenn dies nicht der Fall ist, löschen Sie die unerwünschten Firmware-Dateien mithilfe des `delete bootflash:file_name` Befehl.

3. Kopieren Sie die Kickstart- und Systemdateien auf die Switches:

   `copy` *`source_filetarget_file`*

   Im folgenden Beispiel die Kickstart-Datei (`m9200-s2ek9-kickstart-mz.5.2.1.bin`) Und die Systemdatei (`m9200-s2ek9-mz.5.2.1.bin`) Befinden sich auf dem FTP-Server 10.10.10.55 in der `/firmware/` Pfad:

   Im folgenden Beispiel werden die Befehle angezeigt, die für FC_Switch_A_1 ausgegeben wurden:

   ```
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-
   mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
   FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin
   bootflash:m9200-s2ek9-mz.5.2.1.bin
   ```

4. Deaktivieren Sie alle VSANs auf beiden Switches in dieser Fabric.

   Gehen Sie folgendermaßen vor, um die VSANs zu deaktivieren:

   a. Öffnen Sie das Konfigurations-Terminal:

      `config t`

   b. Geben Sie Ein: **`vsan database`**

   c. Überprüfen Sie den Status der VSANs:

      `show vsan`

      Alle VSANs müssen aktiv sein.

   d. Unterbrechen Sie die VSANs:

      `vsan` *`vsan-num`* `suspend`

      Beispiel: `vsan 10 suspend`

e. Überprüfen Sie den Status der VSANs erneut:

   show vsan+ Alle VSANs müssen ausgesetzt werden.

f. Beenden Sie das config-Terminal:

   end

g. Speichern Sie die Konfiguration.

   copy running-config startup-config

   Im folgenden Beispiel wird die Ausgabe für FC_Switch_A_1 angezeigt:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

```
vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# vsan 1 suspend
FC_switch_A_1(config-vsan-db)# vsan 30 suspend
FC_switch_A_1(config-vsan-db)# vsan 40 suspend
FC_switch_A_1(config-vsan-db)# vsan 70 suspend
FC_switch_A_1(config-vsan-db)# vsan 80 suspend
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
FC_switch_A_1# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan
```

5. Installieren Sie die gewünschte Firmware auf den Switches:

   install all system bootflash:*systemfile_name* kickstart bootflash:*kickstartfile_name*

   Im folgenden Beispiel werden die Befehle angezeigt, die für FC_Switch_A_1 ausgegeben wurden:

   ```
   FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin
   kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
   Enter Yes to confirm the installation.
   ```

6. Überprüfen Sie die Firmware-Version auf jedem Switch, um sicherzustellen, dass die richtige Version installiert ist:

   show version

7. Aktivieren Sie alle VSANs auf beiden Switches in dieser Fabric.

   Gehen Sie folgendermaßen vor, um die VSANs zu aktivieren:

   a. Öffnen Sie das Konfigurations-Terminal:

      config t

   b. Geben Sie Ein: **vsan database**

   c. Überprüfen Sie den Status der VSANs:

      show vsan

      Die VSANs müssen ausgesetzt werden.

   d. VSANs aktivieren:

      no vsan *vsan-num* suspend

      Beispiel: `no vsan 10 suspend`

   e. Überprüfen Sie den Status der VSANs erneut:

      show vsan

      Alle VSANs müssen aktiv sein.

   f. Beenden Sie das config-Terminal:

      end

   g. Konfiguration speichern:

      copy running-config startup-config

      Im folgenden Beispiel wird die Ausgabe für FC_Switch_A_1 angezeigt:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# no vsan 1 suspend
FC_switch_A_1(config-vsan-db)# no vsan 30 suspend
FC_switch_A_1(config-vsan-db)# no vsan 40 suspend
FC_switch_A_1(config-vsan-db)# no vsan 70 suspend
FC_switch_A_1(config-vsan-db)# no vsan 80 suspend
FC_switch_A_1(config-vsan-db)#
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
```

```
        name:VSAN0001  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:up

vsan 30 information
        name:MC1_FCVI_2_30  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id
        operational state:up

vsan 40 information
        name:MC1_STOR_2_40  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:up

vsan 70 information
        name:MC2_FCVI_2_70  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id
        operational state:up

vsan 80 information
        name:MC2_STOR_2_80  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
```

8. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      node run -node *node-name* sysconfig -a

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      system health alert show

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

d. Durchführen einer MetroCluster-Prüfung:

```
metrocluster check run
```

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

9. Wiederholen Sie diesen Vorgang für die zweite Switch-Struktur.

Upgrade auf neue Brocade FC-Switches

Bei einem Upgrade auf neue Brocade FC-Switches müssen Sie die Switches in der ersten Fabric ersetzen, die MetroCluster-Konfiguration vollständig funktionsfähig sein und die Switches in der zweiten Fabric ersetzen.

- Die MetroCluster-Konfiguration muss sich in einem ordnungsgemäßen Zustand und im normalen Betrieb befindet.
- Die MetroCluster Switch Fabrics bestehen aus vier Brocade Switches.

  Die Abbildungen in den folgenden Schritten zeigen aktuelle Schalter.

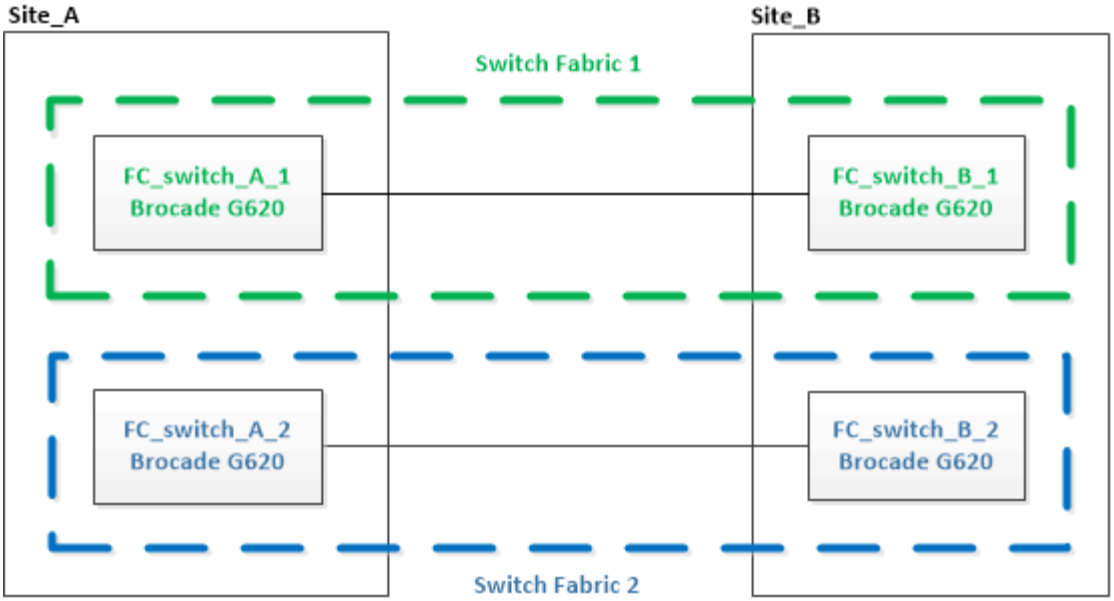
- Auf den Switches muss die zuletzt unterstützte Firmware ausgeführt werden.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Dieser Vorgang läuft unterbrechungsfrei ab und dauert ungefähr zwei Stunden.
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Die Switch-Fabrics werden nacheinander aktualisiert.

Am Ende dieses Verfahrens werden alle vier Schalter auf neue Schalter aktualisiert.

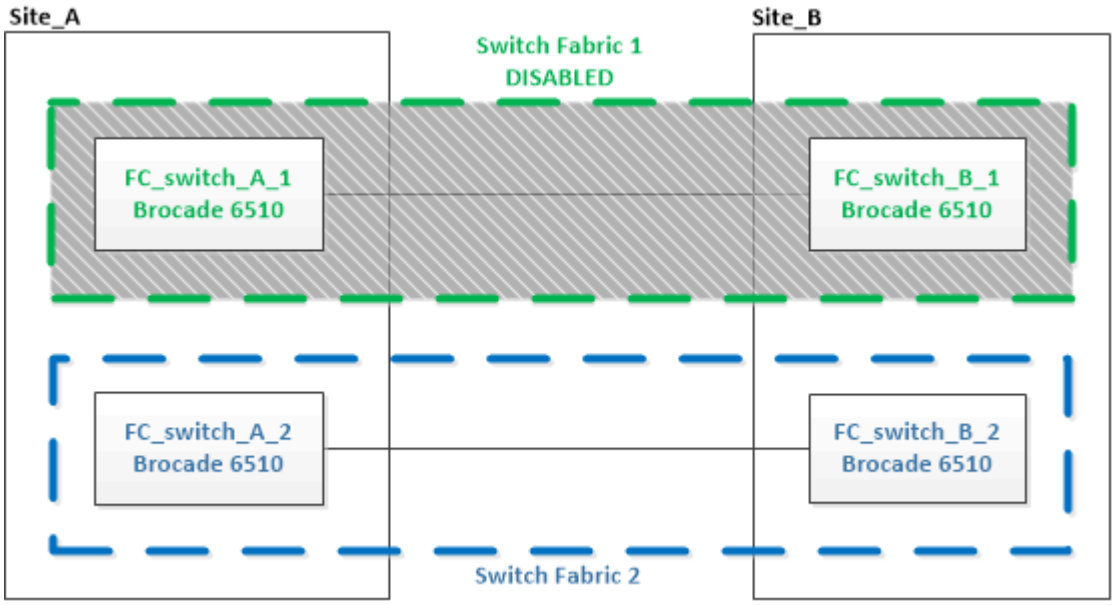


Schritte

1. Deaktivierung der ersten Switch Fabric:

   `FC_switch_A_1:admin> switchCfgPersistentDisable`

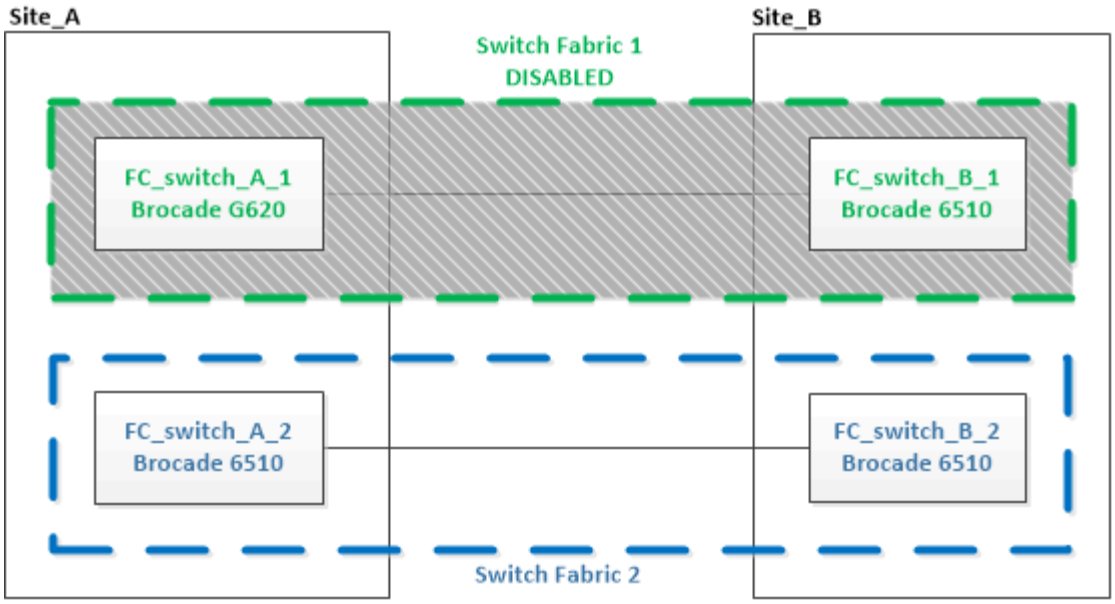
   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```



2. Ersetzen Sie die alten Schalter an einem MetroCluster-Standort.

   a. Trennen Sie die Verkabelung, und entfernen Sie den deaktivierten Schalter.

   b. Setzen Sie den neuen Schalter in das Rack ein.



c. Deaktivieren Sie die neuen Switches, indem Sie den folgenden Befehl auf beiden Switches ausführen:

`switchCfgPersistentDisable`

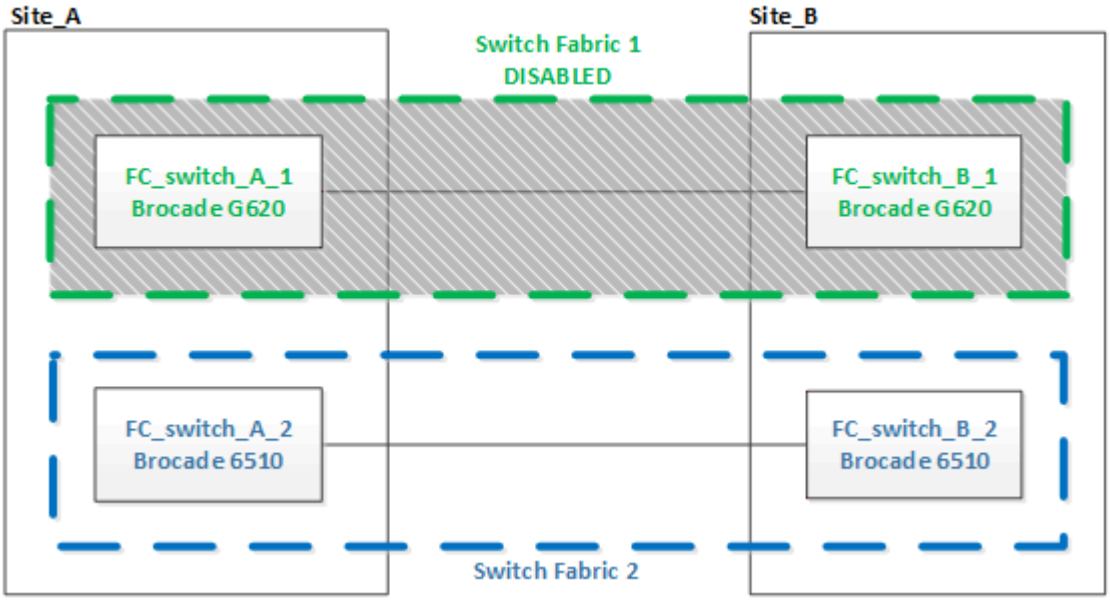
```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

d. Schließen Sie den neuen Switch mithilfe der empfohlenen Anschlusszuordnungen an.

"Portzuweisungen für FC-Switches"

e. Wiederholen Sie diese Unterschritte am Partner-MetroCluster-Standort, um den zweiten Switch der ersten Switch-Fabric zu ersetzen.

Beide Schalter in Fabric 1 wurden ersetzt.



3. Starten Sie die neuen Schalter, und lassen Sie sie hochfahren.
4. Konfigurieren Sie die Brocade FC-Switches mithilfe einer der folgenden Verfahren:

   "Konfigurieren Sie Brocade FC Switches mit RCF-Dateien"

   "Konfigurieren Sie die Brocade FC-Switches manuell"

5. Switch-Konfiguration speichern:

   ```
   cfgSave
   ```

6. Warten Sie 10 Minuten, bis sich die Konfiguration stabilisiert.
7. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:

   ```
   run local sysconfig -v
   ```

   In der Ausgabe werden die mit den Initiator-Ports des Controllers verbundenen Festplatten angezeigt und die mit den FC-to-SAS-Bridges verbundenen Shelfs werden angezeigt:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
   System Serial Number: 940001025471 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   be multi-path HA**
   .
   .
   .
   slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
   Initiator port**
           Firmware rev:      7.5.0
           Flash rev:         0.0.0
           Host Port Id:      0x60130
           FC Node Name:      5:00a:098201:bae312
           FC Port Name:      5:00a:098201:bae312
           SFP Vendor:        UTILITIES CORP.
           SFP Part Number:   FTLF8529P3BCVAN1
           SFP Serial Number: URQ0Q9R
           SFP Capabilities:  4, 8 or 16 Gbit
           Link Data Rate:    16 Gbit
           Switch Port:       brcd6505-fcs40:1
     **<List of disks visible to port\>**
            ID     Vendor   Model            FW    Size
           brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
   847.5GB (1953525168 512B/sect)
           brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
   ```

```
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

8. Überprüfen Sie die Switch-Firmware-Version, um zur Switch-Eingabeaufforderung zurückzukehren:

   `firmwareShow`

   Auf den Switches muss die zuletzt unterstützte Firmware ausgeführt werden.

   "NetApp Interoperabilitäts-Matrix-Tool"

9. Simulation eines Switchover-Vorgangs:

   a. Ändern Sie in der Eingabeaufforderung eines beliebigen Nodes die erweiterte Berechtigungsebene: `set -privilege advanced`

      Sie müssen mit „`y`“ antworten, wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*>) anzuzeigen.

   b. Führen Sie den Switchover mit durch `-simulate` Parameter:

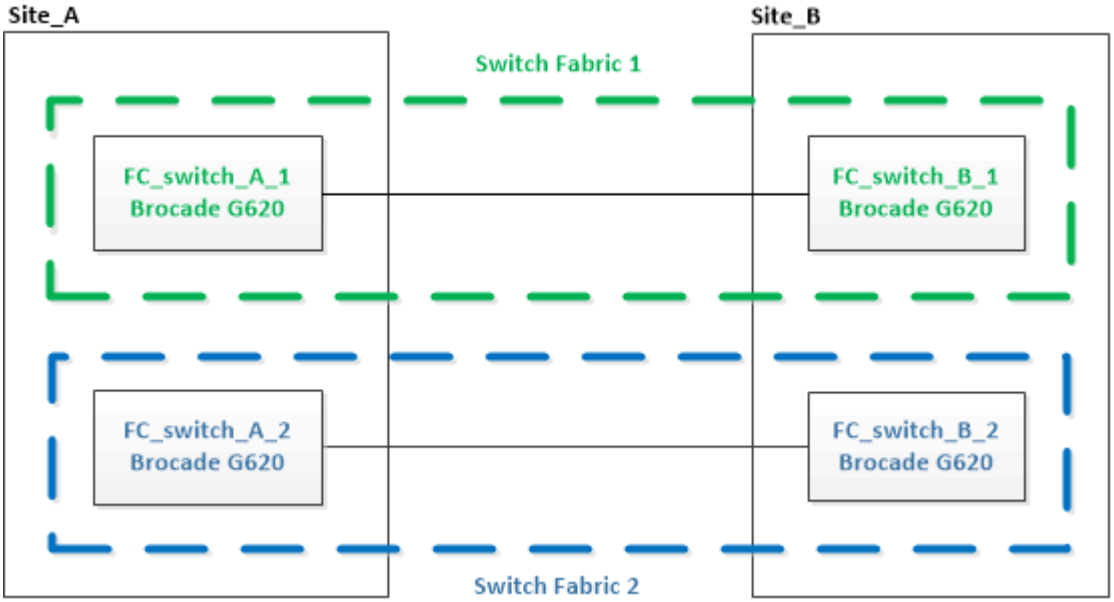
      `metrocluster switchover -simulate`

   c. Zurück zur Administratorberechtigungsebene:

      `set -privilege admin`

10. Wiederholen Sie die vorherigen Schritte auf der zweiten Switch Fabric.

Nach Wiederholung der Schritte wurden alle vier Switches aktualisiert und die MetroCluster-Konfiguration befindet sich im normalen Betrieb.



Austausch eines Brocade FC-Switches

Sie müssen dieses Brocade-spezifische Verfahren zum Austausch eines fehlerhaften Switches verwenden.

Über diese Aufgabe

Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

In den folgenden Beispielen ist FC_Switch_A_1 der gesunde Schalter und FC_Switch_B_1 der beeinträchtigte Schalter. Die Verwendung des Switch-Ports in den Beispielen wird in der folgenden Tabelle dargestellt:

Port-Verbindungen	Ports
FC-VI-Verbindungen	0, 3
HBA-Verbindungen	1, 2, 4, 5
FC-to-SAS-Bridge-Verbindungen	6, 7
ISL-Verbindungen	10, 11

Die Beispiele zeigen zwei FC-to-SAS-Bridges. Wenn mehr vorhanden ist, müssen Sie die zusätzlichen Ports deaktivieren und anschließend aktivieren.

Dieser Vorgang läuft unterbrechungsfrei ab und dauert ungefähr zwei Stunden.

Die Verwendung des Switch-Ports sollte den empfohlenen Zuweisungen folgen.

- "Portzuweisungen für FC-Switches"

Schritte

1. Abschalten des Switch, der ausgetauscht wird, durch Deaktivieren der ISL-Ports am gesunden Switch im Fabric sowie der FC-VI- und HBA-Ports am beeinträchtigten Switch (wenn der beeinträchtigte Schalter noch in Betrieb ist):

   a. Deaktivieren Sie die ISL-Ports auf dem gesunden Switch für jeden Port:

   `portcfgpersistentdisable` *`port-number`*

   ```
   FC_switch_A_1:admin> portcfgpersistentdisable 10
   FC_switch_A_1:admin> portcfgpersistentdisable 11
   ```

   b. Wenn der beeinträchtigte Switch noch funktionsfähig ist, deaktivieren Sie die FC-VI- und HBA-Ports auf diesem Switch für jeden Port:

   `portcfgpersistentdisable` *`port-number`*

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5
```

2. Wenn der Schalter ohne Störungen noch in Betrieb ist, erfassen Sie den Ausgang vom `switchshow` Befehl.

```
FC_switch_B_1:admin> switchshow
    switchName: FC_switch_B_1
    switchType: 71.2
    switchState:Online
    switchMode: Native
    switchRole: Subordinate
    switchDomain:       2
    switchId:   fffc01
    switchWwn:  10:00:00:05:33:86:89:cb
    zoning:             OFF
    switchBeacon:       OFF
```

3. Starten und Vorkonfigurieren des neuen Switches vor der physischen Installation:

   a. Schalten Sie den neuen Schalter ein, und lassen Sie ihn starten.

b. Überprüfen Sie die Firmware-Version auf dem Switch, um sicherzustellen, dass sie mit der Version der anderen FC-Switches übereinstimmt:

```
firmwareShow
```

c. Konfigurieren Sie den neuen Switch, indem Sie die Brocade-Verfahren in befolgen"Konfigurieren Sie die FC-Switches".

> An diesem Punkt ist der neue Switch nicht mit der MetroCluster-Konfiguration verbunden.

d. Deaktivieren Sie die FC-VI-, HBA- und Storage-Ports auf dem neuen Switch sowie die mit den FC-SAS-Bridges verbundenen Ports.

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5

FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. Ersetzen Sie den Schalter physisch:
   a. Schalten Sie den FC-Schalter für beeinträchtigte Personen aus.
   b. Schalten Sie den Ersatz-FC-Switch aus.
   c. Trennen Sie den Schalter für beeinträchtigte Kabel, und entfernen Sie ihn. Beachten Sie dabei sorgfältig, welche Kabel mit welchen Anschlüssen verbunden sind.
   d. Setzen Sie den Ersatzschalter in das Rack ein.
   e. Verkabeln Sie den Ersatzschalter genau so, wie der alte Schalter verkabelt war.
   f. Schalten Sie den neuen FC Switch ein.
5. Informationen zum Aktivieren der ISL-Verschlüsselung finden Sie unter "Konfigurieren Sie die Brocade FC-Switches manuell" .

   Wenn Sie die ISL-Verschlüsselung aktivieren, müssen Sie die folgenden Aufgaben erfüllen:

   - Deaktivieren Sie die virtuelle Fabric
   - Legen Sie die Nutzlast fest
   - Legen Sie die Authentifizierungsrichtlinie fest
   - Aktivierung der ISL-Verschlüsselung bei Brocade Switches
6. Die Konfiguration des neuen Switch abschließen:
   a. ISLs aktivieren:

   ```
   portcfgpersistentenable port-number
   ```

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

b. Überprüfen Sie die Zoning-Konfiguration:

```
cfg show
```

c. Vergewissern Sie sich am Ersatzschalter (im Beispiel FC_Switch_B_1), dass die ISLs online sind:

```
switchshow
```

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

d. Aktivieren Sie die Storage-Ports, die mit den FC-Bridges verbunden sind.

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

e. Aktivieren Sie Storage-, HBA- und FC-VI-Ports.

Im folgenden Beispiel werden Befehle angezeigt, die zum Aktivieren der Ports zum Verbinden von HBA-Adaptern verwendet werden:

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

Im folgenden Beispiel werden die Befehle angezeigt, die zum Aktivieren der Ports, die die FC-VI-Adapter verbinden, verwendet werden:

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

7. Vergewissern Sie sich, dass die Ports online sind:

   `switchshow`

8. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      `node run -node node-name sysconfig -a`

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      `system health alert show`

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

      `metrocluster show`

   d. Durchführen einer MetroCluster-Prüfung:

      `metrocluster check run`

   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

      `metrocluster check show`

   f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

      `storage switch show`

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

Umbenennen eines Brocade FC-Switch

Sie müssen möglicherweise einen Brocade FC-Switch umbenennen, um eine konsistente Benennung in Ihrer Konfiguration sicherzustellen.

Über diese Aufgabe

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Deaktivieren Sie den Switch oder die Switches in einem Fabric dauerhaft:

   `switchcfgpersistentdisable`

   Das folgende Beispiel zeigt die Ausgabe für das **`switchcfgpersistentdisable`** Befehl:

   ```
   7840_FCIP_2:admin> switchcfgpersistentdisable
   Switch's persistent state set to 'disabled'
   2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is DEGRADED.
   2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is OFFLINE.

   7840_FCIP_2:admin>
   ```

2. Umbenennung des Switch oder Switches:

   `switchname` *`new-switch-name`*

   Wenn Sie beide Switches in der Fabric umbenennen, verwenden Sie auf jedem Switch den gleichen Befehl.

   Das folgende Beispiel zeigt die Ausgabe für das **`switchname` *`new-switch-name`*** Befehl:

   ```
   7840_FCIP_2:admin> switchname FC_switch_1_B
   Committing configuration...
   Done.
   Switch name has been changed.Please re-login into the switch for the
   change to be applied.
   2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B,
   Switch name has been successfully changed to FC_switch_1_B.
   7840_FCIP_2:admin>
   ```

3. Starten Sie den Switch oder die Switches neu:

   `reboot`

   Wenn Sie beide Switches in der Fabric umbenennen, booten Sie beide Switches neu. Nach Abschluss des Neubootens wird der Switch an allen Orten umbenannt.

   Das folgende Beispiel zeigt die Ausgabe für das **`reboot`** Befehl:

```
7840_FCIP_2:admin> reboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840,
System is about to reload.
Rebooting! Fri Mar  9 07:42:11 CET 2018

Broadcast message from root (ttyS0) Fri Mar  9 07:42:11 2018...

The system is going down for reboot NOW !!
INIT: Switching to runlevel: 6
INIT:
2018/03/09-07:50:48, [ESM-1013], 146104, FID 128, INFO, FC_switch_1_B,
DP0 Configuration replay has completed.
2018/03/09-07:50:48, [ESM-1011], 146105, FID 128, INFO, FC_switch_1_B,
DP0 is ONLINE.

*** CORE FILES WARNING (03/09/18 - 08:00:00 ) ***
10248 KBytes in 1 file(s)
use "supportsave" command to upload


*** FFDC FILES WARNING (03/09/18 - 08:00:00 ) ***
520 KBytes in 1 file(s)
```

4. Dauerhaft aktivieren Sie die Switches: **`switchcfgpersistentenable`**

   Das folgende Beispiel zeigt die Ausgabe für das **`switchcfgpersistentenable`** Befehl:

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch's persistent state set to 'enabled'
FC_switch_1_B:admin>
FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128,
INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B,
VE Tunnel 24 is ONLINE.

FC_switch_1_B:admin>


FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address  Media Speed   State       Proto
==================================================
   0   0   060000   id    16G     Online      FC  F-Port
50:0a:09:81:06:a5:5a:08
   1   1   060100   id    16G     Online      FC  F-Port
50:0a:09:83:06:a5:5a:08
```

5. Vergewissern Sie sich, dass die Änderung des Switch-Namens von der ONTAP-Cluster-Eingabeaufforderung aus sichtbar ist:

   `storage switch show`

   Das folgende Beispiel zeigt die Ausgabe für das **`storage switch show`** Befehl:

```
cluster_A::*> storage switch show
  (storage switch show)
                      Symbolic                                Is
Monitor
Switch                Name     Vendor  Model Switch WWN       Monitored
Status
--------------------- -------- ------- ----- ---------------- ---------
-------
Brocade_172.20.7.90
                      RTP-FC01-510Q40
                               Brocade Brocade7840
                                             1000c4f57c904bc8 true
ok
Brocade_172.20.7.91
                      RTP-FC02-510Q40
                               Brocade Brocade7840
                                             100050eb1a9aa579 true
ok
Brocade_172.20.7.92
```

Deaktivieren der Verschlüsselung bei Brocade FC-Switches

Möglicherweise müssen Sie die Verschlüsselung auf Brocade FC-Switches deaktivieren.

Schritte

1. Senden Sie von beiden Standorten eine AutoSupport-Nachricht, die den Beginn der Wartung angibt.

```
cluster_A::> autosupport invoke -node * -type all -message MAINT=4h
```

```
cluster_B::> autosupport invoke -node * -type all -message MAINT=4h
```

2. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration von Cluster A

   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
   `metrocluster show`

   ```
   cluster_A::> metrocluster show
   ```

   b. Führen Sie eine MetroCluster-Prüfung durch:
   `metrocluster check run`

```
cluster_A::> metrocluster check run
```

c. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
metrocluster check show

```
cluster_A::> metrocluster check show
```

3. Überprüfen Sie den Status beider Switches:

fabric show

```
switch_A_1:admin> fabric show
```

```
switch_B_1:admin> fabric show
```

4. Beide Switches deaktivieren:

switchdisable

```
switch_A_1:admin> switchdisable
```

```
switch_B_1:admin> switchdisable
```

5. Überprüfen Sie die verfügbaren Pfade für die Nodes auf den einzelnen Clustern:

sysconfig

```
cluster_A::> system node run -node node-name -command sysconfig -a
```

```
cluster_B::> system node run -node node-name -command sysconfig -a
```

Da die Switch-Fabric jetzt deaktiviert ist, sollte die System-Storage-Konfiguration Single-Path HA sein.

6. Überprüfen Sie den Aggregatstatus für beide Cluster.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

Ausgabe des Systems sollte zeigen, dass die Aggregate für beide Cluster gespiegelt und normal sind:

```
mirrored,normal
```

7. Wiederholen Sie die folgenden Teilschritte von der Admin-Eingabeaufforderung auf beiden Switches.

   a. Zeigt an, welche Ports verschlüsselt sind:
   portenccompshow

   ```
   switch_A_1:admin> portenccompshow
   ```

   b. Deaktivieren Sie die Verschlüsselung auf den verschlüsselten Ports:
   portcfgencrypt – disable *port-number*

   ```
   switch_A_1:admin> portcfgencrypt --disable 40
   switch_A_1:admin> portcfgencrypt --disable 41
   switch_A_1:admin> portcfgencrypt --disable 42
   switch_A_1:admin> portcfgencrypt --disable 43
   ```

   c. Legen Sie den Authentifizierungstyp auf alle fest:

   authUtil --set -a all

```
switch_A_1:admin> authUtil --set -a all
```

   a. Legen Sie die Authentifizierungsrichtlinie auf dem Switch fest. Zu aus:
   authutil --policy -sw off

   ```
   switch_A_1:admin> authutil --policy -sw off
   ```

   b. Setzen Sie die Authentifizierung Diffie-Hellman-Gruppe auf * :
   authutil --set -g *

   ```
   switch_A_1:admin> authUtil --set -g *
   ```

   c. Löschen Sie die geheime Schlüsseldatenbank:
   secAuthSecret --remove -all

```
switch_A_1:admin> secAuthSecret --remove -all
```

d. Vergewissern Sie sich, dass die Verschlüsselung auf den Ports: + deaktiviert ist
portenccompshow

```
switch_A_1:admin> portenccompshow
```

e. Schalter aktivieren:
switchenable

```
switch_A_1:admin> switchenable
```

f. Den Status der ISLs bestätigen:
islshow

```
switch_A_1:admin> islshow
```

8. Überprüfen Sie die verfügbaren Pfade für die Nodes auf den einzelnen Clustern:

sysconfig

```
cluster_A::> system node run -node * -command sysconfig -a
```

```
cluster_B::> system node run -node * -command sysconfig -a
```

Die Systemausgabe sollte angeben, dass sich die Storage-Konfiguration in Quad-Path HA geändert hat.

9. Überprüfen Sie den Aggregatstatus für beide Cluster.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

Das System sollte zeigen, dass die Aggregate für beide Cluster gespiegelt und normal sind, wie in der folgenden Befehlsausgabe des Systems dargestellt:

```
mirrored,normal
```

10. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration von Cluster A

    a. Führen Sie eine MetroCluster-Prüfung durch:
    `metrocluster check run`

    ```
    cluster_A::> metrocluster check run
    ```

    b. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
    `metrocluster check show`

    ```
    cluster_A::> metrocluster check show
    ```

11. Senden Sie eine AutoSupport-Nachricht von beiden Standorten, die das Ende der Wartung angibt.

    ```
    cluster_A::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

    ```
    cluster_B::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

Ändern Sie die ISL-Eigenschaften, ISL-Ports oder die IOD/OOD-Konfiguration auf einem Brocade-Switch

Möglicherweise müssen Sie ISLs zu einem Switch hinzufügen, wenn Hardware wie zusätzliche oder schnellere Controller oder Switches hinzugefügt bzw. aktualisiert wird.

Bevor Sie beginnen

Stellen Sie sicher, dass das System ordnungsgemäß konfiguriert ist, dass alle Fabric Switches funktionsfähig sind und keine Fehler auftreten.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Wenn sich die Ausrüstung auf der ISL-Verbindung ändert und die neue Link-Konfiguration die aktuelle Konfiguration-----Trunking und bestellte Anlieferung nicht mehr unterstützt, muss das Fabric neu konfiguriert werden, um die korrekte Routing-Richtlinie zu erhalten: Entweder in-order-Delivery (IOD) oder Out-of-Order-Delivery (OOD).

> Führen Sie die folgenden Schritte aus, um Änderungen an OOD von der ONTAP-Software vorzunehmen: "Konfigurieren von in-Order-Lieferung oder Lieferung von Frames auf ONTAP Software außerhalb der Reihenfolge"

Schritte

1. Deaktivieren von FCVI- und Storage HBA-Ports:

    ```
    portcfgpersistentdisable port number
    ```

Standardmäßig werden die ersten 8 Ports (Ports 0 bis 7) für FCVI und Storage HBA verwendet. Die Ports müssen dauerhaft deaktiviert werden, damit die Ports im Falle eines Switch-Neustarts deaktiviert bleiben.

Im folgenden Beispiel wird gezeigt, dass die ISL-Ports 0—7 auf beiden Switches deaktiviert sind:

```
Switch_A_1:admin> portcfgpersistentdisable 0-7
Switch_B_1:admin> portcfgpersistentdisable 0-7
```

2. Ändern Sie die ISL-Ports nach Bedarf.

Option	Schritt

So ändern Sie die Geschwindigkeit eines ISL-Ports:	Verwenden Sie die `portcfgspeed` *`port number port speed`* Befehl an beiden Switches auf der Fabric.
	
	Im folgenden Beispiel wird die Port-Geschwindigkeit von ISL von 40 Gbit/s auf 16 Gbit/s geändert:
	
	`brocade_switch_A_1:admin> portcfgspeed 40 16`
	
	Sie können überprüfen, ob sich die Geschwindigkeit mit dem geändert hat `switchshow` Befehl:
	
	`brocade_switch_A_1:admin> switchshow`
	
	Die folgende Ausgabe sollte angezeigt werden:
	
	`. . .`
	`40 40 062800 id 16G No_Sync FC Disabled`
	`. . .`

So ändern Sie die Entfernung eines ISL-Ports:	Verwenden Sie die `portcfglongdistance` *`port number port distance`* Befehl an beiden Switches in der Fabric.
So entfernen Sie eine ISL:	Trennen Sie die Verbindung.
ISL hinzufügen…	Fügen Sie SFPs in die Ports ein, die Sie als ISL-Ports hinzufügen. Stellen Sie sicher, dass diese Ports in aufgeführt sind "Installieren Sie eine Fabric-Attached MetroCluster" Für den Schalter, zu dem Sie sie hinzufügen.
So verschieben Sie eine ISL…	Der Standortwechsel eines ISL entspricht dem Entfernen und anschließenden Hinzufügen einer ISL. Entfernen Sie zunächst die ISL, indem Sie die Verbindung trennen und dann SFPs in die Ports einfügen, die Sie als ISL-Ports hinzufügen.

Wenn Sie Änderungen an ISL-Ports vornehmen, müssen Sie möglicherweise auch zusätzliche Einstellungen anwenden, die vom WDM-Anbieter empfohlen werden. Weitere Informationen finden Sie in der Dokumentation des WDM-Anbieters.

3. Rekonfigurieren für Lieferung außerhalb des Auftrags (OOD) oder in-Order-Lieferung (IOD).

Wenn die Routing-Richtlinien unverändert bleiben, müssen Sie die Routingrichtlinien nicht neu konfigurieren, und dieser Schritt kann ignoriert werden. Die ONTAP-Konfiguration muss an die Fabric-Konfiguration angepasst werden. Wenn das Fabric für OOD konfiguriert ist, muss auch ONTAP für OOD konfiguriert sein. Gleiches gilt für IOD.

Dieser Schritt sollte in folgenden Szenarien ausgeführt werden:

- Vor dem Wechsel hatte mehr als eine ISL einen Trunk gebildet, doch nach der Änderung wird Trunking nicht mehr unterstützt. In diesem Fall müssen Sie die Struktur für OOD konfigurieren.
- Es gibt ein ISL vor der Änderung und mehrere ISLs nach der Änderung.
- Wenn mehrere ISLs einen Trunk bilden, konfigurieren Sie das Fabric für IOD. Wenn mehrere ISLs **nicht** einen Trunk bilden können, konfigurieren Sie das Fabric für OOD.
- Deaktivieren Sie die Switches dauerhaft mithilfe der `switchcfgpersistentdisable` Befehl wie im folgenden Beispiel dargestellt:

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

i. Konfigurieren Sie den Trunking-Modus für jede ISL `portcfgtrunkport` *`port number`* Wie in der folgenden Tabelle dargestellt:

Szenario	Schritte

Konfiguration der ISL für das Trunking \(IOD\)	Stellen Sie die ein `portcfgtrunkport` *`port number`* Zu 1:
	`FC_switch_A_1:admin> portcfgtrunkport 20 1`
	`FC_switch_A_1:admin> portcfgtrunkport 21 1`
	`FC_switch_B_1:admin> portcfgtrunkport 20 1`
	`FC_switch_B_1:admin> portcfgtrunkport 21 1`

Konfiguration der ISL für Trunking \ (OOD\)	Stellen Sie die ein `portcfgtrunkport` *`port number`* An 0:
	`FC_switch_A_1:admin> portcfgtrunkport 20 0`
	`FC_switch_A_1:admin> portcfgtrunkport 21 0`
	`FC_switch_B_1:admin> portcfgtrunkport 20 0`
	`FC_switch_B_1:admin> portcfgtrunkport 21 0`

ii. Konfigurieren Sie die Fabric für IOD oder OOD nach Bedarf.

Szenario	Schritte

Konfigurieren Sie die Fabric für IOD	Legen Sie mithilfe des die drei Einstellungen für IOD, APT und DLS fest `iodset`, `aptpolicypolicy`, und `dlsreset` Befehle, wie im folgenden Beispiel gezeigt:
	
	`Switch_A_1:admin> iodset`
	`Switch_A_1:admin> aptpolicy 1`
	`Policy updated successfully.`
	`Switch_A_1:admin> dlsreset`
	`FC_switch_A_1:admin>portcfgtrunkport 40 1`
	`FC_switch_A_1:admin>portcfgtrunkport 41 1`
	
	`Switch_B_1:admin> iodset`
	`Switch_B_1:admin> aptpolicy 1`
	`Policy updated successfully.`
	`Switch_B_1:admin> dlsreset`
	`FC_switch_B_1:admin>portcfgtrunkport 20 1`
	`FC_switch_B_1:admin>portcfgtrunkport 21 1`

Konfigurieren Sie das Fabric für OOD	Legen Sie mithilfe des die drei Einstellungen für IOD, APT und DLS fest `iodreset`, `aptpolicy`*`policy`*, und `dlsset` Befehle, wie im folgenden Beispiel gezeigt:
	
	`Switch_A_1:admin> iodreset`
	`Switch_A_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_A_1:admin> dlsset`
	`FC_switch_A_1:admin> portcfgtrunkport 40 0`
	`FC_switch_A_1:admin> portcfgtrunkport 41 0`
	
	`Switch_B_1:admin> iodreset`
	`Switch_B_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_B_1:admin> dlsset`
	`FC_switch_B_1:admin> portcfgtrunkport 40 0`
	`FC_switch_B_1:admin> portcfgtrunkport 41 0`

iii. Dauerhaft aktivieren Sie die Switches:

```
switchcfgpersistentenable
```

```
switch_A_1:admin>switchcfgpersistentenable
switch_B_1:admin>switchcfgpersistentenable
```

+
Wenn dieser Befehl nicht vorhanden ist, verwenden Sie den `switchenable` Befehl wie im folgenden Beispiel dargestellt:

```
brocade_switch_A_1:admin>
switchenable
```

i. Überprüfen Sie die OOD-Einstellungen mit der `iodshow`, `aptpolicy`, und `dlsshow` Befehle, wie im folgenden Beispiel gezeigt:

```
switch_A_1:admin> iodshow
IOD is not set

switch_A_1:admin> aptpolicy

       Current Policy: 3 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

Sie müssen diese Befehle auf beiden Switches ausführen.

ii. Überprüfen Sie die IOD-Einstellungen mit dem `iodshow`, `aptpolicy`, und `dlsshow` Befehle, wie im folgenden Beispiel gezeigt:

```
switch_A_1:admin> iodshow
IOD is set

switch_A_1:admin> aptpolicy
       Current Policy: 1 0(ap)

       3 0(ap) : Default Policy
       1: Port Based Routing Policy
       3: Exchange Based Routing Policy
       0: AP Shared Link Policy
       1: AP Dedicated Link Policy
       command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is not set
```

Sie müssen diese Befehle auf beiden Switches ausführen.

4. Stellen Sie sicher, dass die ISLs online sind und mit dem Trunking (sofern die Verbindungsausrüstung Trunking unterstützt) getrackt wurden `islshow` Und `trunkshow` Befehle.

Wenn FEC aktiviert ist, kann der Deskew-Wert des letzten Online-Ports der Trunk-Gruppe einen Unterschied von bis zu 36 zeigen, obwohl die Kabel alle dieselbe Länge haben.

Sind ISLs triked?	Sie sehen die folgende Ausgabe des Systems…

Ja.	Wenn die ISLs nicht verfügbar sind, erscheint in der Ausgabe für das nur ein einziger ISL `islshow` Befehl. Port 40 oder 41 können je nach Trunk-Master angezeigt werden. Die Ausgabe von `trunkshow` Sollte ein Trunk mit ID „`1`“ die sowohl physischen ISLs auf den Ports 40 und 41 auflisten. Im folgenden Beispiel sind die Ports 40 und 41 für die Verwendung als ISL konfiguriert:
	`switch_A_1:admin> islshow 1:`
	`40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G`
	`bw: 32.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER`
	`41-> 41 10:00:00:05:33:88:9c:68 2 deskew 15`

Nein	Wenn die ISLs nicht in Trunks sind, erscheinen beide ISLs separat in den Ausgaben für `islshow` Und `trunkshow`. Bei beiden Befehlen werden die ISLs mit ihrer ID von „`1`“ und „`2`“ aufgelistet. Im folgenden Beispiel werden die Ports „`40`“ und „`41`“ für die Verwendung als ISL konfiguriert:
	
	`switch_A_1:admin> islshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC`
	`2: 41-> 41 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER`
	`2: 41-> 41 10:00:00:05:33:88:9c:68 2 deskew 48 MASTER`

5. Führen Sie die aus `spinfab` Befehl an beiden Switches, um sich zu vergewissern, dass die ISLs sich in einem ordnungsgemäßen Zustand befinden:

```
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. Aktivieren Sie die Ports, die in Schritt 1 deaktiviert wurden:

   `portenable` *`port number`*

   Im folgenden Beispiel werden die ISL-Ports „`0`“ bis „`7`“ aktiviert:

```
brocade_switch_A_1:admin> portenable 0-7
```

Austausch eines Cisco FC-Switches

Sie müssen Cisco spezifische Schritte verwenden, um einen fehlerhaften Cisco FC-Switch zu ersetzen.

Bevor Sie beginnen

Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Über diese Aufgabe

Dieser Vorgang läuft unterbrechungsfrei ab und dauert ungefähr zwei Stunden.

In den Beispielen in diesem Verfahren ist FC_Switch_A_1 der gesunde Schalter und FC_Switch_B_1 der beeinträchtigte Schalter. Die Verwendung des Switch-Ports in den Beispielen wird in der folgenden Tabelle dargestellt:

Rolle	Ports
FC-VI-Verbindungen	1, 4
HBA-Verbindungen	2, 3, 5, 6
FC-to-SAS-Bridge-Verbindungen	7, 8
ISL-Verbindungen	36, 40

Die Beispiele zeigen zwei FC-to-SAS-Bridges. Wenn mehr vorhanden ist, müssen Sie die zusätzlichen Ports deaktivieren und anschließend aktivieren.

Die Verwendung des Switch-Ports sollte den empfohlenen Zuweisungen folgen.

- "Portzuweisungen für FC-Switches"

Schritte

1. Deaktivieren Sie die ISL-Ports am Schalter OK, um den Schalter für beeinträchtigte Personen abzuschalten.

   Diese Schritte werden auf dem gesunden Schalter durchgeführt.

   a. Konfigurationsmodus aufrufen:
   `conf t`

   b. Deaktivieren Sie die ISL-Ports auf dem gesunden Switch mit dem `interface` Und `shut` Befehle.

   ```
   FC_switch_A_1# conf t
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config)# shut
   FC_switch_A_1(config)# interface fc1/40
   FC_switch_A_1(config)# shut
   ```

   c. Beenden Sie den Konfigurationsmodus, und kopieren Sie die Konfiguration in die Startkonfiguration.

   ```
   FC_switch_A_1(config)# end
   FC_switch_A_1# copy running-config startup-config
   FC_switch_A_1#
   ```

2. Abtrennung der FC-VI- und HBA-Ports am beeinträchtigten Schalter (falls noch ausgeführt)

   Diese Schritte werden auf dem Schalter mit beeinträchtigten Arbeitsschritten durchgeführt.

   a. Konfigurationsmodus aufrufen:

   ```
   conf t
   ```

b. Wenn der Schalter ohne Beeinträchtigung weiterhin betriebsbereit ist, deaktivieren Sie die FC-VI- und HBA-Ports auf dem beeinträchtigten Switch mit der Schnittstelle und den Befehlen zum Herunterfahren.

```
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
```

c. Beenden Sie den Konfigurationsmodus, und kopieren Sie die Konfiguration in die Startkonfiguration.

```
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. Wenn der Schalter ohne Störungen noch in Betrieb ist, bestimmen Sie den WWN für den Switch:

   `show wwn switch`

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:e3:86:50
FC_switch_B_1#
```

4. Starten Sie den Ersatz-Switch, und konfigurieren Sie ihn vor der physischen Installation.

   An dieser Stelle ist der Ersatzschalter nicht mit der MetroCluster Konfiguration verbunden. Die ISL-Ports am Partner-Switch sind deaktiviert (im ausgeschalteten Modus) und offline.

   a. Schalten Sie den Ersatzschalter ein, und lassen Sie ihn starten.
   b. Überprüfen Sie die Firmware-Version auf dem Ersatzschalter, um sicherzustellen, dass sie mit der Version der anderen FC-Switches übereinstimmt:

      `show version`

   c. Konfigurieren Sie den Ersatz-Switch, wie im Abschnitt „`Configuring Zoning on a Cisco FC Switch`“ beschrieben, wie im Installations- und Konfigurationshandbuch *MetroCluster* beschrieben.

      "Installation und Konfiguration von Fabric-Attached MetroCluster"

   Später konfigurieren Sie das Zoning in diesem Verfahren.

   a. Deaktivieren Sie die FC-VI-, HBA- und Storage-Ports am Ersatz-Switch.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/7-8
FC_switch_B_1(config)# shut
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

5. Ersetzen Sie den Schalter für beeinträchtigte Personen physisch:
   a. Schalten Sie den beeinträchtigten Schalter aus.
   b. Schalten Sie den Ersatzschalter aus.
   c. Trennen Sie den Schalter für beeinträchtigte Kabel, und entfernen Sie ihn. Beachten Sie dabei sorgfältig, welche Kabel mit welchen Anschlüssen verbunden sind.
   d. Setzen Sie den Ersatzschalter in das Rack ein.
   e. Den Ersatzschalter genau so verkabeln, wie der beeinträchtigte Schalter verkabelt war.
   f. Schalten Sie den Ersatzschalter ein.
6. Aktivieren Sie die ISL-Ports am Ersatz-Switch.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#
```

7. Stellen Sie sicher, dass die ISL-Ports am Austausch-Switch aktiviert sind:

```
show interface brief
```

8. Passen Sie das Zoning auf dem Ersatz-Switch an die MetroCluster Konfiguration an:
   a. Verteilen Sie die Zoning-Informationen von der gesunden Fabric.

      In diesem Beispiel wurde FC_Switch_B_1 ersetzt und die Zoning-Informationen von FC_Switch_A_1 abgerufen:

```
FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end
```

b. Überprüfen Sie auf dem Ersatzschalter, ob die Zoning-Informationen ordnungsgemäß vom gesunden Switch abgerufen wurden:

```
show zone
```

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. Suchen Sie die WWNs der Switches.

In diesem Beispiel sind die beiden Switch-WWNs:

- FC_Switch_A_1: 20:00:54:7f:ee:b8:24:c0
- FC_Switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

d. Entfernen Sie die Zonenmitglieder, die nicht zu den Switch-WWNs der beiden Schalter gehören.

   In diesem Beispiel zeigt „`no Member Interface`“ in der Ausgabe, dass die folgenden Mitglieder nicht mit dem Switch WWN eines der Switches in der Fabric verknüpft sind und entfernt werden müssen:

   - Zonenname FC-VI_Zone_1_10 vsan 10
     - Schnittstelle fc1/1, gestreut 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/2 geschwibelt 20:00:54:7f:ee:e3:86:50
   - Zonenname STOR_Zone_1_20_25A vsan 20
     - Schnittstelle fc1/5 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/8 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/9 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/10 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/11 geschwibelt 20:00:54:7f:ee:e3:86:50
   - Zonenname STOR_Zone_1_20_25B vsan 20
     - Schnittstelle fc1/8 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/9 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/10 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/11 swwn 20:00:54:7f:ee:e3:86:50 das folgende Beispiel zeigt, wie Sie diese Schnittstellen entfernen:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

e. Fügen Sie die Anschlüsse des Ersatzschalters zu den Zonen hinzu.

   Alle Kabel des Ersatzschalters müssen mit dem Schalter für beeinträchtigte Kabel übereinstimmen:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

f. Überprüfen Sie, ob das Zoning ordnungsgemäß konfiguriert ist:

```
show zone
```

Die Ausgabe des folgenden Beispiels zeigt die drei Zonen:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

g. Aktivieren der Konnektivität zum Storage und den Controllern

   Im folgenden Beispiel wird die Portnutzung angezeigt:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      `node run -node node-name sysconfig -a`

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      `system health alert show`

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

      `metrocluster show`

   d. Durchführen einer MetroCluster-Prüfung:

      `metrocluster check run`

   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

      `metrocluster check show`

   f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

      `storage switch show`

   g. Nutzen Sie Config Advisor.

      "NetApp Downloads: Config Advisor"

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

Ändern Sie die ISL-Eigenschaften und die IOD/OOD-Konfiguration auf einem Cisco-FC-Switch

Sie können Inter-Switch Links (ISLs) hinzufügen, die ISL-Geschwindigkeit ändern und auf einem Cisco FC-Switch die Einstellungen für die Zustellung in Bestellung (IOD) oder die

Zustellung außerhalb der Bestellung (OOD) neu konfigurieren.

Fügen Sie ISLs zu einem Cisco FC Switch hinzu

Wenn Sie Hardware hinzufügen oder aktualisieren, müssen Sie eventuell ISLs zu einem Switch hinzufügen, z. B. zum Hinzufügen oder Aktualisieren schnellerer Controller oder schnellerer Switches.

Über diese Aufgabe

Führen Sie diese Schritte an beiden Switches in der Fabric aus, um die ISL-Konnektivität zu überprüfen.

Schritte

1. Deaktivieren Sie die ISL-Ports der ISLs, die auf beiden Switches im Fabric hinzugefügt werden:

   ```
   FC_switch_A_1#config t
   ```

   Geben Sie die folgenden Konfigurationsbefehle pro Zeile ein. Geben Sie STRG-Z ein, nachdem Sie alle Konfigurationsbefehle eingegeben haben.

   ```
       FC_switch_A_1(config)# interface fc1/36
       FC_switch_A_1(config-if)# shut
       FC_switch_A_1(config)# end
   ```

2. Setzen Sie SFPs in die Ports ein, die Sie als ISL-Ports hinzufügen, und verkabeln Sie sie gemäß "Fabric-Attached MetroCluster-Konfiguration verkabeln".

   Stellen Sie sicher, dass diese Ports in der Verkabelungsdokumentation für das Switch-Modell aufgeführt sind, dem Sie sie hinzufügen.

3. Konfigurieren Sie die ISL-Ports, indem Sie die Schritte in ausführen"Verkabelung der ISLs zwischen MetroCluster Standorten".
4. Alle ISL-Ports (falls nicht aktiviert) auf beiden Switches in der Fabric aktivieren:

   ```
   FC_switch_A_1# config t
   ```

   Geben Sie die folgenden Konfigurationsbefehle pro Zeile ein. Beenden Sie mit STRG-Z, nachdem Sie alle Konfigurationsbefehle eingegeben haben.

   ```
   FC_switch_A_1# interface fc1/36
       FC_switch_A_1(config-if)# no shut
       FC_switch_A_1(config)# end
   ```

5. Vergewissern Sie sich, dass die ISLs zwischen beiden Switches hergestellt sind:

   ```
   show topology isl
   ```

6. Wiederholen Sie den Vorgang auf dem zweiten Gewebe:

```
-----------------------------------------------------------------------
--------
    __________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

-----------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

Ändern Sie die ISL-Portgeschwindigkeiten auf einem Cisco FC Switch

Sie können die Geschwindigkeit von ISL-Ports auf einem Switch ändern, um die Qualität der ISL zu verbessern, beispielsweise um die Geschwindigkeit bei ISLs zu verringern, die eine größere Entfernung zurücklegen.

Über diese Aufgabe

Führen Sie diese Schritte an beiden Switches in der Fabric aus, um die ISL-Konnektivität zu überprüfen.

Schritte

1. Deaktivieren Sie die ISL-Ports für die ISLs, für die Sie die Geschwindigkeit auf beiden Switches in der Fabric ändern möchten:

   ```
   FC_switch_A_1# config t
   ```

   Geben Sie die folgenden Konfigurationsbefehle pro Zeile ein. Beenden Sie mit STRG-Z, nachdem Sie alle Konfigurationsbefehle eingegeben haben.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# shut
      FC_switch_A_1(config)# end
   ```

2. Ändern Sie die Geschwindigkeit der ISL-Ports an beiden Switches in der Fabric:

   ```
   FC_switch_A_1# config t
   ```

   Geben Sie die folgenden Konfigurationsbefehle pro Zeile ein. Beenden Sie mit STRG-Z, nachdem Sie alle Konfigurationsbefehle eingegeben haben.

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# switchport speed 16000
```

> Die Geschwindigkeiten für die Ports sind 16 = 16,000 Gbit/s, 8 = 8,000 Gbit/s und 4 = 4,000 Gbit/s.

Überprüfen Sie, ob die ISL-Ports für Ihren Switch in aufgeführt sind"Installieren Sie eine Fabric-Attached MetroCluster-Konfiguration".

3. Alle ISL-Ports (falls nicht aktiviert) auf beiden Switches in der Fabric aktivieren:

   ```
   FC_switch_A_1# config t
   ```

   Geben Sie die folgenden Konfigurationsbefehle pro Zeile ein. Beenden Sie mit STRG-Z, nachdem Sie alle Konfigurationsbefehle eingegeben haben.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

4. Vergewissern Sie sich, dass die ISLs zwischen beiden Switches hergestellt sind:

   ```
   show topology isl
   ```

   ```
   ------------------------------------------------------------------------
   --------
       __________Local_________ _________Remote_________ VSAN Cost I/F  PC
   I/F  Band
        PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
   Speed width

   ------------------------------------------------------------------------
   --------
         1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
   16g   64g
   ```

5. Wiederholen Sie das Verfahren für die zweite Switch-Struktur.

Konfigurieren Sie das VSAN neu, um die IOD oder OOD von Frames zu garantieren

Die Standard-IOD-Einstellungen werden empfohlen. Sie sollten OOD nur bei Bedarf neu konfigurieren.

IOD neu konfigurieren

Führen Sie den folgenden Schritt aus, um die IOD von Frames neu zu konfigurieren.

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   conf t
   ```

2. Ermöglichung der in-Order-Garantie für den Austausch des VSAN:

   ```
   in-order-guarantee vsan <vsan-ID>
   ```

   > Für FC-VI VSANs (FCVI_1_10 und FCVI_2_30) müssen Sie die in-Order-Garantie für Frames und Umtausche nur auf VSAN 10 aktivieren.

   a. Lastausgleich für das VSAN aktivieren:

      ```
      vsan <vsan-ID> loadbalancing src-dst-id
      ```

   b. Konfigurationsmodus beenden:

      ```
      end
      ```

   c. Kopieren Sie die Running-config auf die Startup-config:

      ```
      copy running-config startup-config
      ```

      Die Befehle zum Konfigurieren der IOD von Frames auf FC_Switch_A_1:

      ```
      FC_switch_A_1# config t
      FC_switch_A_1(config)# in-order-guarantee vsan 10
      FC_switch_A_1(config)# vsan database
      FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
      FC_switch_A_1(config-vsan-db)# end
      FC_switch_A_1# copy running-config startup-config
      ```

      Die Befehle zum Konfigurieren der IOD von Frames auf FC_Switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

OOD neu konfigurieren

Führen Sie die folgenden Schritte durch, um die OOD-Konfiguration von Frames neu zu konfigurieren.

Schritte

1. Konfigurationsmodus aufrufen:

   ```
   conf t
   ```

2. Deaktivieren der „in-order“-Garantie für den Austausch des VSAN:

   ```
   no in-order-guarantee vsan <vsan-ID>
   ```

3. Lastausgleich für das VSAN aktivieren:

   ```
   vsan <vsan-ID> loadbalancing src-dst-id
   ```

4. Konfigurationsmodus beenden:

   ```
   end
   ```

5. Kopieren Sie die Running-config auf die Startup-config:

   ```
   copy running-config startup-config
   ```

   Die Befehle zum Konfigurieren der OOD-Einstellung von Frames auf FC_Switch_A_1:

   ```
   FC_switch_A_1# config t
   FC_switch_A_1(config)# no in-order-guarantee vsan 10
   FC_switch_A_1(config)# vsan database
   FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
   FC_switch_A_1(config-vsan-db)# end
   FC_switch_A_1# copy running-config startup-config
   ```

   Die Befehle zum Konfigurieren der OOD-Einstellung von Frames auf FC_Switch_B_1:

   ```
   FC_switch_B_1# config t
   FC_switch_B_1(config)# no in-order-guarantee vsan 10
   FC_switch_B_1(config)# vsan database
   FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
   FC_switch_B_1(config-vsan-db)# end
   FC_switch_B_1# copy running-config startup-config
   ```

   Bei der Konfiguration von ONTAP auf den Controller-Modulen muss OOD explizit auf jedem Controller-Modul in der MetroCluster-Konfiguration konfiguriert sein.

"Erfahren Sie mehr über die Konfiguration von IOD oder OOD von Frames auf ONTAP Software".

Ändern Sie den Anbieter oder das Modell der FC-Switches

Möglicherweise müssen Sie den Anbieter für FC Switches von Cisco zu Brocade wechseln oder umgekehrt, das Switch-Modell ändern oder beides ändern.

Über diese Aufgabe

- Dieses Verfahren gilt, wenn Sie NetApp Validated Switches verwenden.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.
- Sie müssen die Schritte in diesem Verfahren für jeweils eine Fabric für beide Fabrics in der Konfiguration ausführen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist: **`metrocluster show`**

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

   b. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist: **`metrocluster node show`**

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

   c. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

   d. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt: **`system health alert show`**

2. Konfigurieren Sie die neuen Switches vor der Installation.

   Folgen Sie den Schritten in "Konfigurieren Sie die FC-Switches".

3. Trennen Sie die Verbindungen von den alten Schaltern, indem Sie die Verbindungen in der folgenden Reihenfolge entfernen:
   a. Trennen Sie die MetroCluster FC- und FCVI-Schnittstellen.
   b. Trennen Sie die ATTO FibreBridge-Brücken.
   c. Trennen Sie die MetroCluster-ISLs.
4. Schalten Sie die alten Schalter aus, entfernen Sie die Kabel, und ersetzen Sie die alten Schalter physisch durch den neuen Schalter.
5. Verkabeln Sie die Schalter in der folgenden Reihenfolge:

   Sie müssen die Schritte in befolgen "Verkabelung einer Fabric-Attached MetroCluster-Konfiguration".

   a. Verkabeln Sie die ISLs mit dem Remote-Standort.
   b. Verkabeln Sie die ATTO FibreBridge-Brücken.
   c. Verkabeln Sie die MetroCluster FC- und FCVI-Schnittstellen.
6. Schalten Sie die Schalter ein.
7. Wiederholen Sie die Schritte, um zu überprüfen, ob die MetroCluster-Konfiguration ordnungsgemäß ist [Schritt 1].
8. Wiederholen Sie Schritt 1 bis Schritt 7 für den zweiten Fabric in der Konfiguration.

Unterbrechungsfreier Austausch eines Shelfs in einer Fabric-Attached MetroCluster-Konfiguration

Möglicherweise müssen Sie wissen, wie ein Shelf in einer Fabric-Attached MetroCluster-Konfiguration unterbrechungsfrei ersetzt werden kann.

> Diese Vorgehensweise gilt nur für die Verwendung in einer Fabric-Attached MetroCluster-Konfiguration.

Deaktivieren des Zugriffs auf das Shelf

Sie müssen den Zugriff auf das Shelf deaktivieren, bevor Sie die Shelf-Module ersetzen.

Überprüfen Sie den Gesamtzustand der Konfiguration. Wenn das System nicht in einem ordnungsgemäßen Zustand angezeigt wird, beheben Sie zuerst das Problem, bevor Sie fortfahren.

Schritte

1. Von beiden Clustern offline sind alle Plexe mit Festplatten auf dem betroffenen Shelf-Stack:

   `aggr offline plex_name`

   Das Beispiel zeigt die Befehle zum Offline-Ausstellen von Plexen für einen Controller, auf dem ONTAP ausgeführt wird.

   ```
   cluster_A_1::> storage aggregate plex offline -aggr aggrA_1_0 -plex
   plex0
   cluster_A_1::> storage aggregate plex offline -aggr dataA_1_data -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr aggrA_2_0 -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr dataA_2_data -plex
   plex0
   ```

2. Überprüfen Sie, ob die Plexe offline sind:

   `aggr status -raggr_name`

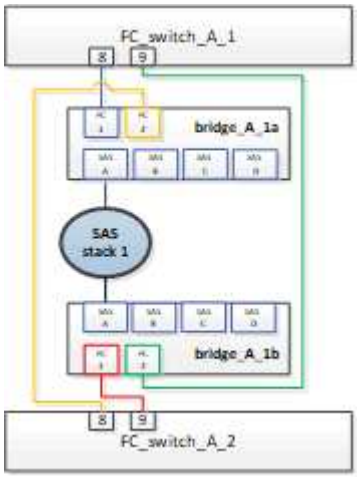
   Das Beispiel zeigt die Befehle zur Überprüfung, ob die Aggregate für einen Controller, auf dem cMode ausgeführt wird, offline sind.

   ```
   Cluster_A_1::> storage aggregate show -aggr aggrA_1_0
   Cluster_A_1::> storage aggregate show -aggr dataA_1_data
   Cluster_A_2::> storage aggregate show -aggr aggrA_2_0
   Cluster_A_2::> storage aggregate show -aggr dataA_2_data
   ```

3. Deaktivieren Sie die SAS-Ports oder Switch-Ports, je nachdem, ob die Bridges, die das Ziel-Shelf verbinden, einen einzelnen SAS-Stack oder zwei oder mehr SAS-Stacks verbinden:

- Wenn die Brücken einen einzelnen SAS-Stack anschließen, deaktivieren Sie die Switch-Ports, an die die Brücken angeschlossen sind. Verwenden Sie dazu den entsprechenden Befehl für Ihren Switch.

  Das folgende Beispiel zeigt ein Bridges-Paar, das einen einzelnen SAS-Stack mit dem Ziel-Shelf verbindet:



  Die Switch-Ports 8 und 9 an jedem Switch verbinden die Brücken mit dem Netzwerk.

  Im folgenden Beispiel sind die Ports 8 und 9 bei einem Brocade Switch deaktiviert.

```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9

FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

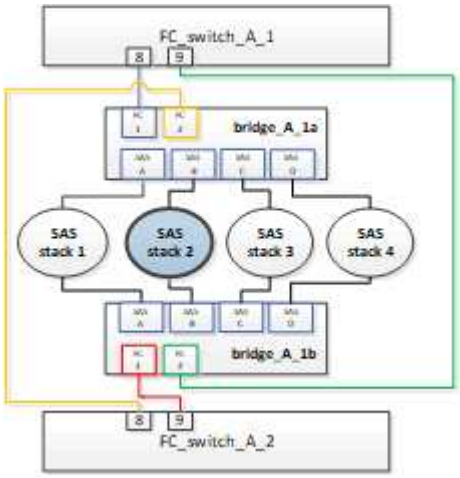
  Das folgende Beispiel zeigt, dass Port 8 und 9 auf einem Cisco Switch deaktiviert sind.

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

- Wenn die Brücken zwei oder mehr SAS-Stacks verbinden, deaktivieren Sie die SAS-Ports, die die Bridges mit dem Ziel-Shelf verbinden:

```
SASportDisable port number
```

Das folgende Beispiel zeigt ein Paar Brücken, die vier SAS-Stacks miteinander verbinden. SAS-Stack 2 enthält das Ziel-Shelf:



SAS-Port B verbindet die Brücken mit dem Ziel-Shelf. Indem nur SAS Port B auf beiden Shelves deaktiviert wird, können die anderen SAS-Stacks während des Austauschvorgangs weiterhin Daten bereitstellen.

Deaktivieren Sie in diesem Fall den SAS-Port, der die Bridge mit dem Ziel-Shelf verbindet:

```
SASportDisable port number
```

Das folgende Beispiel zeigt, dass SAS-Port B von der Bridge deaktiviert ist und dass sie ebenfalls deaktiviert ist. Sie müssen den Befehl auf beiden Brücken wiederholen.

```
Ready. *
SASPortDisable B

SAS Port B has been disabled.
```

4. Wenn Sie die Switch-Ports zuvor deaktiviert haben, vergewissern Sie sich, dass sie deaktiviert sind:

```
switchShow
```

Das Beispiel zeigt, dass die Switch-Ports bei einem Brocade Switch deaktiviert sind.

```
FC_switch_A_1:admin> switchShow
FC_switch_A_2:admin> switchShow
```

Das Beispiel zeigt, dass die Switch-Ports auf einem Cisco Switch deaktiviert sind.

```
FC_switch_A_1# show interface fc1/6
FC_switch_A_2# show interface fc1/6
```

5. Warten Sie, bis ONTAP erkennt, dass die Festplatte fehlt.
6. Schalten Sie das Shelf aus, das Sie ersetzen möchten.

Austauschen des Shelfs

Alle Kabel und das Shelf müssen physisch entfernt werden, bevor die neuen Shelf- und Shelf-Module eingesetzt und verkabelt werden.

Schritte

1. Entfernen Sie alle Festplatten, und trennen Sie alle Kabel vom zu ersetzenden Shelf.
2. Entfernen Sie die Shelf-Module.
3. Setzen Sie das neue Shelf ein.
4. Setzen Sie die neuen Festplatten in das neue Shelf ein.
5. Setzen Sie die Shelf-Module ein.
6. Verbinden Sie das Shelf (SAS oder Stromversorgung).
7. Schalten Sie das Shelf ein.

Den Zugriff erneut aktivieren und den Vorgang überprüfen

Nach dem Austausch des Shelfs müssen Sie den Zugriff erneut aktivieren und überprüfen, ob das neue Shelf ordnungsgemäß funktioniert.

Schritte

1. Überprüfen Sie, ob das Shelf ordnungsgemäß eingeschaltet wird und die Links auf den IOM-Modulen vorhanden sind.
2. Aktivieren Sie die Switch-Ports oder den SAS-Port gemäß den folgenden Szenarien:

Option	Schritt

Wenn Sie zuvor Switch-Ports deaktiviert haben	a. Aktivieren Sie die Switch-Ports:
	
	`portEnable` *`port number`*
	
	Das Beispiel zeigt, dass der Switch-Port auf einem Brocade Switch aktiviert ist.
	
	`Switch_A_1:admin> portEnable 6`
	`Switch_A_2:admin> portEnable 6`
	
	Das Beispiel zeigt, dass der Switch-Port auf einem Cisco Switch aktiviert ist.
	
	`Switch_A_1# conf t`
	`Switch_A_1(config)# int fc1/6`
	`Switch_A_1(config)# no shut`
	`Switch_A_1(config)# end`
	
	`Switch_A_2# conf t`
	`Switch_A_2(config)# int fc1/6`
	`Switch_A_2(config)# no shut`
	`Switch_A_2(config)# end`

Wenn Sie zuvor einen SAS-Port deaktiviert haben	a. Aktivieren Sie den SAS-Port, der den Stack mit dem Shelf-Speicherort verbindet:
	
	`SASportEnable` *`port number`*
	
	Das Beispiel zeigt, dass SAS-Port A von der Bridge aus aktiviert ist und ob sie aktiviert ist.
	
	`Ready. *`
	`SASPortEnable A`
	
	`SAS Port A has been enabled.`

3. Wenn Sie die Switch-Ports zuvor deaktiviert haben, vergewissern Sie sich, dass sie aktiviert und online sind und dass und alle Geräte korrekt angemeldet sind:

   `switchShow`

   Das Beispiel zeigt das `switchShow` Befehl zur Überprüfung, ob ein Brocade Switch online ist.

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

Das Beispiel zeigt das `switchShow` Befehl zur Überprüfung, ob ein Cisco Switch online ist.

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

> Nach einigen Minuten erkennt ONTAP, dass neue Festplatten eingesetzt wurden, und zeigt für jede neue Festplatte eine Meldung an.

4. Überprüfen Sie, ob die Festplatten von ONTAP erkannt wurden:

   `sysconfig -a`

5. Online die Plexe, die früher offline waren:

   `aggr online`*`plex_name`*

   Das Beispiel zeigt die Befehle, mit denen Plexe auf einen Controller platziert werden, auf dem cMode wieder online geschaltet wird.

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

   Die Plexe beginnen sich zu resynchronisieren.

> Sie können den Fortschritt der Neusynchronisierung mit dem überwachen `aggr status -`*`raggr_name`* Befehl.

Hot-Add-Storage zu einer MetroCluster-FC-Konfiguration

Hinzufügen eines SAS-Festplatten-Shelfs in einer Direct-Attached MetroCluster FC-Konfiguration mit optischen SAS-Kabeln

Sie können mit optischen SAS-Kabeln ein SAS-Platten-Shelf zu einem vorhandenen Stack von SAS-Platten-Shelfs in einer Direct-Attached MetroCluster FC-Konfiguration oder als neuer Stack zu einem SAS HBA oder einem integrierten SAS-Port am Controller hinzufügen.

- Dieser Vorgang läuft unterbrechungsfrei ab und dauert ungefähr zwei Stunden.
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.
- Informationen zum Hinzufügen eines IOM12-Shelfs zu einem Stack von IOM6-Shelfs finden Sie unter "Hot-

Adding-IOM12-Shelfs zu einem Stack mit IOM6-Shelfs".

Dieser Schritt betrifft eine MetroCluster FC-Konfiguration, in der der Storage über SAS-Kabel direkt mit den Storage Controllern verbunden ist. Dies gilt nicht für MetroCluster FC-Konfigurationen, die FC-to-SAS-Bridges oder FC-Switch-Fabrics verwenden.

Schritte

1. Befolgen Sie die Anweisungen zum Hinzufügen eines SAS-Festplatten-Shelfs im *Installation Guide*, um Ihr Festplatten-Shelf-Modell die folgenden Aufgaben auszuführen, damit Sie ein Festplatten-Shelf im laufenden Betrieb hinzufügen:
   a. Installieren Sie ein Festplatten-Shelf für eine Hot-Add-Installation.
   b. Schalten Sie die Netzteile ein und legen Sie die Shelf-ID für ein Hot-Add-On fest.
   c. Verkabeln Sie das Hot-Added Festplatten-Shelf.
   d. Überprüfen Sie die SAS-Konnektivität.

Fügen Sie bei laufendem Betrieb SAS-Storage zu einer über eine Bridge angeschlossenen MetroCluster-FC-Konfiguration hinzu

Hinzufügen eines Stacks aus SAS-Platten-Shelfs während des laufenden Betrieb zu einem vorhandenen Paar FibreBridge 7600N- oder 7500N-Bridges

Sie können einem vorhandenen Paar FibreBridge 7600N- oder 7500N-Bridges mit verfügbaren Ports im laufenden Betrieb einen Stack aus SAS-Platten-Shelfs hinzufügen.

Bevor Sie beginnen

- Sie müssen die neueste Festplatten- und Festplatten-Shelf-Firmware heruntergeladen haben.
- Auf allen Festplatten-Shelfs in der MetroCluster-Konfiguration (vorhandene Shelfs) muss dieselbe Firmware-Version ausgeführt werden. Wenn auf einer oder mehreren Festplatten oder Shelfs nicht die neueste Firmware-Version ausgeführt wird, aktualisieren Sie die Firmware, bevor Sie die neuen Festplatten oder Shelfs anschließen.

  "NetApp Downloads: Festplatten-Firmware"

  "NetApp Downloads: Festplatten-Shelf Firmware"

- Die FibreBridge 7600N- oder 7500N-Brücken müssen angeschlossen sein und über verfügbare SAS-Ports verfügen.

Über diese Aufgabe

Dieses Verfahren wird mit der Annahme geschrieben, dass Sie die empfohlenen Bridge Management-Schnittstellen verwenden: Die ATTO ExpressNAV GUI und das ATTO Quicknav Dienstprogramm.

Sie können die ATTO ExpressNAV GUI verwenden, um eine Bridge zu konfigurieren und zu verwalten und die Bridge-Firmware zu aktualisieren. Sie können das Dienstprogramm ATTO Quicknav verwenden, um den Bridge Ethernet Management 1 Port zu konfigurieren.

Bei Bedarf können Sie andere Management-Schnittstellen verwenden. Diese Optionen umfassen die Verwendung eines seriellen Ports oder Telnet zur Konfiguration und Verwaltung einer Bridge sowie zur Konfiguration des Ethernet Management 1-Ports und die Verwendung von FTP zur Aktualisierung der Bridge-Firmware. Wenn Sie eine dieser Management-Schnittstellen auswählen, müssen Sie die entsprechenden Anforderungen in erfüllen "Anderen Bridge-Managementschnittstellen".

> Wenn Sie ein SAS-Kabel in den falschen Port stecken, müssen Sie das Kabel von einem SAS-Port entfernen und mindestens 120 Sekunden warten, bevor Sie das Kabel an einen anderen SAS-Port anschließen. Wenn Sie dies nicht tun, erkennt das System nicht, dass das Kabel auf einen anderen Port verschoben wurde.

Schritte

1. Richtig gemahlen.
2. Vergewissern Sie sich an der Konsole eines der Controller, dass die automatische Zuweisung der Festplatte im System aktiviert ist:

   ```
   storage disk option show
   ```

   In der Spalte Automatische Zuweisung wird angegeben, ob die automatische Zuweisung von Laufwerken aktiviert ist.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

3. Aktivieren Sie an jeder Bridge im Paar den SAS-Port, der eine Verbindung mit dem neuen Stack herstellt:

   ```
   SASPortEnable port-letter
   ```

   Auf beiden Brücken muss derselbe SAS-Port (B, C oder D) verwendet werden.

4. Speichern Sie die Konfiguration, und starten Sie jede Bridge neu:

   ```
   SaveConfiguration Restart
   ```

5. Die Platten-Shelfs mit den Bridges verkabeln:

   a. Schalten Sie die Festplatten-Shelfs in den einzelnen Stacks in Reihe.

      Das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell bietet detaillierte Informationen zum Verketten von Platten-Shelfs in Reihe.

   b. Verkabeln Sie für jeden Stack der Festplatten-Shelfs IOM A des ersten Shelf mit SAS-Port A auf FibreBridge A und verkabeln Sie dann IOM B des letzten Shelfs mit SAS-Port A auf FibreBridge B

      "Installation und Konfiguration von Fabric-Attached MetroCluster"

      "Installation und Konfiguration von Stretch MetroCluster"

      Jede Bridge verfügt über einen Pfad zu ihrem Festplatten-Shelf. Bridge A wird über das erste Shelf mit Der A-Seite des Stacks verbunden, und Bridge B wird über das letzte Shelf mit der B-Seite des Stacks verbunden.

      > Der Bridge-SAS-Port B ist deaktiviert.

6. Überprüfen Sie, ob jede Bridge alle Festplattenlaufwerke und Festplatten-Shelfs erkennen kann, mit denen die Bridge verbunden ist.

Wenn Sie den…	Dann…
ATTO ExpressNAV GUI	a. Geben Sie in einem unterstützten Webbrowser die IP-Adresse einer Bridge in das Browserfenster ein. Sie werden auf die ATTO FibreBridge Homepage gebracht, die einen Link hat. b. Klicken Sie auf den Link, und geben Sie dann Ihren Benutzernamen und das Passwort ein, das Sie beim Konfigurieren der Bridge festgelegt haben. Die ATTO FibreBridge-Statusseite wird mit einem Menü links angezeigt. c. Klicken Sie im Menü auf **Erweitert**. d. Anzeigen der angeschlossenen Geräte: `sastargets` e. Klicken Sie Auf **Absenden**.
Serieller Anschluss	Anzeigen der angeschlossenen Geräte: `sastargets`

Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Die Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können.

> Wenn der Text “response cuted” am Anfang der Ausgabe erscheint, können Sie Telnet verwenden, um die Verbindung mit der Brücke herzustellen, und dann alle Ergebnisse mit dem anzeigen `sastargets` Befehl.

Die folgende Ausgabe zeigt, dass 10 Festplatten angeschlossen sind:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

7. Überprüfen Sie, ob in der Befehlsausgabe angezeigt wird, dass die Bridge mit allen entsprechenden Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Sie den vorherigen Schritt für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie, ob sich die SAS-Kabel lose anschließen oder korrigieren Sie die SAS-Verkabelung, indem Sie den Schritt zum Verkabeln der Platten-Shelfs mit den Bridges wiederholen. b. Wiederholen Sie den vorherigen Schritt für jede verbleibende Brücke.

8. Aktualisieren Sie die Festplatten-Firmware von der Systemkonsole auf die aktuellste Version:

   ```
   disk_fw_update
   ```

   Sie müssen diesen Befehl auf beiden Controllern ausführen.

   "NetApp Downloads: Festplatten-Firmware"

9. Aktualisieren Sie die Festplatten-Shelf-Firmware auf die aktuelle Version, indem Sie die Anweisungen für die heruntergeladene Firmware verwenden.

   Sie können die Befehle des Verfahrens über die Systemkonsole eines der beiden Controller ausführen.

   "NetApp Downloads: Festplatten-Shelf Firmware"

10. Wenn die automatische Zuweisung von Laufwerken auf Ihrem System nicht aktiviert ist, weisen Sie die Eigentumsrechte an der Festplatte zu.

    "Festplatten- und Aggregatmanagement"

    > Wenn Sie die Eigentumsrechte eines einzigen Stacks an Festplatten-Shelfs auf mehrere Controller verteilen, müssen Sie die automatische Zuweisung der Festplatte deaktivieren (`storage disk option modify -autoassign off *` Aus beiden Nodes im Cluster) vor dem Zuweisen von Festplatteneigentum. Anderenfalls werden die übrigen Festplattenlaufwerke ggf. automatisch demselben Controller und Pool zugewiesen, wenn Sie ein einzelnes Laufwerk zuweisen.

    > Sie dürfen Aggregate oder Volumes erst dann Laufwerke hinzufügen, wenn die Festplatten-Firmware und Festplatten-Shelf-Firmware aktualisiert wurden und die Verifizierungsschritte dieser Aufgabe abgeschlossen sind.

11. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
    a. Prüfen Sie, ob das System multipathed ist:

       ```
       node run -node node-name sysconfig -a
       ```

    b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

       ```
       system health alert show
       ```

c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

d. Durchführen einer MetroCluster-Prüfung:

```
metrocluster check run
```

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

f. Prüfen Sie nach dem Hinzufügen der neuen Stacks auf Integritätswarnungen auf den Bridges:

```
storage bridge show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

12. Wiederholen Sie dieses Verfahren bei Bedarf für die Partner Site.

Hot-Adding eines Stacks mit SAS-Platten-Shelves und Brücken zu einem MetroCluster System

Das MetroCluster System kann einen kompletten Stack, einschließlich Bridges, Hot-Add (unterbrechungsfrei hinzufügen) aufnehmen. An den FC-Switches müssen verfügbare Ports vorhanden sein und Sie müssen das Switch-Zoning aktualisieren, um die Änderungen widerzuspiegeln.

Über diese Aufgabe

- Dieses Verfahren kann verwendet werden, um einen Stack mit FibreBridge 7600N- oder 7500N-Brücken hinzuzufügen.
- Dieses Verfahren wird mit der Annahme geschrieben, dass Sie die empfohlenen Bridge Management-Schnittstellen verwenden: Die ATTO ExpressNAV GUI und das ATTO Quicknav Dienstprogramm.
  - Sie verwenden die ATTO ExpressNAV GUI, um eine Bridge zu konfigurieren und zu verwalten und die Bridge-Firmware zu aktualisieren. Sie verwenden das ATTO Quicknav Dienstprogramm, um den Bridge Ethernet Management 1 Port zu konfigurieren.
  - Sie können bei Bedarf andere Management-Schnittstellen verwenden. Zu diesen Optionen gehören die Verwendung eines seriellen Ports oder Telnet zur Konfiguration und Verwaltung einer Bridge sowie die Konfiguration des Ethernet-Management-1-Ports und die Verwendung von FTP zur Aktualisierung der Bridge-Firmware. Wenn Sie eine dieser Managementoberflächen auswählen, muss das System die geltenden Anforderungen in erfüllen "Anderen Bridge-Managementschnittstellen"

Vorbereitung auf den Hot-Add-Stack von SAS-Platten-Shelves und Bridges

Zum Vorbereiten eines Stacks mit SAS-Platten-Shelves und zwei Bridges müssen Dokumente sowie Festplatten- und Festplatten-Shelf-Firmware heruntergeladen werden.

Bevor Sie beginnen

- Ihr System muss eine unterstützte Konfiguration sein und eine unterstützte Version von ONTAP ausführen.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Auf allen Festplatten und Festplatten-Shelfs im System muss die neueste Firmware-Version ausgeführt werden.

  Möglicherweise möchten Sie die Festplatten- und Shelf-Firmware während der MetroCluster-Konfiguration aktualisieren, bevor Sie Shelfs hinzufügen.

  "Upgrade, Zurücksetzen oder Downgrade"

- Jeder FC-Switch muss über einen FC-Port verfügen, damit eine Bridge mit ihm verbunden werden kann.

  > Möglicherweise müssen Sie den FC Switch abhängig von der Kompatibilität mit dem FC Switch aktualisieren.

- Der Computer, den Sie zum Einrichten der Brücken verwenden, muss einen ATTO-unterstützten Webbrowser ausführen, um die ATTO ExpressNAV GUI zu nutzen: Internet Explorer 8 oder 9 oder Mozilla Firefox 3.

  Die *ATTO Product Release Notes* verfügen über eine aktuelle Liste der unterstützten Webbrowser. Sie können mithilfe der in den Schritten enthaltenen Informationen auf dieses Dokument zugreifen.

Schritte

1. Laden Sie folgende Dokumente von der NetApp Support-Website herunter oder lesen Sie sie:
   - "NetApp Interoperabilitäts-Matrix-Tool"
   - Das *Installation and Service Guide* für Ihr Festplatten-Shelf-Modell.
2. Laden Sie Inhalte von der ATTO Website und der NetApp Website herunter:
   a. Gehen Sie zur Seite ATTO FibreBridge Beschreibung.
   b. Über den Link auf der Seite ATTO FibreBridge Description können Sie auf die ATTO-Website zugreifen und Folgendes herunterladen:
      - *ATTO FibreBridge Installations- und Betriebsanleitung* für Ihr Bridge-Modell.
      - ATTO Quicknav Utility (auf den Computer, den Sie für die Einrichtung verwenden).
   c. Gehen Sie zur Seite ATTO FibreBridge Firmware Download, indem Sie auf **Continue** am Ende der ATTO FibreBridge Description-Seite klicken, und gehen Sie dann wie folgt vor:
      - Laden Sie die Bridge-Firmware-Datei gemäß den Anweisungen auf der Download-Seite herunter.

        In diesem Schritt führen Sie nur den Download-Teil der Anweisungen aus, die in den Links angegeben sind. Sie aktualisieren die Firmware auf jeder Bridge später, wenn Sie dazu im aufgefordert werden "Hot-Adding des Shelf-Stacks" Abschnitt.

      - Erstellen Sie eine Kopie der Download-Seite für die ATTO FibreBridge Firmware und den Release Notes, um sie später zu verwenden.
3. Laden Sie die neueste Festplatten- und Festplatten-Shelf-Firmware herunter und erstellen Sie eine Kopie des Installationsanteils der Anweisungen, die Sie später verwenden können.

   Auf allen Festplatten-Shelfs der MetroCluster-Konfiguration (sowohl die neuen Shelfs als auch vorhandene Shelfs) muss dieselbe Firmware-Version ausgeführt werden.

> In diesem Schritt führen Sie nur den Download-Teil der in den Links angegebenen Anweisungen aus und erstellen eine Kopie der Installationsanweisungen. Sie aktualisieren die Firmware auf jeder Festplatte und Festplatten-Shelf später, wenn Sie dazu im aufgefordert werden "Hot-Adding des Shelf-Stacks" Abschnitt.

a. Laden Sie die Festplatten-Firmware herunter, und erstellen Sie eine Kopie der Firmware-Anleitungen für die Festplatte, um sie später zu verwenden.

   "NetApp Downloads: Festplatten-Firmware"

b. Laden Sie die Festplatten-Shelf-Firmware herunter und erstellen Sie eine Kopie der Anleitungen für die Festplatten-Shelf-Firmware, um sie später zu verwenden.

   "NetApp Downloads: Festplatten-Shelf Firmware"

4. Sammeln Sie die Hardware und Informationen, die für die Verwendung der empfohlenen Bridge-Management-Schnittstellen erforderlich sind - das ATTO ExpressNAV GUI und das ATTO Quicknav Dienstprogramm:

   a. Erwerben Sie ein Standard-Ethernet-Kabel, um eine Verbindung zwischen dem Bridge Ethernet Management 1-Port und dem Netzwerk herzustellen.

   b. Legen Sie einen nicht standardmäßigen Benutzernamen und ein Kennwort für den Zugriff auf die Brücken fest.

      Es wird empfohlen, den Standardbenutzernamen und das Standardpasswort zu ändern.

   c. Ermitteln Sie eine IP-Adresse, eine Subnetzmaske und eine Gateway-Informationen für den Ethernet-Management-1-Port auf jeder Bridge.

   d. Deaktivieren Sie VPN-Clients auf dem Computer, den Sie für die Einrichtung verwenden.

      Aktive VPN-Clients führen zum Fehlschlagen des Quicknav-Scans für Brücken.

5. Nehmen Sie für jede Brücke vier Schrauben an, um die Halterungen der Brücke „`L`“ fest an der Vorderseite des Racks zu montieren.

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

6. Aktualisieren Sie bei Bedarf das FC-Switch-Zoning, um die neuen Brücken zu berücksichtigen, die der Konfiguration hinzugefügt werden.

   Wenn Sie die von NetApp zur Verfügung gestellten Referenzkonfigurationsdateien verwenden, wurden die Zonen für alle Ports erstellt, sodass keine Zoning-Updates erforderlich sind. Für jeden Switch-Port muss eine Speicherzone vorhanden sein, die mit den FC-Ports der Bridge verbunden ist.

Hot-Adding eines Stacks mit SAS-Platten-Shelfs und Bridges

Sie können einen Stack von SAS-Platten-Shelves und Bridges hinzufügen, um die Kapazität der Bridges zu erhöhen.

Das System muss alle Anforderungen erfüllen, um einen Stack von SAS-Platten-Shelves und Bridges in den laufenden Betrieb zu schaffen.

"Vorbereitung auf den Hot-Add-Stack von SAS-Platten-Shelves und Bridges"

- Das Hinzufügen eines Stacks mit SAS-Platten-Shelves und Bridges ist ein unterbrechungsfreies Verfahren, wenn alle Interoperabilitätsanforderungen erfüllt werden.

  "NetApp Interoperabilitäts-Matrix-Tool"

  "Mit dem Interoperabilitäts-Matrix-Tool finden Sie MetroCluster Informationen"

- Multipath HA ist die einzige unterstützte Konfiguration für MetroCluster Systeme, die Bridges verwenden.

  Beide Controller-Module müssen über die Brücken zu den Platten-Shelfs in jedem Stack zugreifen können.

- Sie sollten an jedem Standort die gleiche Anzahl an Platten-Shelfs hinzufügen.
- Wenn Sie die bandinterne Verwaltung der Bridge anstelle der IP-Verwaltung verwenden, können die Schritte zur Konfiguration des Ethernet-Ports und der IP-Einstellungen übersprungen werden, wie in den entsprechenden Schritten angegeben.

> 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.

> Wenn Sie ein SAS-Kabel in den falschen Port stecken, müssen Sie das Kabel von einem SAS-Port entfernen und mindestens 120 Sekunden warten, bevor Sie das Kabel an einen anderen SAS-Port anschließen. Wenn Sie dies nicht tun, erkennt das System nicht, dass das Kabel auf einen anderen Port verschoben wurde.

Schritte

1. Richtig gemahlen.
2. Prüfen Sie an der Konsole eines der Controller-Module, ob die automatische Zuweisung von Festplatte im System aktiviert ist:

   ```
   storage disk option show
   ```

   In der Spalte Automatische Zuweisung wird angegeben, ob die automatische Zuweisung von Laufwerken aktiviert ist.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

3. Deaktivieren Sie die Switch-Ports für den neuen Stack.
4. Wenn Sie für die bandinterne Verwaltung konfiguriert sind, schließen Sie ein Kabel vom seriellen FibreBridge RS-232-Port an den seriellen (COM)-Port eines PCs an.

   Die serielle Verbindung wird für die Erstkonfiguration verwendet. Anschließend können die Bridge über ONTAP in-Band-Management und die FC-Ports überwacht und verwaltet werden.

5. Bei der Konfiguration für die IP-Verwaltung konfigurieren Sie den Ethernet-Management-1-Port für jede

Bridge, indem Sie den Vorgang in Abschnitt 2.0 des *ATTO FibreBridge Installations- und Bedienungshandbuchs* für Ihr Bridge-Modell befolgen.

In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

Wenn Quicknav zum Konfigurieren eines Ethernet-Management-Ports ausgeführt wird, wird nur der über das Ethernet-Kabel verbundene Ethernet-Management-Port konfiguriert. Wenn Sie beispielsweise auch den Ethernet-Management-2-Port konfigurieren möchten, müssen Sie das Ethernet-Kabel mit Port 2 verbinden und Quicknav ausführen.

6. Konfigurieren Sie die Bridge.

   Wenn Sie die Konfigurationsinformationen von der alten Bridge abgerufen haben, konfigurieren Sie die neue Bridge mit den Informationen.

   Notieren Sie sich den von Ihnen bestimmen Benutzernamen und das Kennwort.

   Das *ATTO FibreBridge Installations- und Bedienungshandbuch* für Ihr Bridge-Modell enthält die aktuellsten Informationen zu verfügbaren Befehlen und deren Verwendung.

   > Konfigurieren Sie die Zeitsynchronisierung auf ATTO FibreBridge 7600N oder 7500N nicht. Die Zeitsynchronisierung für ATTO FibreBridge 7600N oder 7500N ist auf die Cluster-Zeit eingestellt, nachdem die Brücke von ONTAP erkannt wurde. Sie wird auch regelmäßig einmal täglich synchronisiert. Die verwendete Zeitzone ist GMT und kann nicht geändert werden.

   a. Konfigurieren Sie bei der Konfiguration für die IP-Verwaltung die IP-Einstellungen der Bridge.

      Um die IP-Adresse ohne Quicknav-Dienstprogramm einzustellen, benötigen Sie eine serielle Verbindung mit der FibreBridge.

      Bei Verwendung der CLI müssen Sie die folgenden Befehle ausführen:

      ```
      set ipaddress mp1 ip-address

      set ipsubnetmask mp1 subnet-mask

      set ipgateway mp1 x.x.x.x

      set ipdhcp mp1 disabled

      set ethernetspeed mp1 1000
      ```

   b. Konfigurieren Sie den Brückennamen.

      Die Brücken sollten in der MetroCluster-Konfiguration einen eindeutigen Namen haben.

      Beispiel für Brückennamen für eine Stapelgruppe auf jedem Standort:

      - Bridge_A_1a
      - Bridge_A_1b

- Bridge_B_1a
- Bridge_B_1b Wenn Sie die CLI verwenden, müssen Sie den folgenden Befehl ausführen:

  ```
  set bridgename bridgename
  ```

c. Wenn ONTAP 9.4 oder früher ausgeführt wird, aktivieren Sie SNMP auf der Bridge:
   ```
   set SNMP enabled
   ```

   In Systemen mit ONTAP 9.5 oder höher kann das in-Band-Management verwendet werden, um auf die Bridge über die FC-Ports statt über den Ethernet-Port zuzugreifen. Ab ONTAP 9.8 wird nur in-Band-Management unterstützt und SNMP-Management ist veraltet.

7. Konfigurieren Sie die Bridge-FC-Ports.

   a. Konfigurieren Sie die Datenrate/Geschwindigkeit der Bridge-FC-Ports.

      Die unterstützte FC-Datenrate hängt von Ihrer Modellbrücke ab.

      - Die FibreBridge 7600N unterstützt bis zu 32, 16 oder 8 Gbit/s.
      - Die FibreBridge 7500N unterstützt bis zu 16, 8 oder 4 Gbit/s.

      > Die von Ihnen ausgewählte FCDataRate-Geschwindigkeit ist auf die maximale Geschwindigkeit beschränkt, die sowohl von der Bridge als auch von dem Switch unterstützt wird, an den der Bridge-Port angeschlossen wird. Die Verkabelungsstrecken dürfen die Grenzen der SFPs und anderer Hardware nicht überschreiten.

      Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

      ```
      set FCDataRate port-number port-speed
      ```

   b. Wenn Sie eine FibreBridge 7500N-Bridge konfigurieren, konfigurieren Sie den Verbindungsmodus, den der Port für „ptp“ verwendet.

      > Die Einstellung FCConnMode ist nicht erforderlich, wenn Sie eine FibreBridge 7600N-Bridge konfigurieren.

      Bei Verwendung der CLI müssen Sie den folgenden Befehl ausführen:

      ```
      set FCConnMode port-number ptp
      ```

   a. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, müssen Sie den FC2-Port konfigurieren oder deaktivieren.
      - Wenn Sie den zweiten Port verwenden, müssen Sie die vorherigen Teilschritte für den FC2-Port wiederholen.
      - Wenn Sie den zweiten Port nicht verwenden, müssen Sie den Port: + deaktivieren
        ```
        FCPortDisable port-number
        ```

   b. Wenn Sie eine FibreBridge 7600N oder 7500N-Bridge konfigurieren, deaktivieren Sie die nicht verwendeten SAS-Ports:
      ```
      SASPortDisable sas-port
      ```

> SAS-Ports A bis D sind standardmäßig aktiviert. Sie müssen die SAS-Ports, die nicht verwendet werden, deaktivieren. Wenn nur SAS-Port A verwendet wird, müssen die SAS-Ports B, C und D deaktiviert sein.

8. Sicherer Zugriff auf die Bridge und Speicherung der Bridge-Konfiguration.

   a. Überprüfen Sie in der Eingabeaufforderung des Controllers den Status der Brücken:

      ```
      storage bridge show
      ```

      Der Ausgang zeigt an, welche Brücke nicht gesichert ist.

   b. Überprüfen Sie den Status der Ports der ungesicherten Brücke:
      `info`

      Die Ausgabe zeigt den Status der Ethernet-Ports MP1 und MP2 an.

   c. Wenn der Ethernet-Port MP1 aktiviert ist, führen Sie den folgenden Befehl aus:
      `set EthernetPort mp1 disabled`

      > Wenn auch der Ethernet-Port MP2 aktiviert ist, wiederholen Sie den vorherigen Unterschritt für Port MP2.

   d. Die Konfiguration der Bridge speichern.

      Sie müssen die folgenden Befehle ausführen:

      ```
      SaveConfiguration
      ```

      ```
      FirmwareRestart
      ```

   Sie werden aufgefordert, die Bridge neu zu starten.

9. Aktualisieren Sie die FibreBridge-Firmware auf jeder Bridge.

   Wenn die neue Bridge den gleichen Typ hat wie das Upgrade der Partnerbrücke auf die gleiche Firmware wie die Partner Bridge. Falls sich die neue Brücke von einem anderen Typ der Partnerbrücke unterscheidet, aktualisieren Sie auf die neueste Firmware, die von der Bridge und Version von ONTAP unterstützt wird. Siehe Abschnitt „Firmware auf einer FibreBridge-Brücke aktualisieren“ in *MetroCluster-Wartung*.

10. Verkabeln Sie die Platten-Shelves mit den Bridges:

    a. Schalten Sie die Festplatten-Shelfs in den einzelnen Stacks in Reihe.

       Das *Installation Guide* für Ihr Festplatten-Shelf-Modell bietet detaillierte Informationen zum Verkettung von Platten-Shelfs in Reihe.

    b. Verkabeln Sie für jeden Stack der Festplatten-Shelfs IOM A des ersten Shelf mit SAS-Port A auf FibreBridge A und verkabeln Sie dann IOM B des letzten Shelfs mit SAS-Port A auf FibreBridge B

       "Installation und Konfiguration von Fabric-Attached MetroCluster"

       "Installation und Konfiguration von Stretch MetroCluster"

Jede Bridge verfügt über einen Pfad zu ihrem Festplatten-Shelf. Bridge A wird über das erste Shelf mit Der A-Seite des Stacks verbunden, und Bridge B wird über das letzte Shelf mit der B-Seite des Stacks verbunden.

Der Bridge-SAS-Port B ist deaktiviert.

11. [[Ste11-verify-each-Bridge-Detect]]Überprüfung, dass jede Bridge alle Festplattenlaufwerke und Festplatten-Shelfs erkennen kann, mit denen die Bridge verbunden ist.

Wenn Sie den…	Dann…
ATTO ExpressNAV GUI	a. Geben Sie in einem unterstützten Webbrowser die IP-Adresse einer Bridge in das Browserfenster ein. Sie werden auf die ATTO FibreBridge Homepage gebracht, die einen Link hat. b. Klicken Sie auf den Link, und geben Sie dann Ihren Benutzernamen und das Passwort ein, das Sie beim Konfigurieren der Bridge festgelegt haben. Die ATTO FibreBridge-Statusseite wird mit einem Menü links angezeigt. c. Klicken Sie im Menü auf **Erweitert**. d. Anzeigen der angeschlossenen Geräte: `sastargets` e. Klicken Sie Auf **Absenden**.
Serieller Anschluss	Anzeigen der angeschlossenen Geräte: `sastargets`

Die Ausgabe zeigt die Geräte (Festplatten und Festplatten-Shelfs) an, mit denen die Bridge verbunden ist. Die Ausgabelinien werden nacheinander nummeriert, sodass Sie die Geräte schnell zählen können.

Wenn die abgeschnittene Textantwort zu Beginn der Ausgabe angezeigt wird, können Sie Telnet verwenden, um eine Verbindung zur Bridge herzustellen, und dann die gesamte Ausgabe über anzeigen `sastargets` Befehl.

Die folgende Ausgabe zeigt, dass 10 Festplatten angeschlossen sind:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

12. Überprüfen Sie, ob in der Befehlsausgabe angezeigt wird, dass die Bridge mit allen entsprechenden Festplatten und Festplatten-Shelfs im Stack verbunden ist.

Wenn die Ausgabe…	Dann…
Das Ist Korrekt	Wiederholen Schritt 11 Für jede verbleibende Brücke.
Nicht richtig	a. Überprüfen Sie, ob sich lose SAS-Kabel befinden oder korrigieren Sie die SAS-Verkabelung, indem Sie das Kabel wiederholt Schritt 10. b. Wiederholen Schritt 11.

13. Wenn Sie eine Fabric-Attached MetroCluster-Konfiguration konfigurieren, verkabeln Sie jede Bridge mit den lokalen FC-Switches. Verwenden Sie dabei die in der Tabelle aufgeführten Kabel für Ihre Konfiguration, das Switch-Modell und das FC-to-SAS-Bridge-Modell:

> Bei Brocade- und Cisco-Switches wird die Port-Nummerierung verwendet, wie in den folgenden Tabellen gezeigt.

- Bei Brocade Switches wird der erste Port mit „`0`“ nummeriert.
- Bei Cisco Switches wird der erste Port mit „`1`“ nummeriert.

Konfigurationen mit FibreBridge 7500N oder 7600N mit beiden FC-Ports (FC1 und FC2)											
DR-GRUPPE 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Komponente	Port	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2

Stack 1	Bridge _x_1a	FC1	8		8		8		8		10	
FC2	-	8	-	8	-	8	-	8	-	10	Bridge _x_1B	FC1
9	-	9	-	9	-	9	-	11	-	FC2	-	9
-	9	-	9	-	9	-	11	Stack 2	Bridge _x_2a	FC1	10	-
10	-	10	-	10	-	14	-	FC2	-	10	-	10
-	10	-	10	-	14	Bridge _x_2B	FC1	11	-	11	-	11
-	11	-	17	-	FC2	-	11	-	11	-	11	-
11	-	17	Stapel 3	Bridge _x_3a	FC1	12	-	12	-	12	-	12
-	18	-	FC2	-	12	-	12	-	12	-	12	-
18	Bridge _x_3B	FC1	13	-	13	-	13	-	13	-	19	-
FC2	-	13	-	13	-	13	-	13	-	19	Stapel Y	Bridge _x_ya
FC1	14	-	14	-	14	-	14	-	20	-	FC2	-
14	-	14	-	14	-	14	-	20	Bridge _x_yb	FC1	15	-
15	-	15	-	15	-	21	-	FC2		15		15

Konfigurationen mit FibreBridge 7500N oder 7600N mit beiden FC-Ports (FC1 und FC2)									
DR-GRUPPE 2									
		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G720	
Komponente	Port	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2

Stack 1	Bridge_x_51a	FC1	26	-	32	-	56	-	32	-
FC2	-	26	-	32	-	56	-	32	Bridge_x_51b	FC1
27	-	33	-	57	-	33	-	FC2	-	27
-	33	-	57	-	33	Stack 2	Bridge_x_52a	FC1	30	-
34	-	58	-	34	-	FC2	-	30	-	34
-	58	-	34	Bridge_x_52b	FC1	31	-	35	-	59
-	35	-	FC2	-	31	-	35	-	59	-
35	Stapel 3	Bridge_x_53a	FC1	32	-	36	-	60	-	36
-	FC2	-	32	-	36	-	60	-	36	Bridge_x_53b
FC1	33	-	37	-	61	-	37	-	FC2	-
33	-	37	-	61	-	37	Stapel Y	Bridge_x_5ya	FC1	34
-	38	-	62	-	38	-	FC2	-	34	-
38	-	62	-	38	Bridge_x_5yb	FC1	35	-	39	-
63	-	39	-	FC2	-	35	-	39	-	63

Konfigurationen mit FibreBridge 7500N oder 7600N mit nur einem FC-Port (FC1 oder FC2)											
DR-GRUPPE 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Komponente	Port	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2	Schalter 1	Schalter 2

Stack 1	Bridge_x_1a	8		8		8		8		10	
Bridge_x_1b	-	8	-	8	-	8	-	8	-	10	Stack 2
Bridge_x_2a	9	-	9	-	9	-	9	-	11	-	Bridge_x_2b
-	9	-	9	-	9	-	9	-	11	Stapel 3	Bridge_x_3a
10	-	10	-	10	-	10	-	14	-	Bridge_x_4b	-
10	-	10	-	10	-	10	-	14	Stapel Y	Bridge_x_ya	11
-	11	-	11	-	11	-	15	-	Bridge_x_yb	-	11

Konfigurationen mit FibreBridge 7500N oder 7600N mit nur einem FC-Port (FC1 oder FC2)									
DR-GRUPPE 2									
		Brocade G720		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520	
Stack 1	Bridge_x_51a	32	-	26	-	32	-	56	-
Bridge_x_51b	-	32	-	26	-	32	-	56	Stack 2
Bridge_x_52a	33	-	27	-	33	-	57	-	Bridge_x_52b
-	33	-	27	-	33	-	57	Stapel 3	Bridge_x_53a
34	-	30	-	34	-	58	-	Bridge_x_54b	-
34	-	30	-	34	-	58	Stapel Y	Bridge_x_ya	35

-	31	-	35	-	59	-	Bridge_x_yb	-	35

14. Wenn Sie ein MetroCluster-System mit Bridge-Verbindung konfigurieren, verkabeln Sie jede Bridge mit den Controller-Modulen:
    a. FC-Port 1 der Bridge mit einem 16-GB- oder 8-GB-FC-Port am Controller-Modul in Cluster_A verkabeln
    b. FC-Port 2 der Bridge mit demselben FC-Port mit Geschwindigkeit des Controller-Moduls in „Cluster_A“ verkabeln
    c. Wiederholen Sie diese Teilschritte auf anderen nachfolgenden Brücken, bis alle Brücken verkabelt sind.
15. Aktualisieren Sie die Festplatten-Firmware von der Systemkonsole auf die aktuellste Version:

    ```
    disk_fw_update
    ```

    Sie müssen diesen Befehl auf beiden Controller-Modulen ausführen.

    "NetApp Downloads: Festplatten-Firmware"

16. Aktualisieren Sie die Festplatten-Shelf-Firmware auf die aktuelle Version, indem Sie die Anweisungen für die heruntergeladene Firmware verwenden.

    Sie können die Befehle des Verfahrens über die Systemkonsole eines der beiden Controller-Module ausführen.

    "NetApp Downloads: Festplatten-Shelf Firmware"

17. Wenn die automatische Zuweisung von Laufwerken auf Ihrem System nicht aktiviert ist, weisen Sie die Eigentumsrechte an der Festplatte zu.

    "Festplatten- und Aggregatmanagement"

    > Wenn Sie die Eigentumsrechte eines einzigen Stacks an Festplatten-Shelfs auf mehrere Controller-Module verteilen, müssen Sie die automatische Festplattenzuweisung auf beiden Nodes im Cluster deaktivieren (`storage disk option modify -autoassign off *`) Vor der Zuweisung von Festplatteneigentum; andernfalls werden bei der Zuweisung eines einzelnen Laufwerks die übrigen Laufwerke möglicherweise automatisch demselben Controller-Modul und Pool zugewiesen.

    > Sie dürfen Aggregate oder Volumes erst dann Laufwerke hinzufügen, wenn die Festplatten-Firmware und Festplatten-Shelf-Firmware aktualisiert wurden und die Verifizierungsschritte dieser Aufgabe abgeschlossen sind.

18. Aktivieren Sie die Switch-Ports für den neuen Stack.
19. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
    a. Überprüfen Sie, ob das System multipathed ist:
    `node run -node node-name sysconfig -a`
    b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:
    `system health alert show`

c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
`metrocluster show`

d. Führen Sie eine MetroCluster-Prüfung durch:
`metrocluster check run`

e. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
`metrocluster check show`

f. Überprüfen Sie, ob auf den Switches Zustandswarnmeldungen angezeigt werden (falls vorhanden):
`storage switch show`

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

20. Wiederholen Sie dieses Verfahren bei Bedarf für die Partner Site.

Verwandte Informationen

"In-Band-Management der FC-to-SAS-Bridges"

Fügen Sie ein SAS-Platten-Shelf zu einem Stack von SAS-Platten-Shelves hinzu

Sie können ein Platten-Shelf während des laufenden Betrieb hinzufügen, wenn Sie die Storage-Kapazität erhöhen möchten, ohne die Performance zu beeinträchtigen.

Schritt 1: Bereiten Sie das Hot-Add eines SAS-Platten-Shelfs vor

Um das Hot-Hinzufügen eines SAS-Platten-Shelfs vorzubereiten, müssen Sie Dokumente sowie die Festplatten- und Festplatten-Shelf-Firmware herunterladen.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihr System eine unterstützte Konfiguration ist und eine unterstützte Version von ONTAP ausführt.
- Überprüfen Sie, ob auf allen Festplattenlaufwerken und Festplatten-Shelfs im System die neueste Firmware-Version ausgeführt wird.

  Möglicherweise möchten Sie die Festplatten- und Shelf-Firmware in der gesamten MetroCluster Konfiguration aktualisieren, bevor Sie Shelfs hinzufügen.

  "Upgrade, Zurücksetzen oder Downgrade"

> Eine Kombination aus IOM12-Modulen und IOM6-Modulen wird im selben Stack unterstützt, wenn auf Ihrem System eine unterstützte ONTAP-Version ausgeführt wird. Informationen darüber, ob Ihre ONTAP-Version Shelf-Mischen unterstützt, finden Sie im "Interoperabilitäts-Matrix-Tool (IMT)". Wenn Ihre Version von ONTAP nicht unterstützt wird und Sie die IOM-Module im vorhandenen Stack oder das neue Shelf, das einer unterstützten Kombination von IOM-Modulen hinzugefügt werden soll, nicht aktualisieren oder herunterstufen können, müssen Sie einen der folgenden Schritte durchführen:
>
> - Starten eines neuen Stacks auf einem neuen SAS-Port (sofern vom Bridge-Paar unterstützt)
> - Starten Sie einen neuen Stack auf einem weiteren Brückenpaar.

Schritte

1. Laden Sie folgende Dokumente von der NetApp Support-Website herunter oder lesen Sie sie:
   - "Interoperabilitäts-Matrix-Tool"
   - Das *Installation Guide* für Ihr Festplatten-Shelf-Modell.
2. Überprüfen Sie, ob das Festplatten-Shelf, das Sie hinzufügen, unterstützt wird.

   "Interoperabilitäts-Matrix-Tool"

3. Laden Sie die neueste Festplatten- und Festplatten-Shelf-Firmware herunter:

   > In diesem Schritt schließen Sie nur den Download-Teil der Anweisungen ab. Sie müssen die Schritte in befolgenFügen Sie während des laufenden Betrieb ein Platten-Shelf hinzu, um das Festplatten-Shelf zu installieren.

   a. Laden Sie die Festplatten-Firmware herunter, und erstellen Sie eine Kopie der Firmware-Anleitungen für die Festplatte, um sie später zu verwenden.

      "NetApp Downloads: Festplatten-Firmware"

   b. Laden Sie die Festplatten-Shelf-Firmware herunter und erstellen Sie eine Kopie der Anleitungen für die Festplatten-Shelf-Firmware, um sie später zu verwenden.

      "NetApp Downloads: Festplatten-Shelf Firmware"

Schritt 2: Hinzufügen eines Festplatten-Shelfs während des laufenden Betrieb

Gehen Sie wie folgt vor, um einem Stack im laufenden Betrieb ein Festplatten-Shelf hinzuzufügen.

Bevor Sie beginnen

- Überprüfen Sie, ob das System alle Anforderungen in erfülltBereiten Sie das Hot-Add von SAS-Platten-Shelves vor.
- Vergewissern Sie sich, dass Ihre Umgebung eines der folgenden Szenarien erfüllt, bevor Sie ein Shelf während des laufenden Betrieb hinzufügen:
  - Sie haben zwei FibreBridge 7500N-Bridges mit einem Stack von SAS-Platten-Shelves verbunden.
  - Zwei FibreBridge 7600N-Bridges sind mit einem Stack aus SAS-Platten-Shelfs verbunden.
  - Sie verfügen über eine FibreBridge 7500N und eine FibreBridge 7600N, die mit einem Stack aus SAS-Platten-Shelfs verbunden ist.

Über diese Aufgabe

- Dieses Verfahren dient zum Hinzufügen eines Festplatten-Shelfs zum letzten Festplatten-Shelf im Stack.

  Dieses Verfahren setzt die Annahme ein, dass das letzte Festplatten-Shelf eines Stacks von IOM A mit der Bridge A und von IOM B zu Bridge B verbunden ist

- Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.
- Sie sollten an jedem Standort die gleiche Anzahl an Platten-Shelfs hinzufügen.
- Wenn Sie mehrere Festplatten-Shelfs im laufenden Betrieb hinzufügen, müssen Sie ein Festplatten-Shelf gleichzeitig im laufenden Betrieb hinzufügen.

  Jedes Paar Brücken FibreBridge 7500N oder 7600N kann bis zu vier Stapel unterstützen.

> Zum Hot-Hinzufügen eines Festplatten-Shelfs müssen Sie die Festplatten-Firmware auf dem Hot-Added Disk Shelf aktualisieren, indem Sie die ausführen `storage disk firmware update` Befehl im erweiterten Modus. Diese Ausführung dieses Befehls kann den Betrieb unterbrechen, wenn die Firmware auf vorhandenen Festplattenlaufwerken im System eine ältere Version ist.
>
> Falls Sie ein SAS-Kabel an den falschen Port anschließen, müssen Sie nach dem Abziehen des Kabels von einem SAS-Port mindestens 120 Sekunden warten, bevor Sie das Kabel an einen anderen SAS-Port anschließen. Wenn Sie dies nicht tun, erkennt das System nicht, dass Sie das Kabel an einen anderen Port verlegt haben.

Schritte

1. Richtig gemahlen.
2. Überprüfen Sie die Festplatten-Shelf-Konnektivität von der Systemkonsole eines Controllers:

   ```
   sysconfig -v
   ```

   Die Ausgabe ähnelt der folgenden Ausgabe:

   - Jede Bridge in einer separaten Zeile und unter jedem FC-Port, zu dem sie sichtbar ist, führt zum Beispiel: Wenn ein Platten-Shelf zu einer Reihe von FibreBridge 7500N-Bridges hinzugefügt wird, ergibt dies folgende Ausgabe:

     ```
     FC-to-SAS Bridge:
     cisco_A_1-1:9.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100189
     cisco_A_1-2:1.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100162
     ```

   - Jedes Festplatten-Shelf in einer separaten Zeile unter jedem FC-Port, zu dem es sichtbar ist:

     ```
     Shelf   0: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     Shelf   1: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     ```

   - Jedes Laufwerk in einer separaten Zeile unter jedem FC-Port, zu dem es sichtbar ist:

```
cisco_A_1-1:9.126L1   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
cisco_A_1-1:9.126L2   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
(879097968 520B/sect)
```

3. Überprüfen Sie, ob die automatische Festplattenzuordnung im System von der Konsole eines der Controller aktiviert ist:

   `storage disk option show`

   Die Richtlinie für die automatische Zuweisung wird in der Spalte „Automatische Zuweisung“ angezeigt.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

4. Wenn die automatische Festplattenzuordnung im System nicht aktiviert ist oder Festplattenlaufwerke im selben Stack zu beiden Controllern gehören, weisen Sie den entsprechenden Pools Festplattenlaufwerke zu.

   "Festplatten- und Aggregatmanagement"

   - Wenn Sie einen einzelnen Stack an Platten-Shelfs auf zwei Controller aufteilen, muss die automatische Zuweisung einer Festplatte vor der Zuweisung der Festplatteneigentümer deaktiviert werden. Andernfalls werden die verbleibenden Festplatten beim Zuweisen eines einzelnen Festplattenlaufwerks möglicherweise automatisch demselben Controller und Pool zugewiesen.

     Der `storage disk option modify -node <node-name> -autoassign off` Befehl deaktiviert die automatische Zuweisung von Festplatten.

   - Sie können erst dann Laufwerke zu Aggregaten oder Volumes hinzufügen, nachdem Sie die Festplatten- und Festplatten-Shelf-Firmware aktualisiert haben.

5. Aktualisieren Sie die Festplatten-Shelf-Firmware auf die aktuelle Version, indem Sie die Anweisungen für die heruntergeladene Firmware verwenden.

   Sie können die Befehle des Verfahrens über die Systemkonsole eines der beiden Controller ausführen.

   "NetApp Downloads: Festplatten-Shelf Firmware"

6. Installieren und verkabeln Sie das Festplatten-Shelf:

> Erzwingen Sie keinen Anschluss in einen Port. Die Mini-SAS-Kabel sind codiert; wenn sie korrekt in einen SAS-Port ausgerichtet sind, klickt das SAS-Kabel an ihre Stelle und die Festplatten-Shelf-SAS-Port LNK LED leuchtet grün.für Platten-Shelves setzen Sie einen SAS-Kabelanschluss ein, wobei die Zuglasche nach oben (auf der Oberseite des Anschlusses) ausgerichtet ist.

a. Installieren Sie das Festplatten-Shelf, schalten Sie es ein und legen Sie die Shelf-ID fest.

   Das *Installation Guide* für Ihr Festplatten-Shelf-Modell enthält detaillierte Informationen zur Installation von Festplatten-Shelfs.

   > Sie müssen das Festplatten-Shelf aus- und wieder einschalten und die Shelf-IDs für jedes SAS-Festplatten-Shelf innerhalb des gesamten Storage-Systems eindeutig aufbewahren.

b. Trennen Sie das SAS-Kabel vom Port IOM B des letzten Shelfs im Stack, und schließen Sie es dann wieder an den gleichen Port im neuen Shelf an.

   Das andere Ende dieses Kabels bleibt mit Brücke B. verbunden

c. Schalten Sie das neue Festplatten-Shelf in Reihe, indem Sie die neuen Shelf-IOM-Ports (von IOM A und IOM B) mit den letzten Shelf-IOM-Ports (von IOM A und IOM B) verkabeln.

Das *Installation Guide* für Ihr Festplatten-Shelf-Modell bietet detaillierte Informationen zum Verkettung von Platten-Shelfs in Reihe.

7. Aktualisieren Sie die Festplatten-Firmware von der Systemkonsole auf die aktuellste Version.

   "NetApp Downloads: Festplatten-Firmware"

   a. Wechseln Sie zur erweiterten Berechtigungsebene:
      `set -privilege advanced`

      Sie müssen mit reagieren **`y`** Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*>) anzuzeigen.

   b. Aktualisieren Sie die Festplatten-Firmware von der Systemkonsole aus auf die aktuellste Version:
      `storage disk firmware update`

   c. Zurück zur Administrator-Berechtigungsebene:
      `set -privilege admin`

   d. Wiederholen Sie die vorherigen Unterschritte auf dem anderen Controller.

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

   a. Prüfen Sie, ob das System multipathed ist:

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

   b. Überprüfen Sie auf beiden Clustern auf alle Zustandswarnmeldungen:
      `system health alert show`

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
      `metrocluster show`

d. Führen Sie eine MetroCluster-Prüfung durch:
   `metrocluster check run`

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

   ```
   storage switch show
   ```

g. Führen Sie Active IQ Config Advisor aus.

   "NetApp Downloads: Config Advisor"

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

9. Wenn Sie beim Hinzufügen von mehr als einem Festplatten-Shelf während des laufenden Betrieb die vorherigen Schritte für jedes Festplatten-Shelf wiederholen, das Sie Hot-hinzufügen.

Hot-Adding eines IOM12-Platten-Shelf zu einem Stack von IOM6-Platten-Shelfs in einer Bridge-Attached MetroCluster-Konfiguration

Je nach Ihrer Version von ONTAP können Sie in einer über die Bridge angeschlossenen MetroCluster-Konfiguration ein IOM12 Festplatten-Shelf zu einem Stack mit IOM6-Platten-Shelfs hinzufügen.

Informationen zum Ausführen dieses Verfahrens finden Sie unter "Hot-Adding-Shelfs mit IOM12-Modulen werden in einem Shelf-Stack mit IOM6-Modulen ausgeführt".

Hot-Removing Storage aus einer MetroCluster FC-Konfiguration

Sie können Laufwerk-Shelfs in Betrieb nehmen – physische Shelfs entfernen, bei denen die Aggregate von den Laufwerken entfernt wurden – von einer MetroCluster FC-Konfiguration, die Daten bereitstellt. Sie können ein oder mehrere Shelfs innerhalb eines Shelfs im laufenden Betrieb entfernen oder einen Shelf-Stack entfernen.

- Ihr System muss eine Multipath HA-, Multipath-, Quad-Path-Konfiguration oder Quad-Path-Konfiguration sein.
- In einer MetroCluster FC-Konfiguration mit vier Nodes kann sich das lokale HA-Paar nicht in einem Takeover-Status befinden.
- Sie müssen bereits alle Aggregate aus den Laufwerken in den Shelves entfernt haben, die Sie entfernen.

> Wenn Sie versuchen, dieses Verfahren bei Konfigurationen ohne MetroCluster FC mit Aggregaten auf dem Shelf zu entfernen, können Sie dazu führen, dass das System mit mehreren Laufwerkpanik ausfällt.

Das Entfernen von Aggregaten beinhaltet das Aufteilen der gespiegelten Aggregate auf den Shelves, die Sie entfernen, und anschließende Neuerstellen der gespiegelten Aggregate mit einem anderen Satz an Laufwerken.

"Festplatten- und Aggregatmanagement"

- Nachdem Sie die Aggregate aus den Laufwerken in den Shelfs entfernt haben, müssen Sie die Laufwerkeigentümer entfernt haben.

  "Festplatten- und Aggregatmanagement"

- Wenn Sie ein oder mehrere Shelfs aus einem Stack entfernen, müssen Sie die Entfernung berücksichtigt haben, um die entfernenden Shelfs zu umgehen.

  Wenn die aktuellen Kabel nicht lang genug sind, müssen Sie längere Kabel zur Verfügung haben.

Dieser Task gilt für die folgenden MetroCluster FC-Konfigurationen:

- Direct-Attached MetroCluster FC-Konfigurationen, in denen die Storage Shelfs direkt über SAS-Kabel mit den Storage Controllern verbunden sind
- Fabric-Attached- oder Bridge-Attached MetroCluster-FC-Konfigurationen, bei denen Storage-Shelfs über FC-to-SAS-Bridges verbunden werden

Schritte

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

   a. Überprüfen Sie, ob das System multipathed ist:
   node run -node *node-name* sysconfig -a

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

   ```
   system health alert show
   ```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
   metrocluster show

   d. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

   ```
   storage switch show
   ```

   g. Nutzen Sie Config Advisor.

   "NetApp Downloads: Config Advisor"

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

2. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

3. Vergewissern Sie sich, dass sich kein Postfachlaufwerk in den Regalen befindet:
   storage failover mailbox-disk show

4. Entfernen Sie das Regal gemäß den Schritten für das jeweilige Szenario.

Szenario	Schritte
Zur Entfernung eines Aggregats, wenn das Shelf entweder nicht gespiegelt, gespiegelt oder beide Typen von Aggregat enthält…	a. Verwenden Sie die `storage aggregate delete -aggregate` *`aggregate name`* Befehl zum Entfernen des Aggregats. b. Verwenden Sie das Standardverfahren, um die Eigentümerschaft aller Laufwerke im Shelf zu entfernen und dann das Shelf physisch zu entfernen. Folgen Sie den Anweisungen im *SAS Disk Shelfs Service Guide*, um Shelfs beim Hot-remove-Modell zu entfernen.

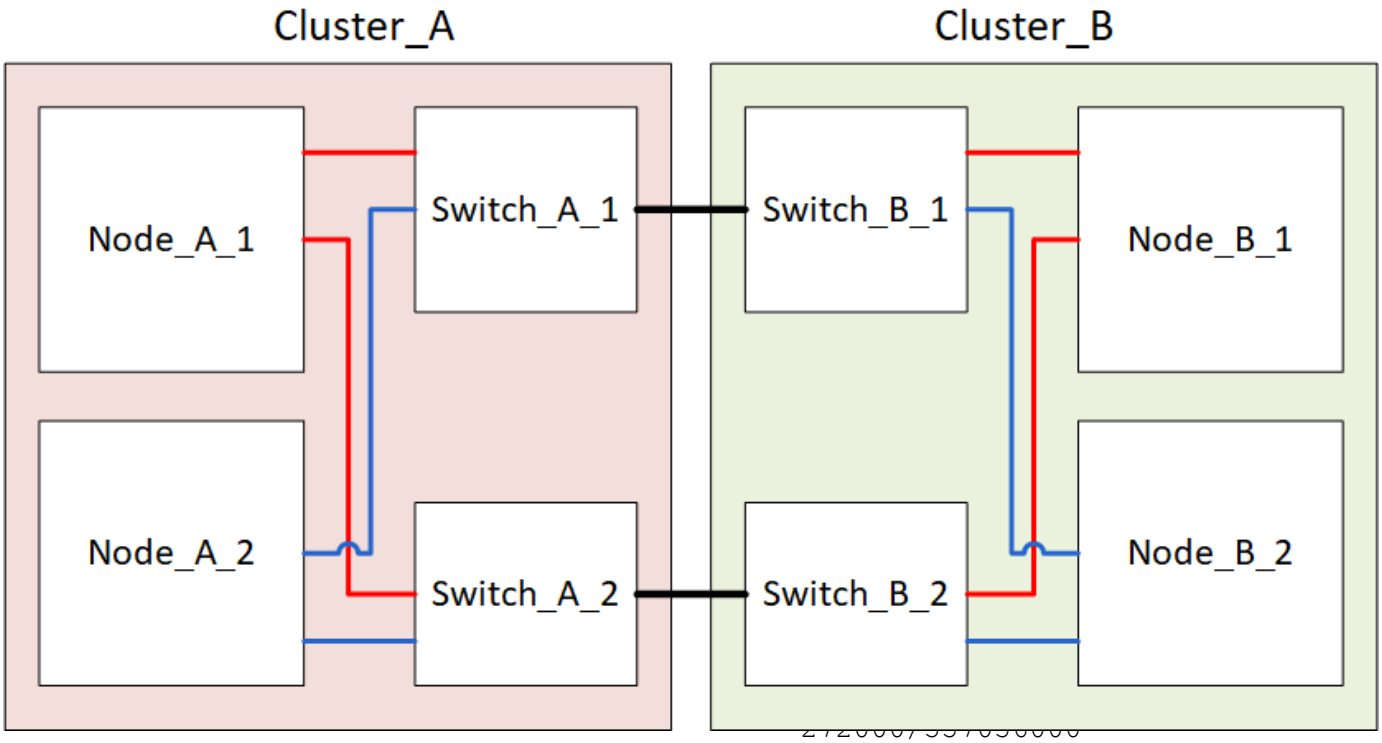
Um einen Plex aus einem gespiegelten Aggregat zu entfernen, müssen Sie das Aggregat unspiegeln.	a. Identifizieren Sie den Plex, den Sie entfernen möchten, indem Sie den verwenden `run -node local sysconfig -r` Befehl.
	
	Im folgenden Beispiel können Sie den Plex aus der Zeile identifizieren `Plex /dpg_mcc_8020_13_a1_aggr1/plex0`. In diesem Fall ist der zu angegebene Plex „ `plex0`“.
	
	``
	dpgmcc_8020_13_a1a2::storage aggregate> run -node local sysconfig -r
	*** This system has taken over dpg-mcc-8020-13-a1
	Aggregate dpg_mcc_8020_13_a1_aggr1 (online, raid_dp, mirrored) (block checksums)
	  Plex /dpg_mcc_8020_13_a1_aggr1/plex0 (online, normal, active, pool0)
	  RAID group /dpg_mcc_8020_13_a1_aggr1/plex0/rg0 (normal, block checksums)
	  RAID Disk Device HA SHELF BAY CHAN Pool Type RPM Used (MB/blks) Phys (MB/blks)
	  --------- ------ ------------- ---- ---- ---- ----- -------------- --------------
	  dparity mcc-cisco-8Gb-fab-2:1-1.126L16 0c 32 15 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	  parity mcc-cisco-8Gb-fab-2:1-1.126L18 0c 32 17 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	  data mcc-cisco-8Gb-fab-2:1-1.126L19 0c 32 18 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	``
	
	1033

Schalten Sie einen einzelnen Standort in einer MetroCluster FC-Konfiguration aus und wieder ein

Wenn Sie eine Standortwartung durchführen oder einen einzelnen Standort in einer MetroCluster FC-Konfiguration verlagern müssen, müssen Sie wissen, wie Sie den Standort ausschalten und einschalten müssen.

Wenn Sie einen Standort verschieben und neu konfigurieren müssen (wenn Sie z. B. von einem Cluster mit vier Nodes auf ein Cluster mit acht Nodes erweitern müssen), können diese Aufgaben nicht gleichzeitig ausgeführt werden. Dieser Vorgang deckt nur die Schritte ab, die zur Durchführung von Wartungsarbeiten am Standort oder zum Standortwechsel ohne Änderung der Konfiguration erforderlich sind.

Das folgende Diagramm zeigt eine MetroCluster-Konfiguration. Cluster_B wird aus Wartungszwecken ausgeschaltet.



Schalten Sie einen MetroCluster-Standort aus

Sie müssen einen Standort und die gesamte Ausrüstung abschalten, bevor die Wartung oder der Standortwechsel beginnen können.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von dem Standort ausgegeben, der weiterhin eingeschaltet bleibt.

Schritte

1. Bevor Sie beginnen, überprüfen Sie, ob alle nicht gespiegelten Aggregate am Standort offline sind.
2. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      ```
      node run -node node-name sysconfig -a
      ```

b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

```
system health alert show
```

c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

d. Führen Sie eine MetroCluster-Prüfung durch:
```
metrocluster check run
```

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

3. Implementieren Sie von dem Standort aus, an dem Sie weiterhin arbeiten möchten, die Umschaltung:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Der Vorgang kann einige Minuten dauern.

Die nicht gespiegelten Aggregate sind erst nach einem Switchover online, wenn die Remote-Festplatten im Aggregat zugänglich sind. Wenn die ISLs ausfallen, kann der lokale Node möglicherweise nicht auf die Daten auf den nicht gespiegelten Remote-Festplatten zugreifen. Der Ausfall eines Aggregats kann zu einem Neustart des lokalen Node führen.

4. Überwachen und überprüfen Sie den Abschluss der Umschaltung:

```
metrocluster operation show
```

```
fab3:1-1.126L45  0d    34  18
FC:A   1   SAS 15000
272000/557056000
280104/573653840
```

b. Verwenden Sie die `storage aggregate plex delete -aggregate` *`aggr_name`* `-plex` *`plex_name`* Befehl zum Entfernen des Plex.

plex definiert den Plex-Namen, z. B. „`plex3`“ oder „`plex6`“.

c. Verwenden Sie das Standardverfahren, um die Eigentümerschaft aller Laufwerke im Shelf zu entfernen und dann das Shelf physisch zu entfernen.

Folgen Sie den Anweisungen im *SAS Disk Shelfs Service Guide*, um Shelfs beim Hot-remove-Modell zu entfernen.

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Verschieben Sie alle Volumes und LUNs, die zu nicht gespiegelten Aggregaten gehören, offline.
   a. Verschieben Sie die Volumes in den Offline-Modus.

      ```
      cluster_A::* volume offline <volume name>
      ```

   b. Verschieben Sie die LUNs in den Offline-Modus.

      ```
      cluster_A::* lun offline lun_path <lun_path>
      ```

6. Nicht gespiegelte Aggregate lassen sich offline verschieben: `storage aggregate offline`

   ```
   cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
   ```

7. Identifizieren und verschieben Sie je nach Konfiguration und ONTAP-Version die betroffenen Plexe, die sich am Disaster-Standort (Cluster_B) befinden, offline.

   Sie sollten die folgenden Plexe offline verschieben:

   - Nicht gespiegelte Plexe befinden sich auf Festplatten am DR-Standort.

     Wenn Sie die nicht gespiegelten Plexe am Disaster-Standort nicht offline schalten, kann es zu einem Ausfall kommen, wenn der Disaster-Standort später ausgeschaltet wird.

   - Gespiegelte Plexe auf Festplatten am Disaster Site zur Aggregatspiegelung Nachdem sie offline verschoben wurden, sind die Plexe nicht mehr zugänglich.

   a. Identifizieren Sie die betroffenen Plexe.

      Plexe, die Nodes auf dem verbleibenden Platz gehören, bestehen aus Pool1-Festplatten. Plexe, die im Eigentum von Nodes am Disaster-Site sind, bestehen aus Pool0-Platten.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

Die betroffenen Plexe sind diejenigen, die Remote zu Cluster A sind In der folgenden Tabelle wird gezeigt, ob die Festplatten lokal oder Remote relativ zu Cluster A sind:

Knoten	Disks im Pool	Sollten die Festplatten offline geschaltet werden?	Beispiel für Plexe, die offline verschoben werden sollen
Node_A_1 und Node_A_2	Laufwerke im Pool 0	Nein Festplatten sind lokal für Cluster A	-

Festplatten in Pool 1	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Node _B_1 und Node _B_2
Laufwerke im Pool 0	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Festplatten in Pool 1

b. Verschieben Sie die betroffenen Plexe offline:

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

> Führen Sie diesen Schritt für alle Plexe aus, die über Remote-Festplatten für Cluster_A verfügen

8. Die ISL-Switch-Ports werden je nach Switch-Typ permanent offline geschaltet.

Switch-Typ	Aktion

Für Brocade FC Switches…	a. Verwenden Sie die `portcfgpersistentdisable <port>` Befehl zum Persistenz-Deaktivieren der Ports, wie im folgenden Beispiel dargestellt. Dies muss an beiden Schaltern am überlebenden Standort erfolgen.
	
	`Switch_A_1:admin> portcfgpersistentdisable 14`
	`Switch_A_1:admin> portcfgpersistentdisable 15`
	`Switch_A_1:admin>`
	
	b. Vergewissern Sie sich, dass die Ports mit deaktiviert sind `switchshow` Befehl, der im folgenden Beispiel angezeigt wird:
	
	`Switch_A_1:admin> switchshow`
	`switchName:  Switch_A_1`
	`switchType:  109.1`
	`switchState:  Online`
	`switchMode:  Native`
	`switchRole:  Principal`
	`switchDomain:  2`
	`switchId:  fffc02`
	`switchWwn: 10:00:00:05:33:88:9c:68`
	`zoning:  ON (T5_T6)`
	`switchBeacon:  OFF`
	`FC Router: OFF`
	`FC Router BB Fabric ID:  128`
	`Address Mode:  0`
	
	`Index Port Address Media Speed State  Proto`
	`==========`
	`...`
	`14  14  020e00  id  16G  No_Light  FC Disabled (Persistent)`
	`15  15  020f00  id  16G  No_Light  FC Disabled (Persistent)`
	`...`
	`Switch_A_1:admin>`

Für Cisco FC Switches…	a. Verwenden Sie die `interface` Befehl zum Persistenz Deaktivieren der Ports. Im folgenden Beispiel werden die Ports 14 und 15 deaktiviert:
	
	`Switch_A_1# conf t`
	`Switch_A_1(config)# interface fc1/14-15`
	`Switch_A_1(config)# shut`
	
	`Switch_A_1(config-if)# end`
	`Switch_A_1# copy running-config startup-config`
	
	b. Vergewissern Sie sich, dass der Switch-Port mithilfe des deaktiviert ist `show interface brief` Befehl wie im folgenden Beispiel dargestellt:
	
	`Switch_A_1# show interface brief`
	`Switch_A_1`

9. Schalten Sie die Geräte am DR-Standort aus.

   Folgende Geräte müssen in der angegebenen Reihenfolge ausgeschaltet werden:

   - Speicher-Controller: Die Speicher-Controller sollten sich derzeit am befinden `LOADER` Sie müssen sie vollständig ausschalten.
   - MetroCluster FC-Switches
   - ATTO FibreBridges (falls vorhanden)
   - Storage Shelfs

Verlagerung des ausgeschalteten Standorts des MetroCluster

Nachdem der Standort ausgeschaltet ist, können Sie mit der Wartung beginnen. Das Verfahren ist dasselbe, ob die MetroCluster Komponenten innerhalb desselben Datacenters verlegt oder in ein anderes Datacenter verlagert werden.

- Die Hardware sollte auf die gleiche Weise wie der vorherige Standort verkabelt werden.
- Wenn sich die Geschwindigkeit, Länge oder Zahl der Inter-Switch-Verbindung (ISL) geändert hat, müssen alle neu konfiguriert werden.

Schritte

1. Vergewissern Sie sich, dass die Verkabelung aller Komponenten sorgfältig aufgezeichnet wurde, damit sie am neuen Standort wieder richtig angeschlossen werden kann.
2. Physische Verlagerung der gesamten Hardware, Storage-Controller, FC-Switches, FibreBridges und Storage Shelfs
3. Konfiguration der ISL-Ports und Überprüfung der Konnektivität zwischen Standorten

   a. Schalten Sie die FC-Switches ein.

Schalten Sie keine anderen Geräte ein.

b. Aktivieren Sie die Ports.

Aktivieren Sie die Ports entsprechend den richtigen Switch-Typen in der folgenden Tabelle:

Switch-Typ	Befehl

Für Brocade FC Switches…	i. Verwenden Sie die `portcfgpersistentenable <port number>` Befehl zum Persistenz-Aktivieren des Ports. Dies muss an beiden Schaltern am überlebenden Standort erfolgen. Im folgenden Beispiel werden die Ports 14 und 15 bei Switch_A_1 aktiviert. ``` switch_A_1:admin> portcfgpersistentenable 14 switch_A_1:admin> portcfgpersistentenable 15 switch_A_1:admin> ``` ii. Vergewissern Sie sich, dass der Switch-Port aktiviert ist: `switchshow` Im folgenden Beispiel werden die Ports 14 und 15 aktiviert: ``` switch_A_1:admin> switchshow switchName: Switch_A_1 switchType: 109.1 switchState: Online switchMode: Native switchRole: Principal switchDomain: 2 switchId: fffc02 switchWwn: 10:00:00:05:33:88:9c:68 zoning: ON (T5_T6) switchBeacon: OFF FC Router: OFF FC Router BB Fabric ID: 128 Address Mode: 0 Index Port Address Media Speed State Proto == ==== ... 14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" 15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream) ... switch_A_1:admin> ``` 1042

Für Cisco FC Switches…	i. Geben Sie das ein `interface` Befehl zum Aktivieren des Ports.
	
	Im folgenden Beispiel werden die Ports 14 und 15 bei Switch_A_1 aktiviert.
	
	`switch_A_1# conf t`
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# no shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	ii. Vergewissern Sie sich, dass der Switch-Port aktiviert ist: `show interface brief`
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

4. Überprüfen Sie mithilfe von Tools auf den Switches (wie sie verfügbar sind) die Verbindung zwischen den Standorten.

   Sie sollten nur fortfahren, wenn die Links korrekt konfiguriert und stabil sind.

5. Deaktivieren Sie die Links erneut, wenn sie stabil sind.

   Deaktivieren Sie die Ports basierend darauf, ob Sie Brocade- oder Cisco-Switches wie in der folgenden Tabelle dargestellt verwenden:

Switch-Typ	Befehl

Für Brocade FC Switches…	a. Geben Sie das ein `portcfgpersistentdisable <port_number>` Befehl zum Persistenz-Deaktivieren des Ports.
	
	Dies muss an beiden Schaltern am überlebenden Standort erfolgen. Im folgenden Beispiel werden die Ports 14 und 15 bei Switch_A_1 deaktiviert:
	
	`switch_A_1:admin> portpersistentdisable 14`
	`switch_A_1:admin> portpersistentdisable 15`
	`switch_A_1:admin>`
	
	b. Vergewissern Sie sich, dass der Switch-Port deaktiviert ist: `switchshow`
	
	Im folgenden Beispiel werden die Ports 14 und 15 deaktiviert:
	
	`switch_A_1:admin> switchshow`
	`switchName: Switch_A_1`
	`switchType: 109.1`
	`switchState:  Online`
	`switchMode: Native`
	`switchRole: Principal`
	`switchDomain:  2`
	`switchId:  fffc02`
	`switchWwn:  10:00:00:05:33:88:9c:68`
	`zoning:  ON (T5_T6)`
	`switchBeacon:  OFF`
	`FC Router:  OFF`
	`FC Router BB Fabric ID: 128`
	`Address Mode:  0`
	
	`Index Port Address Media Speed State Proto`
	`==========`
	`...`
	`14  14  020e00  id  16G  No_Light FC  Disabled (Persistent)`
	`15  15  020f00  id  16G  No_Light FC  Disabled (Persistent)`
	`...`
	`switch_A_1:admin>`

Für Cisco FC Switches…	a. Deaktivieren Sie den Port mithilfe des `interface` Befehl.
	
	Im folgenden Beispiel werden die Ports fc1/14 und fc1/15 auf Switch A_1 deaktiviert:
	
	`switch_A_1# conf t`
	
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Vergewissern Sie sich, dass der Switch-Port mithilfe des deaktiviert ist `show interface brief` Befehl.
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

Einschalten der MetroCluster-Konfiguration und Zurückkehren zum normalen Betrieb

Nach Abschluss der Wartung oder Verschieben des Standorts müssen Sie den Standort einschalten und die MetroCluster Konfiguration wiederherstellen.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von der Website ausgegeben, die Sie einschalten.

Schritte

1. Schalten Sie die Schalter ein.

   Schalten Sie die Schalter zuerst ein. Möglicherweise wurden sie im vorherigen Schritt eingeschaltet, wenn der Standort verlegt wurde.

   a. Konfigurieren Sie den Inter-Switch Link (ISL), falls erforderlich, oder falls dieser nicht Teil der Verschiebung abgeschlossen wurde.
   b. ISL aktivieren, falls Fechten abgeschlossen wurde.
   c. ISL überprüfen.
2. Deaktivieren Sie die ISLs auf den FC-Switches.
3. Schalten Sie die Shelfs ein und geben Sie ihnen genügend Zeit, vollständig eingeschaltet zu werden.
4. Die FibreBridge-Brücken mit Strom versorgen.
   a. Vergewissern Sie sich bei den FC-Switches, dass die Ports, die die Brücken verbinden, online geschaltet werden.

      Sie können z. B. einen Befehl verwenden `switchshow` Für Brocade Switches und `show interface`

`brief` Für Cisco Switches.

b. Stellen Sie sicher, dass die Regale und Festplatten auf den Brücken deutlich sichtbar sind.

   Sie können z. B. einen Befehl verwenden `sastargets` Auf der ATTO-CLI.

5. Aktivieren Sie die ISLs auf FC Switches.

   Aktivieren Sie die Ports basierend darauf, ob Sie Brocade- oder Cisco-Switches wie in der folgenden Tabelle dargestellt verwenden:

Switch-Typ	Befehl

Für Brocade FC Switches…	a. Geben Sie das ein `portcfgpersistentenable <port>` Befehl zum Persistenz-Aktivieren der Ports. Dies muss an beiden Schaltern am überlebenden Standort erfolgen.
	
	Im folgenden Beispiel werden die Ports 14 und 15 bei Switch_A_1 aktiviert:
	
	`Switch_A_1:admin> portcfgpersistentenable 14`
	`Switch_A_1:admin> portcfgpersistentenable 15`
	`Switch_A_1:admin>`
	
	b. Vergewissern Sie sich, dass der Switch-Port mit dem + aktiviert ist `switchshow` Befehl:
	
	`switch_A_1:admin> switchshow`
	`switchName: Switch_A_1`
	`switchType: 109.1`
	`switchState: Online`
	`switchMode: Native`
	`switchRole: Principal`
	`switchDomain: 2`
	`switchId: fffc02`
	`switchWwn: 10:00:00:05:33:88:9c:68`
	`zoning: ON (T5_T6)`
	`switchBeacon: OFF`
	`FC Router: OFF`
	`FC Router BB Fabric ID: 128`
	`Address Mode: 0`
	
	`Index Port Address Media Speed State Proto`
	`==========`
	`...`
	`14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1"`
	`15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)`
	`...`
	`switch_A_1:admin>`

Für Cisco FC Switches…	a. Verwenden Sie die `interface` Befehl zum Aktivieren der Ports.
	
	Das folgende Beispiel zeigt, dass Port fc1/14 und fc1/15 auf Switch A_1 aktiviert sind:
	
	`switch_A_1# conf t`
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# no shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Vergewissern Sie sich, dass der Switch-Port deaktiviert ist:
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

6. Vergewissern Sie sich, dass der Speicher sichtbar ist.
   a. Vergewissern Sie sich, dass der Speicher vom verbleibenden Standort aus sichtbar ist. Versetzen Sie die Offline-Plexe wieder in den Online-Modus, um die Neusynchronisierung neu zu starten und die SyncMirror wiederherzustellen.
   b. Überprüfen Sie, ob der lokale Speicher vom Knoten im Wartungsmodus sichtbar ist:

      ```
      disk show -v
      ```

7. Wiederherstellung der MetroCluster-Konfiguration

   Befolgen Sie die Anweisungen unter "Überprüfen, ob das System für einen Wechsel bereit ist" Um Healing- und Switchback-Vorgänge gemäß Ihrer MetroCluster-Konfiguration durchzuführen.

Herunterfahren einer gesamten MetroCluster FC-Konfiguration

Sie müssen die gesamte MetroCluster FC-Konfiguration und alle Geräte ausschalten, bevor die Wartungsarbeiten oder Standortwechsel beginnen können.

Über diese Aufgabe

Sie müssen die in diesem Verfahren beschriebenen Schritte von beiden Standorten aus gleichzeitig ausführen.

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

Schritte

1. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.
   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus.

metrocluster show

b. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:
run local sysconfig -v

c. Führen Sie den folgenden Befehl aus:
storage bridge show

d. Führen Sie den folgenden Befehl aus:
storage port show

e. Führen Sie den folgenden Befehl aus:
storage switch show

f. Führen Sie den folgenden Befehl aus:
network port show

g. Führen Sie eine MetroCluster-Prüfung durch:
metrocluster check run

h. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
metrocluster check show

2. Deaktivieren Sie AUSO, indem Sie die AUSO-Fehlerdomäne in ändern

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

3. Die Änderung wird mit dem Befehl überprüft

metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Beenden Sie die Knoten mit folgendem Befehl:
halt

   - Verwenden Sie für eine MetroCluster-Konfiguration mit vier oder acht Nodes die **inhibit-takeover** Und **skip-lif-migration-before-shutdown** Parameter:

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore
-quorum-warnings true -skip-lif-migration-before-shutdown true
```

- Verwenden Sie für eine MetroCluster-Konfiguration mit zwei Nodes den Befehl:

```
system node halt -node node1_SiteA -ignore-quorum-warnings true
```

5. Schalten Sie die folgenden Geräte am Standort aus:
   - Storage Controller
   - MetroCluster FC-Switches (wenn verwendet und die Konfiguration keine Stretch-Konfiguration mit zwei Nodes bietet)
   - ATTO FibreBridges
   - Storage Shelfs
6. Warten Sie 30 Minuten, und schalten Sie dann die folgenden Geräte am Standort ein:
   - Storage Shelfs
   - ATTO FibreBridges
   - MetroCluster FC-Switches
   - Storage Controller
7. Nachdem die Controller eingeschaltet sind, überprüfen Sie die MetroCluster-Konfiguration von beiden Standorten aus.

   Um die Konfiguration zu überprüfen, wiederholen Sie Schritt 1.

8. Führen Sie Prüfungen der Einschaltzyklus durch.
   a. Vergewissern Sie sich, dass alle Sync-Source-SVMs online sind:
      `vserver show`
   b. Starten Sie alle Sync-Source-SVMs, die nicht online sind:
      `vserver start`

Wartungsverfahren für MetroCluster IP-Konfigurationen

Wartung und Austausch von IP-Switches

Ersetzen Sie einen IP-Switch oder ändern Sie die Verwendung vorhandener MetroCluster IP-Switches

Möglicherweise müssen Sie einen ausgefallenen Switch ersetzen, einen Switch aktualisieren oder herunterstufen oder die Verwendung vorhandener MetroCluster IP-Switches ändern.

Über diese Aufgabe

Dieses Verfahren gilt, wenn Sie NetApp Validated Switches verwenden. Wenn Sie MetroCluster-konforme Switches verwenden, wenden Sie sich an den Switch-Anbieter.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

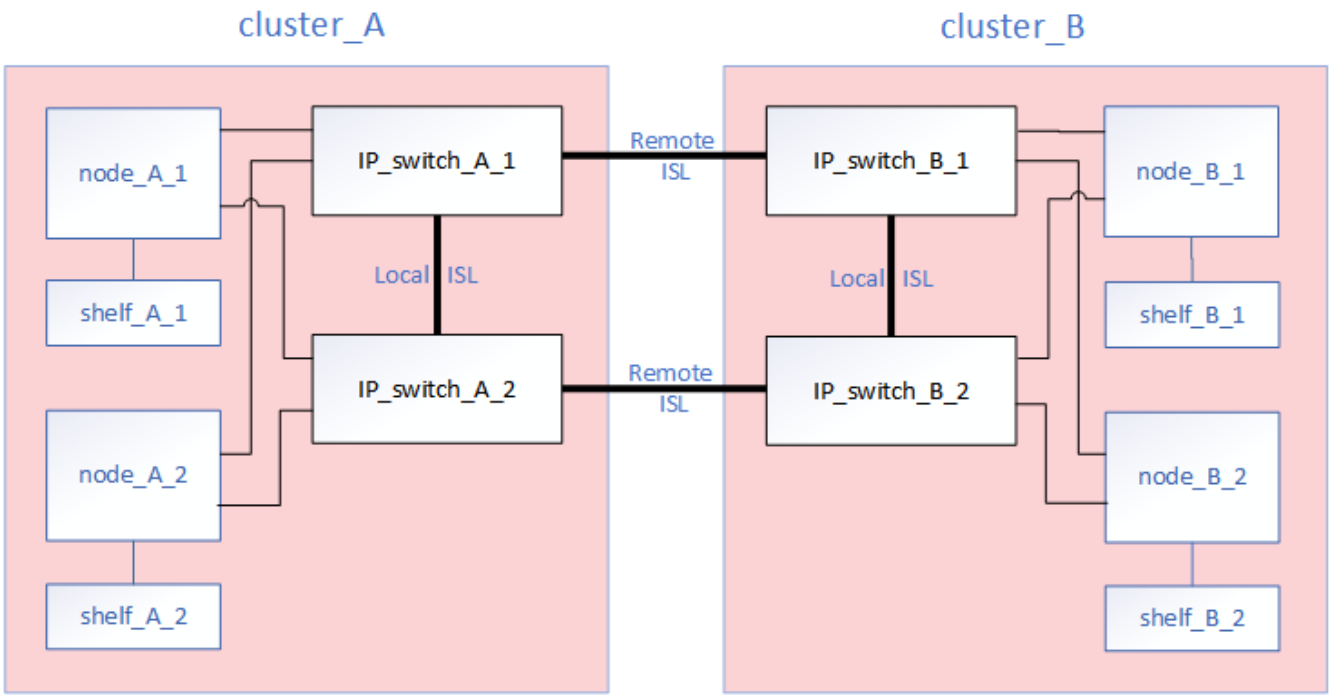
Dieses Verfahren unterstützt die folgenden Konvertierungen:

- Ändern des Switch-Anbieters, -Typs oder beider Typen. Der neue Switch kann mit dem alten Schalter

identisch sein, wenn ein Switch ausgefallen ist, oder Sie können den Switch-Typ ändern (Upgrade oder Downgrade des Schalters).

Um beispielsweise eine MetroCluster IP-Konfiguration von einer Konfiguration mit vier Nodes mit AFF A400 Controllern und BES-53248 Switches auf eine Konfiguration mit acht Nodes mit AFF A400 Controllern zu erweitern, müssen Sie die Switches auf einen unterstützten Typ für die Konfiguration ändern, da BES-53248 Switches in der neuen Konfiguration nicht unterstützt werden.

Wenn Sie einen defekten Switch durch denselben Switch-Typ ersetzen möchten, tauschen Sie nur den ausgefallenen Switch aus. Wenn Sie einen Switch aktualisieren oder herunterstufen möchten, müssen Sie zwei Switches anpassen, die sich im gleichen Netzwerk befinden. Zwei Switches befinden sich im selben Netzwerk, wenn sie mit einer ISL (Inter-Switch Link) verbunden sind und sich nicht am selben Standort befinden. Netzwerk 1 umfasst z. B. IP_Switch_A_1 und IP_Switch_B_1, Netzwerk 2 enthält IP_Switch_A_2 und IP_Switch_B_2, wie in der folgenden Abbildung dargestellt:



> Wenn Sie einen Switch ersetzen oder auf verschiedene Switches aktualisieren, können Sie die Switches vorkonfigurieren, indem Sie die Switch-Firmware und die RCF-Datei installieren.

- Konvertieren einer MetroCluster IP-Konfiguration in eine MetroCluster IP-Konfiguration mit MetroCluster-Switches für Shared Storage.

  Wenn Sie beispielsweise über eine regelmäßige MetroCluster IP-Konfiguration mit AFF A700 Controllern verfügen und die MetroCluster neu konfigurieren möchten, um NS224-Shelfs mit denselben Switches zu verbinden.

> - Wenn Sie Shelfs in einer MetroCluster IP-Konfiguration mithilfe von MetroCluster IP-Switches für gemeinsamen Speicher hinzufügen oder entfernen, führen Sie die Schritte in aus "Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von MetroCluster-Switches mit Shared-Storage"
> - Die MetroCluster IP-Konfiguration stellt möglicherweise bereits eine direkte Verbindung zu NS224-Shelfs oder zu dedizierten Storage-Switches her.

Arbeitsblatt zur Portnutzung

Im Folgenden finden Sie ein Beispiel-Arbeitsblatt zum Konvertieren einer MetroCluster IP-Konfiguration in eine Konfiguration mit gemeinsamem Speicher, bei der zwei NS224-Shelfs unter Verwendung der vorhandenen Switches verbunden werden.

Arbeitsblattdefinitionen:

- Vorhandene Konfiguration: Verkabelung der vorhandenen MetroCluster-Konfiguration.
- Neue Konfiguration mit NS224 Shelfs: Die Zielkonfiguration, bei der die Switches zwischen Storage und MetroCluster gemeinsam genutzt werden

Die hervorgehobenen Felder in diesem Arbeitsblatt geben Folgendes an:

- Grün: Sie müssen die Verkabelung nicht ändern.
- Gelb: Sie müssen Ports mit derselben oder einer anderen Konfiguration verschieben.
- Blau: Ports, die neue Verbindungen sind.

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist: **`metrocluster show`**

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

   b. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt: **`system health alert show`**

2. Konfigurieren Sie den neuen Switch vor der Installation.

   Wenn Sie vorhandene Switches erneut verwenden, fahren Sie mit fort Schritt 4.

   > Wenn Sie die Switches aktualisieren oder verkleinern, müssen Sie alle Switches im Netzwerk konfigurieren.

   Befolgen Sie die Schritte im Abschnitt *Konfigurieren der IP-Switches* im "Installation und Konfiguration von MetroCluster IP"

   Stellen Sie sicher, dass Sie die korrekte RCF-Datei für den Schalter _A_1, _A_2, _B_1 oder _B_2 anwenden. Wenn der neue Switch mit dem alten Switch identisch ist, müssen Sie dieselbe RCF-Datei anwenden.

   Wenn Sie einen Switch aktualisieren oder herunterstufen, wenden Sie die neueste unterstützte RCF-Datei für den neuen Switch an.

3. Führen Sie den Befehl Port show aus, um Informationen zu den Netzwerkports anzuzeigen:

   `network port show`

   a. Ändern Sie alle Cluster-LIFs, um die automatische Zurücksetzung zu deaktivieren:

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. Trennen Sie die Verbindungen vom alten Switch.

> Sie trennen nur Verbindungen, die nicht denselben Port in der alten und neuen Konfiguration verwenden. Wenn Sie neue Switches verwenden, müssen Sie alle Verbindungen trennen.

Entfernen Sie die Anschlüsse in der folgenden Reihenfolge:

a. Trennen Sie die lokalen Cluster-Schnittstellen
b. Trennen Sie die lokalen Cluster-ISLs
c. Trennen Sie die MetroCluster IP-Schnittstellen
d. Trennen Sie die MetroCluster-ISLs

   Im Beispiel [port_usage_worksheet]Die Schalter ändern sich nicht. Die MetroCluster-ISLs werden verschoben und müssen getrennt werden. Sie müssen die grün markierten Verbindungen auf dem Arbeitsblatt nicht trennen.

5. Wenn Sie neue Schalter verwenden, schalten Sie den alten Schalter aus, entfernen Sie die Kabel, und entfernen Sie den alten Schalter.

   Wenn Sie vorhandene Switches erneut verwenden, fahren Sie mit fort Schritt 6.

> Verkabeln Sie die neuen Switches mit Ausnahme der Verwaltungsschnittstelle (falls verwendet) nicht.

6. Konfigurieren Sie die vorhandenen Switches.

   Wenn Sie die Switches bereits vorkonfiguriert haben, können Sie diesen Schritt überspringen.

   Führen Sie zum Konfigurieren der vorhandenen Switches die Schritte zum Installieren und Aktualisieren der Firmware- und RCF-Dateien aus:

   - "Aktualisieren der Firmware auf MetroCluster IP Switches"
   - "Aktualisieren Sie RCF-Dateien auf MetroCluster IP-Switches"

7. Verkabeln Sie die Schalter.

   Sie können die Schritte im Abschnitt *verkabeln der IP-Switches* in befolgen "Installation und Konfiguration von MetroCluster IP".

   Verkabeln Sie die Schalter in der folgenden Reihenfolge (falls erforderlich):

a. Verkabeln Sie die ISLs mit dem Remote-Standort.
b. Verkabeln Sie die MetroCluster IP-Schnittstellen.
c. Verkabeln Sie die lokalen Cluster-Schnittstellen.

- Die verwendeten Ports können von denen auf dem alten Switch abweichen, wenn der Switch-Typ anders ist. Wenn Sie die Switches aktualisieren oder verkleinern, müssen Sie die lokalen ISLs nicht * verkabeln. Verkabeln Sie die lokalen ISLs nur, wenn Sie die Switches im zweiten Netzwerk aktualisieren oder herunterstufen und beide Switches an einem Standort den gleichen Typ und die gleiche Verkabelung aufweisen.
- Wenn Sie Switch-A1 und Switch-B1 aktualisieren, müssen Sie die Schritte 1 bis 6 für Schalter A2 und Switch-B2 ausführen.

8. Schließen Sie die lokale Clusterverkabelung ab.
   a. Wenn die lokalen Cluster-Schnittstellen mit einem Switch verbunden sind:
      i. Verkabeln Sie die lokalen Cluster-ISLs.
   b. Wenn die lokalen Clusterschnittstellen **nicht** mit einem Switch verbunden sind:
      i. Verwenden Sie die "Migration zu einer NetApp Cluster-Umgebung mit Switch" Vorgehensweise zum Konvertieren eines Clusters ohne Switches in ein Cluster mit Switches. Verwenden Sie die in angegebenen Anschlüsse "Installation und Konfiguration von MetroCluster IP" Oder die RCF-Verkabelungsdateien, um die lokale Clusterschnittstelle zu verbinden.
9. Schalten Sie den Schalter ein oder schalten Sie den Schalter ein.

   Wenn der neue Schalter gleich ist, schalten Sie den neuen Schalter ein. Wenn Sie die Schalter aktualisieren oder verkleinern, schalten Sie beide Schalter ein. Die Konfiguration kann mit zwei verschiedenen Switches an jedem Standort betrieben werden, bis das zweite Netzwerk aktualisiert wird.

10. Wiederholen Sie die Schritte, um zu überprüfen, ob die MetroCluster-Konfiguration ordnungsgemäß ist Schritt 1.

    Wenn Sie die Switches im ersten Netzwerk aktualisieren oder verkleinern, werden möglicherweise einige Warnmeldungen im Zusammenhang mit dem lokalen Clustering angezeigt.

    Wenn Sie die Netzwerke aktualisieren oder herunterstufen, dann wiederholen Sie alle Schritte für das zweite Netzwerk.

11. Ändern Sie alle Cluster-LIFs, um die automatische Zurücksetzung erneut zu aktivieren:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. Verschieben Sie optional die NS224-Shelfs.

    Wenn Sie eine MetroCluster IP-Konfiguration neu konfigurieren, bei der keine NS224-Shelfs mit den MetroCluster IP-Switches verbunden werden, gehen Sie wie folgt vor, um die NS224-Shelfs hinzuzufügen oder zu verschieben:

    - "Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von MetroCluster-Switches mit Shared-Storage"
    - "Migrieren Sie von einem Cluster ohne Switches mit Direct-Attached Storage"
    - "Migrieren Sie mit der erneuten Nutzung der Storage-Switches von einer Konfiguration ohne Switches mit Switch-Attached Storage"

Online- oder Offline-Ports der MetroCluster IP-Schnittstelle

Wenn Sie Wartungsaufgaben durchführen, müssen Sie möglicherweise einen MetroCluster IP-Schnittstellenport offline oder online schalten.

Über diese Aufgabe

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

Sie können die folgenden Schritte durchführen, um einen MetroCluster-IP-Schnittstellen-Port online zu schalten oder in den Offline-Modus zu versetzen.

1. Legen Sie die Berechtigungsebene auf erweitert fest.

   ```
   set -privilege advanced
   ```

   Beispielausgabe

   ```
   Cluster A_1::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them
   only when
            directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

2. Versetzen Sie den Port der MetroCluster IP-Schnittstelle in den Offline-Modus.

   ```
   system ha interconnect link off -node <node_name> -link <link_num, 0 or
   1>
   ```

   Beispielausgabe

   ```
   Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
   ```

   a. Überprüfen Sie, ob die MetroCluster-IP-Schnittstelle offline ist.

      ```
      Cluster_A1::*> system ha interconnect port show
      ```

      Beispielausgabe

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                Link            Layer     Layer      Physical   Physical
Active
Node            Monitor  Port   State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                            0  disabled  down              4          3
false
                            1  linkup    active            4          2
true
node-a2        off
                            0  linkup    active            4          2
true
                            1  linkup    active            4          2
true
2 entries were displayed.
```

3. Versetzen Sie den MetroCluster IP-Schnittstellenport in den Online-Modus.

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. Überprüfen Sie, ob der Port der MetroCluster IP-Schnittstelle online ist.

```
Cluster_A1::*> system ha interconnect port show
```

Beispielausgabe

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                Link            Layer     Layer      Physical   Physical
Active
Node            Monitor  Port   State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                            0  linkup    active            5          3
true
                            1  linkup    active            4          2
true
node-a2        off
                            0  linkup    active            4          2
true
                            1  linkup    active            4          2
true
2 entries were displayed.
```

Aktualisieren Sie Firmware auf MetroCluster IP Switches

Möglicherweise müssen Sie die Firmware auf einem MetroCluster IP Switch aktualisieren.

Stellen Sie sicher, dass die RCF unterstützt wird

Wenn Sie die ONTAP-Version oder die Switch-Firmware-Version ändern, sollten Sie überprüfen, ob eine Referenzkonfigurationsdatei (RCF) vorhanden ist, die für diese Version unterstützt wird. Wenn Sie das Tool verwenden"RCfFileGenerator", wird die richtige RCF für Ihre Konfiguration generiert.

Schritte

1. Verwenden Sie die folgenden Befehle der Switches, um die Version der RCF zu überprüfen:

Von diesem Schalter…	Geben Sie diesen Befehl aus…
Broadcom-Switch	`(IP_switch_A_1) # show clibanner`
Cisco Switch	`IP_switch_A_1# show banner motd`
NVIDIA SN2100-Switch	`cumulus@mcc1:mgmt:~$ nv config find message`

Suchen Sie die Zeile in der Befehlsausgabe, die die RCF-Version angibt. Die folgende Ausgabe von einem Cisco-Switch zeigt beispielsweise an, dass die RCF-Version „`v1.80`“ ist.

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Um zu überprüfen, welche Dateien für eine bestimmte ONTAP-Version, einen Switch und eine bestimmte Plattform unterstützt werden, verwenden Sie die "RCfFileGenerator für MetroCluster-IP". Wenn Sie die RCF für die Konfiguration generieren können, auf die Sie aktualisieren möchten, wird sie unterstützt.
3. Um sicherzustellen, dass die Switch-Firmware unterstützt wird, lesen Sie bitte die folgenden Informationen:
   - "Hardware Universe"
   - "NetApp Interoperabilitätsmatrix"

Aktualisieren Sie die Switch-Firmware

Über diese Aufgabe

Sie müssen diese Aufgabe nacheinander an jedem der Schalter wiederholen.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist:

   ```
   metrocluster show
   ```

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

   b. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist:

   ```
   metrocluster node show
   ```

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind:

   `metrocluster check run`

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

d. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

   `metrocluster check show`

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
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.
```

a. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

   `system health alert show`

2. Installieren Sie die Software auf dem ersten Switch.

> Sie müssen die Switch-Software auf den Switches in der folgenden Reihenfolge installieren: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

Befolgen Sie die Schritte zum Installieren der Switch-Software im entsprechenden Thema, je nachdem, ob der Switch-Typ Broadcom, Cisco oder NVIDIA ist:

- "Laden Sie die Broadcom-Switch-EFOS-Software herunter, und installieren Sie sie"
- "Laden Sie die Cisco Switch NX-OS-Software herunter, und installieren Sie sie"
- "Laden Sie die NVIDIA SN2100 Switch Cumulus Software herunter und installieren Sie sie"

3. Wiederholen Sie den vorherigen Schritt für jeden der Schalter.
4. Wiederholen Schritt 1 Um den Zustand der Konfiguration zu überprüfen.

Aktualisieren Sie RCF-Dateien auf MetroCluster IP-Switches

Möglicherweise müssen Sie eine RCF-Datei (Reference Configuration File) auf einem MetroCluster IP-Switch aktualisieren. Wenn beispielsweise die RCF-Version, die Sie auf den Switches ausführen, nicht von der ONTAP-Version, der Switch-Firmware-Version oder beiden unterstützt wird.

Bevor Sie beginnen

- Wenn Sie neue Switch-Firmware installieren, müssen Sie die Switch-Firmware installieren, bevor Sie die RCF-Datei aktualisieren.
- Bevor Sie den RCF aktualisieren, "Stellen Sie sicher, dass die RCF unterstützt wird".
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Über diese Aufgabe

- Dieses Verfahren unterbricht den Datenverkehr auf dem Switch, auf dem die RCF-Datei aktualisiert wird. Der Datenverkehr wird wieder aufgenommen, wenn die neue RCF-Datei angewendet wird.
- Führen Sie die Schritte jeweils an einem Schalter in der folgenden Reihenfolge aus: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   `metrocluster check run`

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

   b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführung `metrocluster check show` Um die Ergebnisse anzuzeigen.

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
-----------
::*> metrocluster check show

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

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id 38
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

   Befolgen Sie die Schritte für Ihren Switch-Anbieter:

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

3. Laden Sie je nach Switch-Anbieter die IP RCF-Datei herunter, und installieren Sie sie.
   - "Laden Sie die Broadcom IP RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die Cisco IP RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die NVIDIA IP RCF-Dateien herunter, und installieren Sie sie"

> Wenn Sie über eine freigegebene L2- oder L3-Netzwerkkonfiguration verfügen, müssen Sie möglicherweise die ISL-Ports an den Zwischen-/Kunden-Switches anpassen. Der Switchport-Modus kann von „Access“ auf „Trunk“ geändert werden. Fahren Sie nur mit dem Upgrade des zweiten Switch-Paares (A_2, B_2) fort, wenn die Netzwerkverbindung zwischen den Switches A_1 und B_1 voll funktionsfähig ist und das Netzwerk ordnungsgemäß ist.

Aktualisieren Sie RCF-Dateien auf Cisco IP-Switches mithilfe von CleanUpFiles

Möglicherweise müssen Sie eine RCF-Datei auf einem Cisco IP-Switch aktualisieren. Beispielsweise ist für ein ONTAP Upgrade oder ein Switch-Firmware-Upgrade eine neue RCF-Datei erforderlich.

Über diese Aufgabe

- Ab der Version 1.4a von RcfFileGenerator gibt es eine neue Option, die Switch-Konfiguration auf Cisco IP-Switches zu ändern (Upgrade, Downgrade oder Ersetzen), ohne dass eine 'Schreiblöschung' durchgeführt werden muss.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.
- Der Cisco 9336C-FX2 Switch verfügt über zwei verschiedene Switch-Speichertypen, die im RCF unterschiedlich benannt sind. Verwenden Sie die folgende Tabelle, um den richtigen Cisco 9336C-FX2-Speichertyp für Ihre Konfiguration zu ermitteln:

Wenn Sie den folgenden Speicher verbinden…	Wählen Sie den Cisco 9336C-FX2-Speichertyp…	Beispiel für RCF-Dateibanner/MOTD
• Direkt verbundene SAS-Shelfs • Direkt verbundene NVMe-Shelfs • NVMe-Shelfs, die mit dedizierten Storage-Switches verbunden sind	9336C-FX2 – nur Direct Storage	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• Direkt verbundene SAS-Shelfs • Mit den MetroCluster IP-Switches verbundene NVMe Shelfs ⓘ Es ist mindestens ein Ethernet-angeschlossenes NVMe-Shelf erforderlich	9336C-FX2 – SAS- und Ethernet-Speicher	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

Bevor Sie beginnen

Sie können diese Methode verwenden, wenn Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Es wird die Standard-RCF-Konfiguration angewendet.
- Der "RCfFileGenerator" Muss in der Lage sein, dieselbe RCF-Datei zu erstellen, die angewendet wird, und zwar mit derselben Version und Konfiguration (Plattformen, VLANs).
- Die angewandte RCF-Datei wurde von NetApp nicht für eine spezielle Konfiguration zur Verfügung gestellt.
- Die RCF-Datei wurde vor der Anwendung nicht geändert.
- Die Schritte zum Zurücksetzen des Switches auf die Werkseinstellungen wurden vor dem Anwenden der aktuellen RCF-Datei befolgt.
- Nach der Anwendung des RCF wurden an der Switch(Port)-Konfiguration keine Änderungen vorgenommen.

  Wenn Sie diese Anforderungen nicht erfüllen, können Sie die CleanUpFiles, die beim Erstellen der RCF-Dateien erstellt wurden, nicht verwenden. Sie können jedoch die Funktion nutzen, um generische

CleanUpFiles zu erstellen — die Bereinigung mit dieser Methode ist aus der Ausgabe von abgeleitet `show running-config` Und ist die Best Practice.

> Sie müssen die Switches in folgender Reihenfolge aktualisieren: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. Oder Sie können die Schalter Switch_A_1 und Switch_B_1 gleichzeitig aktualisieren, gefolgt von den Schaltern Switch_A_2 und Switch_B_2.

Schritte

1. Legen Sie die aktuelle RCF-Dateiversion fest, welche Ports und VLANs verwendet werden:
   `IP_switch_A_1# show banner motd`

   > Sie müssen diese Informationen von allen vier Switches erhalten und die folgende Informationstabelle ausfüllen.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*

#
IP_switch_A_1#
```

   In dieser Ausgabe müssen Sie die in den folgenden beiden Tabellen aufgeführten Informationen erfassen.

Allgemeine Informationen	MetroCluster	Daten
RCF-Dateiversion		1.81
Switch-Typ		NX9336
Netzwerktypologie		L2-Netzwerke, direkte ISL
Storage-Typ		SAS-Storage
Plattformen	1	AFF A400
	2	FAS9000

VLAN-Informationen	Netzwerk	MetroCluster-Konfiguration	Switchports	Standort A	Standort B
VLAN lokaler Cluster	Netzwerk 1	1	1, 2	111	222
		2	3, 4	151	251
	Netzwerk 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN-MetroCluster	Netzwerk 1	1	9, 10	119	119
		2	11, 12	159	159
	Netzwerk 2	1	9, 10	219	219
		2	11, 12	259	259

2. [[Create-RCF-files-and-CleanUpFiles-or-create-generic-CleanUp Files] Erstellen Sie die RCF-Dateien und CleanUpFiles oder erstellen Sie allgemeine CleanUpFiles für die aktuelle Konfiguration.

   Wenn Ihre Konfiguration die in den Voraussetzungen beschriebenen Anforderungen erfüllt, wählen Sie **Option 1**. Wenn Ihre Konfiguration die in den Voraussetzungen beschriebenen Anforderungen nicht erfüllt, wählen Sie **Option 2**.

Option 1: Erstellen Sie die RCF-Dateien und CleanUpFiles

Gehen Sie folgendermaßen vor, wenn die Konfiguration den Anforderungen entspricht.

Schritte

a. Verwenden Sie den RCfFileGenerator 1.4a (oder höher), um die RCF-Dateien mit den Informationen zu erstellen, die Sie in Schritt 1 abgerufen haben. Die neue Version des RcfFileGenerators erstellt einen zusätzlichen Satz von CleanUpFiles, mit denen Sie einige Konfigurationen zurücksetzen und den Switch vorbereiten können, um eine neue RCF-Konfiguration anzuwenden.

b. Vergleichen Sie das Banner motd mit den derzeit verwendeten RCF-Dateien. Die Plattformtypen, der Switch-Typ, die Port- und die VLAN-Nutzung müssen identisch sein.

> Sie müssen die CleanUpFiles aus derselben Version wie die RCF-Datei und für die exakt gleiche Konfiguration verwenden. Die Verwendung von CleanUpFile funktioniert nicht und erfordert möglicherweise ein vollständiges Zurücksetzen des Switches.

> Die ONTAP-Version, für die die RCF-Datei erstellt wurde, ist nicht relevant. Es ist nur die RCF-Dateiversion wichtig.

> Die RCF-Datei (auch die gleiche Version ist) könnte weniger oder mehr Plattformen auflisten. Stellen Sie sicher, dass Ihre Plattform aufgeführt ist.

Option 2: Erstellen Sie allgemeine CleanUpFiles

Gehen Sie folgendermaßen vor, wenn die Konfiguration nicht alle Anforderungen erfüllt.

Schritte

a. Abrufen der Ausgabe von `show running-config` Von jedem Schalter.

b. Öffnen Sie das RcfFileGenerator-Tool und klicken Sie unten im Fenster auf 'Generic CleanUpFiles erstellen'

c. Kopieren Sie die Ausgabe, die Sie in Schritt 1 von „One“-Schalter in das obere Fenster abgerufen haben. Sie können die Standardausgabe entfernen oder belassen.

d. Klicken Sie auf „CUF-Dateien erstellen“.

e. Kopieren Sie die Ausgabe aus dem unteren Fenster in eine Textdatei (diese Datei ist die CleanUpFile).

f. Wiederholen Sie die Schritte c, d und e für alle Schalter in der Konfiguration.

   Am Ende dieses Verfahrens sollten Sie vier Textdateien haben, eine für jeden Switch. Sie können diese Dateien auf die gleiche Weise wie die CleanUpFiles verwenden, die Sie mit Option 1 erstellen können.

3. Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration. Erstellen Sie diese Dateien auf die gleiche Weise, wie Sie die Dateien im vorherigen Schritt erstellt haben, außer wählen Sie die entsprechende ONTAP und RCF-Dateiversion.

   Nach Abschluss dieses Schritts sollten Sie zwei Sätze RCF-Dateien haben, die jeweils aus zwölf Dateien

bestehen.

4. Laden Sie die Dateien auf den Bootflash herunter.

   a. Laden Sie die CleanUpFiles herunter, die Sie in erstellt haben Erstellen Sie die RCF-Dateien und CleanUpFiles oder erstellen Sie allgemeine CleanUpFiles für die aktuelle Konfiguration

   > Diese CleanUpFile ist für die aktuelle RCF-Datei, die angewendet wird und **NICHT** für die neue RCF, auf die Sie aktualisieren möchten.

   Beispiel CleanUpFile für Switch-A1: `Cleanup_NX9336_v1.81_Switch-A1.txt`

   b. Laden Sie die neuen RCF-Dateien herunter, die Sie in erstellt haben Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration.

   Beispiel für RCF-Datei für Switch-A1: `NX9336_v1.90_Switch-A1.txt`

   c. Laden Sie die CleanUpFiles herunter, die Sie in erstellt haben Erstellen Sie die 'neuen' RCF-Dateien für die neue Konfiguration. Dieser Schritt ist optional — Sie können die Datei in Zukunft verwenden, um die Switch-Konfiguration zu aktualisieren. Es stimmt mit der aktuell verwendeten Konfiguration überein.

   Beispiel CleanUpFile für Switch-A1: `Cleanup_NX9336_v1.90_Switch-A1.txt`

   > Sie müssen die CleanUpFile für die korrekte (passende) RCF-Version verwenden. Wenn Sie eine CleanUpFile für eine andere RCF-Version oder eine andere Konfiguration verwenden, funktioniert die Bereinigung der Konfiguration möglicherweise nicht richtig.

   Im folgenden Beispiel werden die drei Dateien auf den Bootflash kopiert:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

> Sie werden aufgefordert, Virtual Routing und Forwarding (VRF) anzugeben.

5. Übernehmen Sie die CleanUpFile- oder die allgemeine CleanUpFile-Datei.

   Einige der Konfigurationen werden zurückgesetzt und die Switchports gehen „offline“.

a. Vergewissern Sie sich, dass keine ausstehenden Änderungen an der Startkonfiguration vorliegen: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Wenn Sie die Systemausgabe sehen, speichern Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

> Die Systemausgabe zeigt an, dass die Startkonfiguration und die laufende Konfiguration unterschiedlich und ausstehende Änderungen sind. Wenn Sie die ausstehenden Änderungen nicht speichern, können Sie den Switch nicht erneut laden.

a. Anwenden der CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

> Das Skript kann eine Weile dauern, bis es zur Switch-Eingabeaufforderung zurückkehrt. Es wird keine Ausgabe erwartet.

7. Zeigen Sie die laufende Konfiguration an, um zu überprüfen, ob die Konfiguration gelöscht wurde: `show running-config`

   Die aktuelle Konfiguration sollte Folgendes zeigen:

   - Es sind keine Klassenkarten und IP-Zugriffslisten konfiguriert
   - Es wurden keine Richtlinienzuordnungen konfiguriert
   - Es sind keine Service-Richtlinien konfiguriert
   - Es werden keine Port-Profile konfiguriert
   - Alle Ethernet-Schnittstellen (außer mgmt0 die keine Konfiguration zeigen sollten, und nur VLAN 1 sollte konfiguriert sein).

     Wenn Sie feststellen, dass eines der oben genannten Elemente konfiguriert ist, können Sie möglicherweise keine neue RCF-Dateikonfiguration anwenden. Sie können jedoch auf die vorherige Konfiguration zurücksetzen, indem Sie den Switch *neu laden, ohne die laufende Konfiguration in die Startkonfiguration zu speichern. Der Switch verfügt über die vorherige Konfiguration.

8. Wenden Sie die RCF-Datei an und stellen Sie sicher, dass die Ports online sind.

   a. Wenden Sie die RCF-Dateien an.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

> Beim Anwenden der Konfiguration werden einige Warnmeldungen angezeigt. Fehlermeldungen werden in der Regel nicht erwartet. Wenn Sie jedoch mit SSH angemeldet sind, wird möglicherweise die folgende Fehlermeldung angezeigt: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. Überprüfen Sie nach der Anwendung der Konfiguration, ob die Cluster- und MetroCluster-Ports mit einem der folgenden Befehle online geschaltet werden: `show interface brief`, `show cdp neighbors`, Oder `show lldp neighbors`

> Wenn Sie das VLAN für den lokalen Cluster geändert haben und Sie den ersten Switch am Standort aktualisiert haben, wird der Zustand der Cluster-Zustandsüberwachung möglicherweise nicht als „stabil" angegeben, da die VLANs der alten und der neuen Konfigurationen nicht übereinstimmen. Nach der Aktualisierung des zweiten Schalters sollte der Status wieder in den Status „gesund" zurückkehren.

Wenn die Konfiguration nicht korrekt angewendet wird oder Sie die Konfiguration nicht beibehalten möchten, können Sie die vorherige Konfiguration wiederherstellen, indem Sie den Switch wieder laden **ohne** die laufende Konfiguration in die Startkonfiguration zu speichern. Der Switch verfügt über die vorherige Konfiguration.

9. Speichern Sie die Konfiguration, und laden Sie den Schalter neu.

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Umbenennen eines Cisco IP-Switches

Möglicherweise müssen Sie einen Cisco IP-Switch umbenennen, um während der Konfiguration eine konsistente Benennung zu ermöglichen.

Über diese Aufgabe

- In den Beispielen in dieser Aufgabe wird der Switch-Name von geändert `myswitch` Bis `IP_switch_A_1`.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   Im folgenden Beispiel wird die Eingabeaufforderung für den Konfigurationsmodus angezeigt. In beiden Eingabeaufforderungen wird der Switch-Name von angezeigt `myswitch`.

```
myswitch# configure terminal
myswitch(config)#
```

2. Umbenennung des Switches:

   `switchname new-switch-name`

   Wenn Sie beide Switches im Netzwerk umbenennen, verwenden Sie auf jedem Switch denselben Befehl.

   Die CLI-Eingabeaufforderung wird geändert, um den neuen Namen wiederzugeben:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Konfigurationsmodus beenden:

   `exit`

   Die Eingabeaufforderung für den Schalter auf oberster Ebene wird angezeigt:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Kopieren der aktuellen Konfiguration in die Startkonfigurationsdatei:

   `copy running-config startup-config`

5. Vergewissern Sie sich, dass die Änderung des Switch-Namens von der ONTAP-Cluster-Eingabeaufforderung aus sichtbar ist.

   Beachten Sie, dass der neue Switch-Name und der alte Switch-Name angezeigt werden (`myswitch`) Erscheint nicht.

   a. Rufen Sie den erweiterten Berechtigungsmodus auf, und drücken Sie **`y`** Wenn Sie dazu aufgefordert werden:
      `set -privilege advanced`
   b. Anzeige der angeschlossenen Geräte:
      `network device-discovery show`
   c. Zurück zum Admin-Berechtigungsmodus:
      `set -privilege admin`

      Das folgende Beispiel zeigt, dass der Schalter mit dem neuen Namen angezeigt wird. `IP_switch_A_1`:

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Unterbrechungsfreies Hinzufügen, Entfernen oder Ändern von ISL-Ports auf Cisco IP-Switches

Möglicherweise müssen Sie ISL-Ports bei Cisco IP-Switches hinzufügen, entfernen oder ändern. Sie können dedizierte ISL-Ports in gemeinsame ISL-Ports konvertieren oder die

Geschwindigkeit von ISL-Ports auf einem Cisco IP-Switch ändern.

Über diese Aufgabe

Wenn Sie dedizierte ISL-Ports in gemeinsam genutzte ISL-Ports konvertieren, stellen Sie sicher, dass die neuen Ports den entsprechen "Voraussetzungen für gemeinsam genutzte ISL-Ports".

Um die ISL-Konnektivität sicherzustellen, müssen Sie alle Schritte auf beiden Switches ausführen.

Im folgenden Verfahren wird vorausgesetzt, dass Sie eine 10-GB-ISL, die am Switch-Port eth1/24/1 angeschlossen ist, durch zwei 100-GB-ISLs ersetzen, die mit den Switch-Ports 17 und 18 verbunden sind.

> Wenn Sie einen Cisco 9336C-FX2-Switch in einer gemeinsam genutzten Konfiguration verwenden, die NS224-Shelfs verbindet, erfordert das Ändern der ISLs möglicherweise eine neue RCF-Datei. Sie benötigen keine neue RCF-Datei, wenn Ihre aktuelle und neue ISL-Geschwindigkeit 40 Gbit/s und 100 Gbit/s beträgt. Für alle anderen Änderungen an der ISL-Geschwindigkeit ist eine neue RCF-Datei erforderlich. Wenn Sie beispielsweise die ISL-Geschwindigkeit von 40 Gbit/s auf 100 Gbit/s ändern, ist keine neue RCF-Datei erforderlich, aber wenn Sie die ISL-Geschwindigkeit von 10 Gbit/s auf 40 Gbit/s ändern, ist eine neue RCF-Datei erforderlich.

Bevor Sie beginnen

Weitere Informationen finden Sie im Abschnitt **Schalter** des "NetApp Hardware Universe" Überprüfen der unterstützten Transceiver.

"Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Schritte

1. Deaktivieren Sie die ISL-Ports der ISLs auf beiden Switches in der Fabric, die Sie ändern möchten.

   > Die aktuellen ISL-Ports müssen nur deaktiviert werden, wenn sie zu einem anderen Port verschoben werden oder sich die Geschwindigkeit der ISL ändert. Wenn Sie einen ISL-Port mit derselben Geschwindigkeit wie die vorhandenen ISLs hinzufügen, fahren Sie mit Schritt 3 fort.

   Sie müssen nur einen Konfigurationsbefehl für jede Zeile eingeben und Strg-Z drücken, nachdem Sie alle Befehle eingegeben haben, wie im folgenden Beispiel dargestellt:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/24/1
   switch_A_1(config-if)# shut
   switch_A_1(config-if)#
   switch_A_1#

   switch_B_1# conf t
   switch_B_1(config)# int eth1/24/1
   switch_B_1(config-if)# shut
   switch_B_1(config-if)#
   switch_B_1#
   ```

2. Entfernen Sie die vorhandenen Kabel und Transceiver.
3. Ändern Sie den ISL-Port nach Bedarf.

> Wenn Sie Cisco 9336C-FX2-Switches in einer gemeinsam genutzten Konfiguration verwenden, die NS224-Shelfs verbindet, und Sie die RCF-Datei aktualisieren und die neue Konfiguration für die neuen ISL-Ports anwenden müssen, befolgen Sie die Schritte unter "Aktualisieren Sie die RCF-Dateien auf MetroCluster IP-Switches."

Option	Schritt
So ändern Sie die Geschwindigkeit eines ISL-Ports:	Verkabeln Sie die neuen ISLs entsprechend ihrer Geschwindigkeit an die entsprechenden Ports. Sie müssen sicherstellen, dass diese ISL-Ports für Ihren Switch in der *MetroCluster IP Installation and Configuration* aufgeführt sind.
ISL hinzufügen…	Fügen Sie QFSPs in die Ports ein, die Sie als ISL-Ports hinzufügen. Stellen Sie sicher, dass sie in der *MetroCluster IP-Installation und -Konfiguration* aufgeführt sind und verkabeln Sie sie entsprechend.

4. Aktivieren Sie alle ISL-Ports (falls nicht aktiviert) auf beiden Switches in der Fabric und beginnen Sie mit dem folgenden Befehl:

   ```
   switch_A_1# conf t
   ```

   Sie müssen nur einen Konfigurationsbefehl pro Zeile eingeben und Strg-Z drücken, nachdem Sie alle Befehle eingegeben haben:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/17
   switch_A_1(config-if)# no shut
   switch_A_1(config-if)# int eth1/18
   switch_A_1(config-if)# no shut
   switch_A_1(config-if)#
   switch_A_1#
   switch_A_1# copy running-config startup-config

   switch_B_1# conf t
   switch_B_1(config)# int eth1/17
   switch_B_1(config-if)# no shut
   switch_B_1(config-if)# int eth1/18
   switch_B_1(config-if)# no shut
   switch_B_1(config-if)#
   switch_B_1#
   switch_B_1# copy running-config startup-config
   ```

5. Überprüfen Sie, ob die ISLs und Port-Kanäle für die ISLs zwischen beiden Switches eingerichtet sind:

```
switch_A_1# show int brief
```

Die ISL-Schnittstellen in der Befehlsausgabe sollten wie im folgenden Beispiel gezeigt werden:

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                 Speed
Port
Interface
Ch #
--------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. Wiederholen Sie das Verfahren für Stoff 2.

Identifizierung des Storage in einer MetroCluster IP-Konfiguration

Wenn Sie ein Laufwerk- oder Shelf-Modul ersetzen müssen, müssen Sie zunächst den Standort identifizieren.

Identifizierung lokaler und Remote-Shelfs

Wenn Sie Shelf-Informationen von einem MetroCluster-Standort aus anzeigen, befinden sich alle Remote-Laufwerke auf 0 m, dem virtuellen iSCSI-Host-Adapter. Das bedeutet, dass über die MetroCluster IP Schnittstellen auf die Laufwerke zugegriffen wird. Alle anderen Laufwerke sind lokal.

Nachdem Sie erkannt haben, ob ein Shelf Remote ist (auf 0m), können Sie das Laufwerk oder Shelf nach der Seriennummer oder, abhängig von den Shelf-ID-Zuordnungen in Ihrer Konfiguration, nach Shelf-ID identifizieren.

> Bei MetroCluster IP-Konfigurationen mit ONTAP 9.4 muss die Shelf-ID nicht zwischen den MetroCluster Standorten eindeutig sein. Hierzu zählen sowohl interne als auch externe Shelfs. Die Seriennummer ist konsistent, wenn sie von einem beliebigen Node auf einem MetroCluster Standort aus angezeigt wird.

Shelf-IDs sollten innerhalb der Disaster Recovery-Gruppe (DR) eindeutig sein, außer im internen Shelf.

Wenn das Laufwerk- oder Shelf-Modul identifiziert wurde, können Sie die Komponente durch das entsprechende Verfahren ersetzen.

"Aufrechterhaltung der Festplatten-Shelfs DS460C DS224C und DS212C"

Beispiel einer Ausgabe von sysconfig -a

Im folgenden Beispiel wird das verwendet `sysconfig -a` Befehl zum Anzeigen der Geräte auf einem Knoten in der MetroCluster IP-Konfiguration. Dieser Node ist mit den folgenden Shelfs und Geräten verbunden:

- Steckplatz 0: Interne Laufwerke (lokale Laufwerke)
- Steckplatz 3: Externe Shelf-ID 75 und 76 (lokale Laufwerke)
- Steckplatz 0: Virtueller iSCSI-Host-Adapter 0 m (Remote-Laufwerke)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
```

```
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
```

```
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

Hinzufügen von Shelfs zu einer MetroCluster IP mithilfe von Shared Storage MetroCluster Switches

Möglicherweise müssen Sie einem MetroCluster NS224-Shelfs mit Shared-Storage-MetroCluster-Switches hinzufügen.

Ab ONTAP 9.10.1 können Sie NS224-Shelfs von einem MetroCluster aus mithilfe der Shared Storage-/MetroCluster-Switches hinzufügen. Sie können mehrere Shelfs gleichzeitig hinzufügen.

Bevor Sie beginnen

- Nodes müssen ONTAP 9.9.1 oder höher ausführen.
- Alle derzeit verbundenen NS224-Shelfs müssen mit den gleichen Switches verbunden sein wie die MetroCluster (Konfiguration für Shared Storage/MetroCluster-Switches).
- Mit diesem Verfahren können Konfigurationen nicht mit direkt verbundenen NS224-Shelfs oder mit dedizierten Ethernet-Switches verbundenen NS224-Shelfs in eine Konfiguration mit Shared Storage/MetroCluster-Switches umgewandelt werden.
- "Aktivieren Sie die Konsolenprotokollierung" Bevor Sie diese Aufgabe ausführen.

Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung

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

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit das Upgrade ausgeführt wird.

a. Geben Sie den folgenden Befehl ein:

```
system node autosupport invoke -node * -type all -message "Maint=10h Adding
or Removing NS224 shelves"_
```

Dieses Beispiel gibt ein Wartungsfenster von 10 Stunden an. Je nach Plan sollten Sie möglicherweise zusätzliche Zeit einplanen.

Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

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

a. Wiederholen Sie den Befehl im Partner-Cluster.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie müssen den Zustand und die Konnektivität der MetroCluster Konfiguration vor der Durchführung der Transition überprüfen.

Schritte

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

   a. Prüfen Sie, ob das System multipathed ist:

   ```
   node run -node node-name sysconfig -a
   ```

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

   ```
   system health alert show
   ```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

   ```
   metrocluster show
   ```

   d. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   f. Nutzen Sie Config Advisor.

   "NetApp Downloads: Config Advisor"

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

2. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

3. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

   `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

   `network interface show -vserver Cluster`

   Jede Cluster-LIF sollte True für IS Home anzeigen und einen Status Admin/Oper von up/Up haben

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Vergewissern Sie sich, dass die automatische Umrüstung auf allen Cluster-LIFs aktiviert ist:

   ```
   network interface show -vserver Cluster -fields auto-revert
   ```

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Anwenden der neuen RCF-Datei auf die Switches

> Wenn Ihr Switch bereits richtig konfiguriert ist, können Sie diese nächsten Abschnitte überspringen und direkt zu gehen Konfiguration der MACsec-Verschlüsselung bei Cisco 9336C-Switches, Sofern zutreffend oder für Anschließen des neuen NS224-Regals.

- Sie müssen die Switch-Konfiguration ändern, um Shelfs hinzuzufügen.
- Sie sollten sich die Details zur Verkabelung unter ansehen "Zuweisung von Plattform-Ports".
- Sie müssen das **RcfFileGenerator**-Tool verwenden, um die RCF-Datei für Ihre Konfiguration zu erstellen. Der "RCfFileGenerator" Bietet außerdem eine Übersicht über die Verkabelung pro Port für jeden Switch. Stellen Sie sicher, dass Sie die richtige Anzahl an Shelves auswählen. Es gibt zusätzliche Dateien, die zusammen mit der RCF-Datei erstellt werden, die ein detailliertes Verkabelungslayout bieten, das Ihren spezifischen Optionen entspricht. Mithilfe dieser Verkabelungsübersicht können Sie bei der Verkabelung der neuen Shelves Ihre Verkabelung überprüfen.

Aktualisieren von RCF-Dateien auf MetroCluster IP-Switches

Wenn Sie neue Switch-Firmware installieren, müssen Sie die Switch-Firmware installieren, bevor Sie die RCF-Datei aktualisieren.

Dieses Verfahren unterbricht den Datenverkehr auf dem Switch, auf dem die RCF-Datei aktualisiert wird. Der Datenverkehr wird wieder aufgenommen, sobald die neue RCF-Datei angewendet wurde.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführung `metrocluster check show` Um die Ergebnisse anzuzeigen.

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Um den Status des laufenden MetroCluster-Prüfvorgangs zu überprüfen, verwenden Sie den Befehl: **`metrocluster operation history show -job-id 38`**

b. Stellen Sie sicher, dass es keine Zustandswarnmeldungen gibt: **`system health alert show`**

2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen

Bevor Sie eine neue Softwareversion und RCFs installieren, müssen Sie die Cisco Switch-Konfiguration löschen und eine grundlegende Konfiguration durchführen.

Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

a. Löschen Sie die vorhandene Konfiguration: `write erase`

b. Laden Sie die Switch-Software neu: `reload`

Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung Auto Provisioning abbrechen und mit der normalen Einrichtung fortfahren?(ja/nein)[n], sollten Sie antworten `yes` Fortfahren.

c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:

- Admin-Passwort
- Switch-Name
- Out-of-Band-Managementkonfiguration
- Standard-Gateway
- SSH-Service (RSA) nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

   Das folgende Beispiel zeigt die Eingabeaufforderungen und Systemantworten bei der Konfiguration des Switches. Die Winkelklammern (`<<<`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

   Sie geben grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Managementadresse und Gateway, und wählen SSH mit RSA aus.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
   Number of rsa key bits <1024-2048> [1024]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Reihe von Eingabeaufforderungen vervollständigt die Konfiguration:

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[##########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch-A-1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch-A-1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco Switch NX-OS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Software-Download"

2. Kopieren Sie die Switch-Software auf den Switch: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In diesem Beispiel wird die Datei nxos.7.0.3.I4.6.bin vom SFTP-Server 10.10.99.99 auf den lokalen Bootflash kopiert:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind: `dir bootflash:`

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software: `install all nxos bootflash:nxos.version-number.bin`

   Der Switch wird automatisch neu geladen (neu gestartet), nachdem die Switch-Software installiert wurde.

   Das folgende Beispiel zeigt die Softwareinstallation auf IP_Switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
-- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Vergewissern Sie sich, dass die Switch-Software installiert ist: `show version`

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Konfiguration der MACsec-Verschlüsselung bei Cisco 9336C-Switches

Auf Wunsch können Sie die MACsec-Verschlüsselung für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

Die MACsec-Verschlüsselung kann nur auf die WAN-ISL-Ports angewendet werden.

Lizenzierungsanforderungen für MACsec

MACsec erfordert eine Sicherheitslizenz. Eine vollständige Erläuterung des Cisco NX-OS-Lizenzschemas und der Beschaffung und Anwendung von Lizenzen finden Sie im "Cisco NX-OS Licensing Guide"

Aktivierung von Cisco MACs Encryption WAN-ISLs in MetroCluster IP-Konfigurationen

Sie können die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration aktivieren.

1. Den globalen Konfigurationsmodus aufrufen: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Aktivieren Sie MACsec und MKA auf dem Gerät: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Kopieren Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Deaktivieren von Cisco MACsec Encryption

Möglicherweise müssen Sie die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration deaktivieren.

Wenn Sie die Verschlüsselung deaktivieren, müssen Sie auch Ihre Schlüssel löschen.

1. Den globalen Konfigurationsmodus aufrufen: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Deaktivieren Sie die MACsec-Konfiguration auf dem Gerät: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Durch Auswahl der Option „Keine“ wird die Funktion „MACsec“ wiederhergestellt.

3. Wählen Sie die Schnittstelle aus, die Sie bereits mit MACsec konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Entfernen Sie die auf der Schnittstelle konfigurierte Schlüsselanhänger, Richtlinie und Fallback-keychain, um die MACsec-Konfiguration zu entfernen: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
   keychain fb_kc2
   ```

5. Wiederholen Sie die Schritte 3 und 4 auf allen Schnittstellen, für die MACsec konfiguriert ist.
6. Kopieren Sie die laufende Konfiguration in die Startkonfiguration: `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Konfigurieren einer MACsec-Schlüsselkette und -Tasten

Weitere Informationen zur Konfiguration einer MACsec-Schlüsselkette finden Sie in der Cisco-Dokumentation für Ihren Switch.

Anschließen des neuen NS224-Regals

Schritte

1. Installieren Sie das im Lieferumfang des Regals beiliegte Schienensatz mithilfe des im Kit enthaltenen Installationsflyers.
2. Montieren und befestigen Sie das Regal mithilfe des Installationsflyers an den Halterungen und Rack oder Schrank.
3. Schließen Sie die Stromkabel an das Shelf an, befestigen Sie sie in der Kabelhalterung, und schließen Sie die Netzkabel anschließend an verschiedene Stromquellen an, um für Ausfallsicherheit zu sorgen.

   Ein Shelf schaltet sich ein, wenn es mit einer Stromquelle verbunden ist. Es verfügt nicht über Netzschalter. Bei ordnungsgemäßer Funktion leuchtet die zweifarbige LED des Netzteils grün.

4. Legen Sie die Shelf-ID auf eine Zahl fest, die innerhalb des HA-Paars und über die Konfiguration eindeutig ist.
5. Verbinden Sie die Shelf-Ports in folgender Reihenfolge:
   a. NSM-A, e0a mit dem Switch verbinden (Switch-A1 oder Switch-B1)
   b. NSM-B, e0a mit dem Switch verbinden (Switch-A2 oder Switch-B2)

c. Verbinden Sie NSM-A, e0b mit dem Switch (Switch-A1 oder Switch-B1).

d. Verbinden Sie NSM-B, e0b mit dem Switch (Switch-A2 oder Switch-B2).

6. Verwenden Sie das aus dem **RcfFileGenerator**-Werkzeug generierte Verkabelungslayout, um das Shelf mit den entsprechenden Ports zu verkabeln.

   Sobald das neue Shelf ordnungsgemäß verkabelt ist, erkennt ONTAP es automatisch im Netzwerk.

Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration

Ab ONTAP 9.15.1 können Sie auf unterstützten Systemen eine End-to-End-Verschlüsselung konfigurieren, um Back-End-Verkehr, wie z. B. NVlog- und Speicherreplikationsdaten, zwischen den Standorten in einer MetroCluster -IP -Konfiguration zu verschlüsseln.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Bevor Sie die End-to-End-Verschlüsselung konfigurieren können, müssen Sie dies tun "Externes Verschlüsselungsmanagement konfigurieren".
- Prüfen Sie die unterstützten Systeme und die Mindestversion von ONTAP, die erforderlich sind, um die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration zu konfigurieren:

Minimale ONTAP-Version	Unterstützte Systeme
ONTAP 9.17.1	• AFF A800, AFF C800 • AFF A20, AFF A30, AFF C30, AFF A50, AFF C60 • AFF A70, AFF A90, AFF A1K, AFF C80 • FAS50, FAS70 UND FAS90
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700

End-to-End-Verschlüsselung

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu aktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

```
metrocluster check show
```

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

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

3. End-to-End-Verschlüsselung für jede DR-Gruppe aktivieren:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung aktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

End-to-End-Verschlüsselung deaktivieren

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu deaktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

```
metrocluster check show
```

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

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

3. Deaktivieren Sie die End-to-End-Verschlüsselung für jede DR-Gruppe:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung deaktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

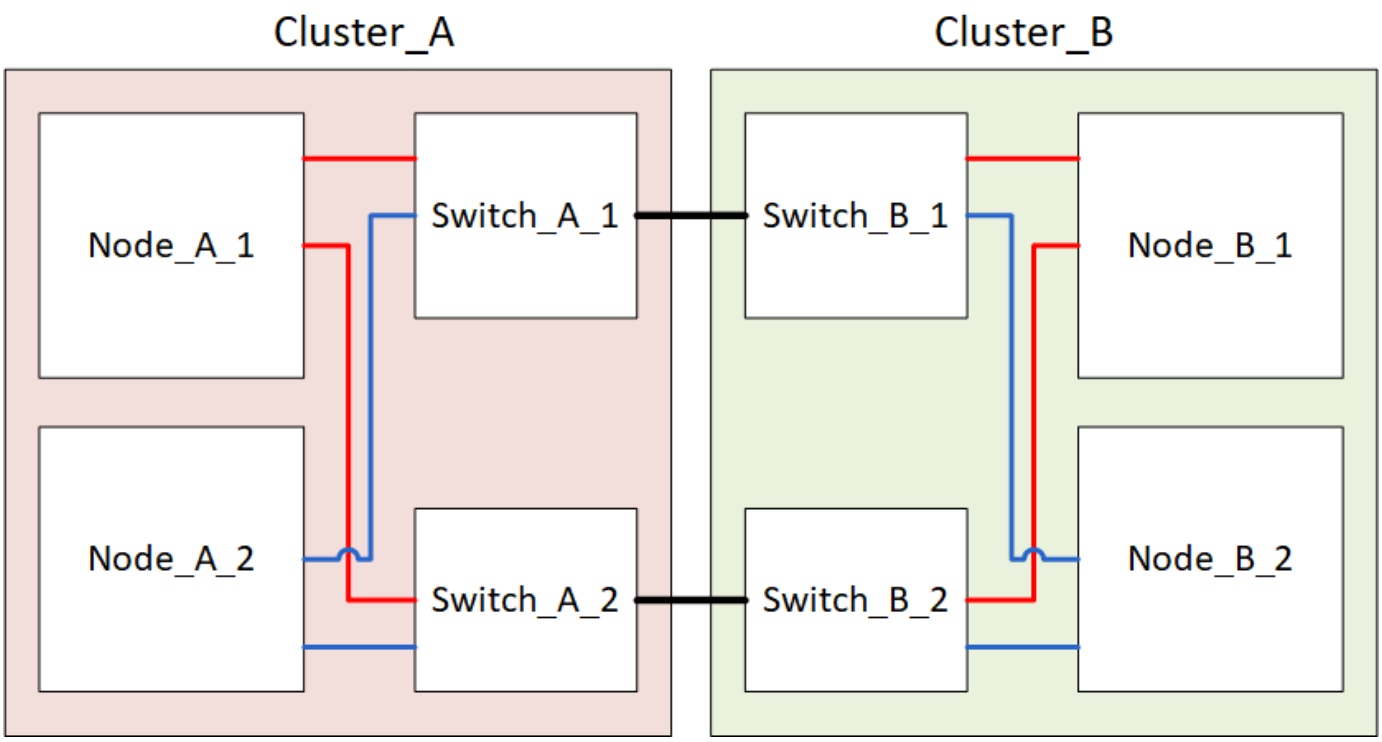
```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Schalten Sie einen einzelnen Standort in einer MetroCluster IP-Konfiguration aus und wieder ein

Wenn Sie eine Standortwartung durchführen oder einen einzelnen Standort in einer MetroCluster IP-Konfiguration verlagern müssen, müssen Sie wissen, wie Sie den Standort ausschalten und einschalten müssen.

Wenn Sie einen Standort verschieben und neu konfigurieren müssen (wenn Sie z. B. von einem Cluster mit vier Nodes auf ein Cluster mit acht Nodes erweitern müssen), können diese Aufgaben nicht gleichzeitig ausgeführt werden. Dieser Vorgang deckt nur die Schritte ab, die zur Durchführung von Wartungsarbeiten am Standort oder zum Standortwechsel ohne Änderung der Konfiguration erforderlich sind.

Das folgende Diagramm zeigt eine MetroCluster-Konfiguration. Cluster_B wird aus Wartungszwecken ausgeschaltet.



Schalten Sie einen MetroCluster-Standort aus

Sie müssen einen Standort und die gesamte Ausrüstung abschalten, bevor die Wartung oder der Standortwechsel beginnen können.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von dem Standort ausgegeben, der weiterhin eingeschaltet bleibt.

Schritte

1. Bevor Sie beginnen, überprüfen Sie, ob alle nicht gespiegelten Aggregate am Standort offline sind.
2. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      ```
      system health alert show
      ```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

      ```
      metrocluster show
      ```

   d. Führen Sie eine MetroCluster-Prüfung durch:
      `metrocluster check run`
   e. Ergebnisse der MetroCluster-Prüfung anzeigen:

      ```
      metrocluster check show
      ```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

3. Implementieren Sie von dem Standort aus, an dem Sie weiterhin arbeiten möchten, die Umschaltung:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Der Vorgang kann einige Minuten dauern.

4. Überwachen und überprüfen Sie den Abschluss der Umschaltung:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Wenn Sie eine MetroCluster IP-Konfiguration mit ONTAP 9.6 oder höher ausführen, warten Sie, bis die Plexe der Disaster-Site online geschaltet sind und die Heilungsvorgänge automatisch abgeschlossen sind.

Bei MetroCluster IP-Konfigurationen mit ONTAP 9.5 oder älteren Versionen werden die Knoten der Disaster-Standorte nicht automatisch von ONTAP gebootet, und die Plexe bleiben offline.

6. Verschieben Sie alle Volumes und LUNs, die zu nicht gespiegelten Aggregaten gehören, offline.

a. Verschieben Sie die Volumes in den Offline-Modus.

```
cluster_A::* volume offline <volume name>
```

b. Verschieben Sie die LUNs in den Offline-Modus.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Nicht gespiegelte Aggregate lassen sich offline verschieben: `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. Identifizieren und verschieben Sie je nach Konfiguration und ONTAP-Version die betroffenen Plexe, die sich am Disaster-Standort (Cluster_B) befinden, offline.

   Sie sollten die folgenden Plexe offline verschieben:

   - Nicht gespiegelte Plexe befinden sich auf Festplatten am DR-Standort.

     Wenn Sie die nicht gespiegelten Plexe am Disaster-Standort nicht offline schalten, kann es zu einem Ausfall kommen, wenn der Disaster-Standort später ausgeschaltet wird.

   - Gespiegelte Plexe auf Festplatten am Disaster Site zur Aggregatspiegelung Nachdem sie offline verschoben wurden, sind die Plexe nicht mehr zugänglich.

   a. Identifizieren Sie die betroffenen Plexe.

      Plexe, die Nodes auf dem verbleibenden Platz gehören, bestehen aus Pool1-Festplatten. Plexe, die im Eigentum von Nodes am Disaster-Site sind, bestehen aus Pool0-Platten.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

Die betroffenen Plexe sind diejenigen, die Remote zu Cluster A sind In der folgenden Tabelle wird gezeigt, ob die Festplatten lokal oder Remote relativ zu Cluster A sind:

Knoten	Disks im Pool	Sollten die Festplatten offline geschaltet werden?	Beispiel für Plexe, die offline verschoben werden sollen
Node_A_1 und Node_A_2	Laufwerke im Pool 0	Nein Festplatten sind lokal für Cluster A	-

Festplatten in Pool 1	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Node _B_1 und Node _B_2
Laufwerke im Pool 0	Ja. Die Festplatten befinden sich Remote auf Cluster A	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Festplatten in Pool 1

b. Verschieben Sie die betroffenen Plexe offline:

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

> Führen Sie diesen Schritt für alle Plexe aus, die über Remote-Festplatten für Cluster_A verfügen

9. Die ISL-Switch-Ports werden je nach Switch-Typ permanent offline geschaltet.
10. Beenden Sie die Nodes, indem Sie für jeden Node den folgenden Befehl ausführen:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Schalten Sie die Geräte am DR-Standort aus.

    Sie müssen die folgenden Geräte in der angegebenen Reihenfolge ausschalten:

    - Speicher-Controller: Die Speicher-Controller sollten sich derzeit am befinden `LOADER` Sie müssen sie vollständig ausschalten.
    - MetroCluster IP-Switches
    - Storage Shelfs

Verlagerung des ausgeschalteten Standorts des MetroCluster

Nachdem der Standort ausgeschaltet ist, können Sie mit der Wartung beginnen. Das Verfahren ist dasselbe, ob die MetroCluster Komponenten innerhalb desselben Datacenters verlegt oder in ein anderes Datacenter verlagert werden.

- Die Hardware sollte auf die gleiche Weise wie der vorherige Standort verkabelt werden.
- Wenn sich die Geschwindigkeit, Länge oder Zahl der Inter-Switch-Verbindung (ISL) geändert hat, müssen

alle neu konfiguriert werden.

Schritte

1. Vergewissern Sie sich, dass die Verkabelung aller Komponenten sorgfältig aufgezeichnet wurde, damit sie am neuen Standort wieder richtig angeschlossen werden kann.
2. Verlagern Sie physisch die gesamte Hardware, Speichercontroller, IP-Switches und Speicherregale.
3. Konfiguration der ISL-Ports und Überprüfung der Konnektivität zwischen Standorten
   a. Schalten Sie die IP-Switches ein.

   > Schalten Sie keine anderen Geräte ein.

4. Überprüfen Sie mithilfe von Tools auf den Switches (wie sie verfügbar sind) die Verbindung zwischen den Standorten.

   > Sie sollten nur fortfahren, wenn die Links korrekt konfiguriert und stabil sind.

5. Deaktivieren Sie die Links erneut, wenn sie stabil sind.

Einschalten der MetroCluster-Konfiguration und Zurückkehren zum normalen Betrieb

Nach Abschluss der Wartung oder Verschieben des Standorts müssen Sie den Standort einschalten und die MetroCluster Konfiguration wiederherstellen.

Über diese Aufgabe

Alle Befehle in den folgenden Schritten werden von der Website ausgegeben, die Sie einschalten.

Schritte

1. Schalten Sie die Schalter ein.

   Schalten Sie die Schalter zuerst ein. Möglicherweise wurden sie im vorherigen Schritt eingeschaltet, wenn der Standort verlegt wurde.

   a. Konfigurieren Sie den Inter-Switch Link (ISL), falls erforderlich, oder falls dieser nicht Teil der Verschiebung abgeschlossen wurde.
   b. ISL aktivieren, falls Fechten abgeschlossen wurde.
   c. ISL überprüfen.

2. Schalten Sie die Storage-Controller ein, und warten Sie, bis die angezeigt wird `LOADER` Eingabeaufforderung: Die Controller dürfen nicht vollständig gebootet werden.

   Wenn der automatische Start aktiviert ist, drücken Sie `Ctrl+C` Um das automatische Booten der Controller zu stoppen.

   > Schalten Sie die Shelfs vor dem Einschalten der Controller nicht ein. Dadurch wird verhindert, dass die Controller unbeabsichtigt in ONTAP booten.

3. Schalten Sie die Shelfs ein, damit sie sich vollständig einschalten können.
4. Überprüfen Sie, ob der Speicher im Wartungsmodus sichtbar ist.
   a. Booten Sie in den Wartungsmodus:

```
boot_ontap maint
```

b. Vergewissern Sie sich, dass der Speicher vom verbleibenden Standort aus sichtbar ist.

c. Überprüfen Sie, ob der lokale Speicher vom Knoten im Wartungsmodus aus sichtbar ist:

```
disk show -v
```

5. Anhalten der Knoten:

```
halt
```

6. Wiederherstellung der MetroCluster-Konfiguration

   Befolgen Sie die Anweisungen unter "Überprüfen, ob das System für einen Wechsel bereit ist" Um Healing- und Switchback-Vorgänge gemäß Ihrer MetroCluster-Konfiguration durchzuführen.

Ausschalten einer gesamten MetroCluster IP-Konfiguration

Bevor die Wartung oder Umsiedlung beginnen kann, müssen Sie die gesamte MetroCluster IP-Konfiguration und alle Geräte ausschalten.

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

1. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Konfiguration und der Betriebsmodus normal sind.
   `metrocluster show`

   b. Führen Sie den folgenden Befehl aus:
   `metrocluster interconnect show`

   c. Überprüfen Sie die Verbindung zu den Festplatten, indem Sie auf einem der MetroCluster-Knoten den folgenden Befehl eingeben:
   `run local sysconfig -v`

   d. Führen Sie den folgenden Befehl aus:
   `storage port show`

   e. Führen Sie den folgenden Befehl aus:
   `storage switch show`

   f. Führen Sie den folgenden Befehl aus:
   `network interface show`

   g. Führen Sie den folgenden Befehl aus:
   `network port show`

   h. Führen Sie den folgenden Befehl aus:
   `network device-discovery show`

   i. Führen Sie eine MetroCluster-Prüfung durch:
   `metrocluster check run`

j. Zeigen Sie die Ergebnisse der MetroCluster-Prüfung an:
metrocluster check show

k. Führen Sie den folgenden Befehl aus:
metrocluster configuration-settings interface show

2. Deaktivieren Sie gegebenenfalls AUSO, indem Sie die AUSO-Fehlerdomäne in ändern

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

> In einer MetroCluster-IP-Konfiguration ist die AUSO-Fehlerdomäne bereits auf „deaktiviert“ gesetzt, es sei denn, die Konfiguration ist mit dem ONTAP-Mediator konfiguriert.

3. Die Änderung wird mit dem Befehl überprüft

metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Anhalten der Knoten:

halt

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. Schalten Sie die folgenden Geräte am Standort aus:
   - Storage Controller
   - MetroCluster IP-Switches
   - Storage Shelfs
6. Warten Sie dreißig Minuten, und schalten Sie dann alle Storage Shelfs, MetroCluster IP Switches und Storage-Controller ein.
7. Nachdem die Controller eingeschaltet sind, überprüfen Sie die MetroCluster-Konfiguration von beiden Standorten aus.

   Um die Konfiguration zu überprüfen, wiederholen Sie Schritt 1.

8. Führen Sie Prüfungen der Einschaltzyklus durch.
   a. Vergewissern Sie sich, dass alle Sync-Source-SVMs online sind:
      `vserver show`
   b. Starten Sie alle Sync-Source-SVMs, die nicht online sind:
      `vserver start`

Wartungsverfahren für alle MetroCluster Konfigurationen

Unterbrechungsfreies Ersetzen eines Shelfs in einer Stretch-MetroCluster-Konfiguration

In einer Stretch MetroCluster Konfiguration können Sie Festplatten-Shelfs ohne Unterbrechungen durch ein vollständig bestücktes Festplatten-Shelf oder ein Festplatten-Shelf-Chassis ersetzen und Komponenten aus dem zu entfernenden Shelf übertragen.

Das installiertes Festplatten-Shelf-Modell muss die in angegebenen Anforderungen des Storage-Systems erfüllen "Hardware Universe", Die unterstützte Shelf-Modelle, unterstützte Festplattentypen, die maximale Anzahl an Platten-Shelfs in einem Stack und unterstützte ONTAP-Versionen umfasst.

Schritte

1. Richtig gemahlen.
2. Ermitteln Sie alle Aggregate und Volumes, deren Festplatten aus der Schleife enthalten sind, die das zu ersetzende Shelf enthält, und notieren Sie sich den betroffenen Plex-Namen.

   Jeder Node kann Festplatten aus dem Loop des betroffenen Shelf- und Host-Aggregaten oder Host-Volumes enthalten.

3. Wählen Sie basierend auf dem von Ihnen geplanten Ersatzszenario eine der folgenden zwei Optionen aus.
   - Wenn Sie ein vollständiges Festplatten-Shelf, einschließlich des Shelf-Chassis, Festplatten und I/O-Modulen (IOM), ersetzen, führen Sie die entsprechende Aktion durch, wie in der folgenden Tabelle beschrieben:

Szenario	Aktion
Der betroffene Plex enthält weniger Festplatten aus dem betroffenen Shelf.	Ersetzen Sie die Festplatten eins für eins auf dem betroffenen Regal durch Ersatzteile von einem anderen Regal. Nach Abschluss des Festplattenaustauschs können Sie den Plex offline schalten.
Der betroffene Plex enthält mehr Disks, als sich im betroffenen Shelf befinden.	Verschieben Sie den Plex offline und löschen Sie dann den Plex.
Der betroffene Plex enthält eine Festplatte aus dem betroffenen Shelf.	Verschieben Sie den Plex offline, aber löschen Sie ihn nicht.

- Wenn Sie nur das Festplatten-Shelf-Chassis ohne andere Komponenten ersetzen, führen Sie die folgenden Schritte aus:
  i. Offline die betroffenen Plexe vom Controller, auf dem sie gehostet werden:

     ```
     aggregate offline
     ```

  ii. Überprüfen Sie, ob die Plexe offline sind:

     ```
     aggregate status -r
     ```

4. Identifizieren Sie die Controller-SAS-Ports, mit denen die betroffene Shelf-Schleife verbunden ist, und deaktivieren Sie die SAS-Ports an beiden Standort-Controllern:

   `storage port disable -node` *`node_name`* `-port` *`SAS_port`*

   Die betroffene Shelf-Schleife ist mit beiden Standorten verbunden.

5. Warten Sie, bis ONTAP erkennt, dass die Festplatte fehlt.
   a. Vergewissern Sie sich, dass die Festplatte fehlt:

      `sysconfig -a` Oder `sysconfig -r`

6. Schalten Sie den Netzschalter am Festplatten-Shelf aus.
7. Ziehen Sie alle Netzkabel vom Festplatten-Shelf ab.
8. Erstellen Sie eine Aufzeichnung der Anschlüsse, von denen Sie die Kabel trennen, damit Sie das neue Platten-Shelf auf die gleiche Weise verkabeln können.
9. Trennen Sie die Kabel vom Festplatten-Shelf und entfernen Sie sie, um die anderen Festplatten-Shelfs oder das Speichersystem anzuschließen.
10. Entfernen Sie das Festplatten-Shelf aus dem Rack.

    Um das Platten-Shelf leichter und leichter zu manövrieren, entfernen Sie die Netzteile und das IOM. Wenn Sie ein Festplatten-Shelf-Chassis installieren, entfernen Sie auch die Festplattenlaufwerke oder Laufwerksträger. Vermeiden Sie andernfalls, wenn möglich, das Entfernen von Festplattenlaufwerken oder Trägern, da ein übermäßiges Handling zu einer Beschädigung des internen Laufwerks führen kann.

11. Installieren und befestigen Sie das Ersatz-Festplatten-Shelf an den Halterungen und am Rack.
12. Wenn Sie ein Festplatten-Shelf-Chassis installiert haben, installieren Sie die Netzteile und IOM neu.
13. Konfigurieren Sie den Stack der Festplatten-Shelfs neu, indem Sie alle Kabel mit den Ersatz-Festplatten-Shelf-Ports genau so verbinden, wie sie auf dem entfernten Festplatten-Shelf konfiguriert wurden.
14. Schalten Sie das Ersatz-Festplatten-Shelf ein und warten Sie, bis die Festplatten erweitert werden.
15. Ändern Sie die Festplatten-Shelf-ID in eine eindeutige ID von 0 bis 98.
16. Aktivieren Sie alle SAS-Ports, die Sie zuvor deaktiviert haben.
    a. Warten Sie, bis ONTAP erkennt, dass die Festplatten eingesetzt wurden.
    b. Vergewissern Sie sich, dass die Festplatten eingesetzt sind:

       `sysconfig -a` Oder `sysconfig -r`

17. Wenn Sie das gesamte Festplatten-Shelf (Festplatten-Shelf-Chassis, Festplatten, IOM) ersetzen, führen

Sie die folgenden Schritte aus:

> Wenn Sie nur das Festplatten-Shelf-Chassis ohne weitere Komponenten ersetzen, fahren Sie mit Schritt 19 fort.

a. Legen Sie fest, ob die automatische Festplattenzuordnung aktiviert ist (ein).

```
storage disk option modify -autoassign
```

Die Festplattenzuordnung erfolgt automatisch.

a. Wenn die automatische Zuweisung der Festplatte nicht aktiviert ist, weisen Sie den Festplattenbesitzer manuell zu.

18. Verschieben Sie die Plexe wieder online:

```
aggregate online plex name
```

19. Erstellen Sie alle Plexe, die durch eine Spiegelung des Aggregats gelöscht wurden, neu.
20. Überwachen Sie die Plexe, wenn sie neu synchronisiert werden:

```
aggregate status -r <aggregate name>
```

21. Vergewissern Sie sich, dass das Storage-System wie erwartet funktioniert:

```
system health alert show
```

Wann werden Root-Volumes zu einem neuen Ziel migriert

Unter Umständen müssen Sie Root-Volumes in ein anderes Root-Aggregat innerhalb einer MetroCluster Konfiguration mit zwei oder vier Nodes verschieben.

Migration von Root-Volumes innerhalb einer MetroCluster Konfiguration mit zwei Nodes

Informationen zur Migration von Root-Volumes zu einem neuen Root-Aggregat innerhalb einer MetroCluster-Konfiguration mit zwei Nodes finden Sie unter "Verschieben von mroot zu einem neuen Root-Aggregat in einem Clustered MetroCluster mit 2 Nodes mit Switchover". Dieses Verfahren zeigt Ihnen, wie Sie die Root-Volumes während einer MetroCluster-Umschaltung unterbrechungsfrei migrieren. Dieses Verfahren unterscheidet sich leicht von dem Verfahren, das in einer Konfiguration mit vier Nodes verwendet wird.

Migration von Root-Volumes innerhalb einer MetroCluster Konfiguration mit vier Nodes

Um Root-Volumes innerhalb einer MetroCluster Konfiguration mit vier Nodes auf ein neues Root-Aggregat zu migrieren, können Sie das verwenden "System-Node-Migration-Root" Befehl und Erfüllung der folgenden Anforderungen.

- Mit System Node Migration-Root können Root-Aggregate in einer MetroCluster Konfiguration mit vier Nodes verschoben werden.
- Alle Root-Aggregate müssen gespiegelt werden.
- Sie können neue Shelves auf beiden Seiten mit kleineren Laufwerken hinzufügen, um das Root-Aggregat zu hosten.

- Vor dem Anschließen neuer Laufwerke müssen Sie die von der Plattform unterstützten Laufwerksgrenzen überprüfen.

  "NetApp Hardware Universe"

- Wenn Sie das Root-Aggregat auf kleinere Laufwerke verschieben, müssen Sie die minimale Root-Volume-Größe der Plattform berücksichtigen, um sicherzustellen, dass alle Kerndateien gespeichert werden.

> Das Verfahren mit vier Nodes kann auch auf eine Konfiguration mit acht Nodes angewendet werden.

Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen

Sie können ein Metadaten-Volume in eine MetroCluster Konfiguration von einem Aggregat zu einem anderen Aggregat verschieben. Unter Umständen möchten Sie ein Metadaten-Volume verschieben, wenn das Quellaggregat deaktiviert oder nicht gespiegelt wird, oder aus anderen Gründen, aus denen das Aggregat nicht mehr berechtigt ist.

- Um diese Aufgabe ausführen zu können, müssen Sie über Cluster-Administratorrechte verfügen.
- Das Zielaggregat muss gespiegelt werden und darf nicht im eingeschränkten Zustand sein.
- Der verfügbare Speicherplatz im Zielaggregat muss größer sein als das zu bewegende Metadaten-Volume.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Identifizierung des zu verschiebenden Metadaten-Volumes:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Ermittlung eines geeigneten Zielaggregats:

   `metrocluster check config-replication show-aggregate-eligibility`

   Mit dem folgenden Befehl werden die Aggregate in „Cluster_A“ identifiziert, die zum Hosten von Metadaten-Volumes geeignet sind:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

In dem vorherigen Beispiel können Node_A_1_aggr2 und Node_A_2_aggr2 ausgewählt werden.

4. Starten Sie die Volume-Verschiebung:

   volume move start -vserver *svm_name* -volume *metadata_volume_name* -destination -aggregate *destination_aggregate_name*

   Mit dem folgenden Befehl werden das Metadaten-Volume verschoben `MDV_CRS_14c00d4ac9f311e7922800a0984395f1` Von `aggregate Node_A_1_aggr1` Bis `aggregate Node_A_1_aggr2`:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Überprüfung des Status der Verschiebung eines Volumes:

   `volume move show -volume vol_constituent_name`

6. Zurück zur Administratorberechtigungsebene:

   `set -privilege admin`

Umbenennen eines Clusters in MetroCluster-Konfigurationen

Wenn Sie einen Cluster in einer MetroCluster-Konfiguration umbenennen, müssen die Änderungen vorgenommen und dann sowohl auf den lokalen als auch auf den Remote-Clustern überprüft werden, ob die Änderung ordnungsgemäß wirksam wurde.

Schritte

1. Zeigen Sie die Cluster-Namen mit an

   `metrocluster node show`

   Befehl:

   ```
   cluster_1::*> metrocluster node show
   DR                               Configuration  DR
   Group Cluster Node               State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_1
                 node_A_1           configured     enabled   normal
                 node_A_2           configured     enabled   normal
         cluster_2
                 node_B_1           configured     enabled   normal
                 node_B_2           configured     enabled   normal
   4 entries were displayed.
   ```

2. Umbenennen des Clusters:

   `cluster identity modify -name *new_name*`

   Im folgenden Beispiel wird der verwendet `cluster_1` Das Cluster wird umbenannt `cluster_A`:

   ```
   cluster_1::*> cluster identity modify -name cluster_A
   ```

3. Überprüfen Sie auf dem lokalen Cluster, ob das umbenannte Cluster ordnungsgemäß ausgeführt wird:

   `metrocluster node show`

   Im folgenden Beispiel wurde der neu umbenannt `cluster_A` Läuft normal:

```
cluster_A::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

4. Benennen Sie den Remote-Cluster um:

   `cluster peer modify-local-name -name cluster_2 -new-name cluster_B`

   Im folgenden Beispiel: `cluster_2` Wird umbenannt `cluster_B`:

```
cluster_A::> cluster peer modify-local-name -name cluster_2 -new-name
cluster_B
```

5. Überprüfen Sie auf dem Remote-Cluster, ob der lokale Cluster umbenannt wurde und ordnungsgemäß ausgeführt wird:

   `metrocluster node show`

   Im folgenden Beispiel wurde der neu umbenannt `cluster_B` Läuft normal:

```
cluster_B::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
      cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
4 entries were displayed.
```

6. Wiederholen Sie diese Schritte für jedes Cluster, das Sie umbenennen möchten.

Überprüfen Sie den Funktionszustand einer MetroCluster-Konfiguration

Erfahren Sie, wie Sie überprüfen, ob sich die MetroCluster Komponenten in einem ordnungsgemäßen Zustand befinden.

Über diese Aufgabe

- In MetroCluster IP- und FC-Konfigurationen können Sie die CLI verwenden, um Zustandspeckbefehle auszuführen und den Status der MetroCluster-Komponenten zu überprüfen.
- In MetroCluster IP-Konfigurationen, auf denen ONTAP 9 8 oder höher ausgeführt wird, können Sie auch ONTAP System Manager verwenden, um Warnmeldungen zur Integritätsprüfung zu überwachen und zu beheben.

Schritte

Überprüfen Sie den Systemzustand der MetroCluster Konfiguration in Abhängigkeit davon, ob Sie die CLI oder System Manager verwenden.

CLI

Führen Sie die folgenden Schritte aus, um den Systemzustand einer MetroCluster Konfiguration mithilfe der CLI zu überprüfen.

Schritte

1. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

Der Vorgang wird im Hintergrund ausgeführt.

2. Zeigen Sie nach Abschluss des `metrocluster check run` Vorgangs die Ergebnisse an:

```
metrocluster check show
```

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

3. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

4. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

ONTAP System Manager (nur MetroCluster IP)

Ab ONTAP 9.8 überwacht System Manager den Systemzustand der MetroCluster IP Konfigurationen und unterstützt Sie bei der Identifizierung und Behebung von möglicherweise auftretenden Problemen.

System Manager überprüft regelmäßig den Zustand Ihrer MetroCluster IP-Konfiguration. Wenn Sie den Abschnitt „MetroCluster“ auf dem Dashboard anzeigen, wird in der Regel die Meldung „MetroCluster-Systeme sind ordnungsgemäß“ ausgegeben.

Wenn jedoch ein Problem auftritt, wird in der Meldung die Anzahl der Ereignisse angezeigt. Sie können auf diese Meldung klicken und die Ergebnisse der Integritätsprüfung für die folgenden Komponenten anzeigen:

- Knoten
- Netzwerkschnittstelle
- Ebene (Storage)
- Cluster
- Verbindung
- Datenmenge
- Konfigurationsreplizierung

In der Spalte **Status** werden die Komponenten mit Problemen identifiziert, und in der Spalte **Details** wird erläutert, wie das Problem behoben werden kann.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Sehen Sie sich die Nachricht im Abschnitt **MetroCluster** an:
   a. Wenn die Meldung angibt, dass Ihre MetroCluster-Konfiguration ordnungsgemäß ist und die Verbindungen zwischen den Clustern und dem ONTAP Mediator in einem ordnungsgemäßen Zustand sind (siehe Häkchen), können Sie keine Probleme beheben.
   b. Wenn die Meldung die Anzahl der Ereignisse auflistet oder die Verbindungen (mit einem „X“ angezeigt) abwärts gegangen sind, fahren Sie mit dem nächsten Schritt fort.
3. Klicken Sie auf die Nachricht, die die Anzahl der Ereignisse anzeigt.

   Der MetroCluster-Integritätsbericht wird angezeigt.
4. Beheben Sie die im Bericht angezeigten Probleme mithilfe der Vorschläge in der Spalte **Details**.
5. Wenn alle Probleme behoben wurden, klicken Sie auf **MetroCluster-Zustand prüfen**.

   > Sie sollten alle Fehlerbehebungsaufgaben ausführen, bevor Sie die Prüfung ausführen, da die MetroCluster-Integritätsprüfung eine intensive Menge an Ressourcen verwendet.

   Die MetroCluster-Integritätsprüfung wird im Hintergrund ausgeführt. Sie können andere Aufgaben bearbeiten, während Sie warten, bis der Vorgang abgeschlossen ist.

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration, Bedienung und Überwachung einer MetroCluster Konfiguration finden Sie in der umfassenden Dokumentation von NetApp.

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen
"Lösungsarchitektur und Design der NetApp MetroCluster Lösung"	• Eine technische Übersicht über Konfiguration und Betrieb von MetroCluster • Best Practices für die Konfiguration von MetroCluster.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von MetroCluster IP"	• MetroCluster IP Architektur • Verkabelung der MetroCluster IP-Konfiguration • Konfigurieren der MetroCluster in ONTAP
"NetApp Dokumentation: Produktleitfäden und Ressourcen"	• Monitoring der MetroCluster Konfiguration und Performance
"Installation und Konfiguration der MetroCluster Tiebreaker Software"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen

Umstellung von MetroCluster FC auf MetroCluster IP

Wählen Sie Ihr Übergangsverfahren

Beim Umstieg auf eine MetroCluster IP-Konfiguration müssen Sie über eine Kombination unterstützter Plattformmodelle verfügen.

Sie sollten außerdem sicherstellen, dass die MetroCluster IP-Plattform für die Auslastung geeignet ist, die Sie von der MetroCluster FC-Konfiguration auf die MetroCluster IP-Konfiguration umstellen.

Unterstützte Plattformkombinationen

- Für alle Umstiegsprozesse ist ONTAP 9.8 oder höher erforderlich, sofern in den Hinweisen oder den Voraussetzungen einer einzelnen Plattform nicht anders angegeben.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im"Hardware Universe".

- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielplattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster neu konfigurieren, damit sie die Grenzen der Zielplattform erreichen oder darunter liegen, bevor Sie die neuen Nodes hinzufügen.
- Siehe "Hardware Universe" Für Plattformgrenzen

Unterstützte AFF- und FAS-Übergangskombinationen

Die folgenden Tabellen zeigen die unterstützten Plattformkombinationen. Sie können von Plattformen in der ersten Spalte zu Plattformen wechseln, die in den Spalten nach rechts als unterstützt aufgeführt sind, wie durch die farbigen Tabellenzellen angegeben.

Beispielsweise wird der Wechsel von einer MetroCluster FC-Konfiguration aus AFF8060 Controller-Modulen zu einer IP-Konfiguration aus AFF A400 Controller-Modulen unterstützt.

Die Tabellen sind in zwei Gruppen aufgeteilt:

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

Die folgenden Hinweise gelten für beide Gruppen:

- Hinweis 1: Diese Plattform erfordert ONTAP 9.11.1 oder höher.
- Hinweis 2: Auf den FC-Nodes ist eine 40-GbE-Schnittstelle für die lokalen Cluster-Schnittstellen erforderlich.

- Hinweis 3: Auf FC-Nodes ist eine 100-GbE-Schnittstelle für die lokalen Cluster-Schnittstellen erforderlich.

AFF- und FAS-Kombinationen, Gruppe 1

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

AFF and FAS		Target MetroCluster IP platform									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300				Note 1						
	FAS8300 AFF A400										
	FAS9000 AFF A700										
	FAS9500 AFF A900										

AFF und FAS Kombinationsgruppe 2

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

AFF and FAS		Target MetroCluster IP platform									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300										
	FAS8300 AFF A400										
	FAS9000 AFF A700			Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2
	FAS9500 AFF A900							Note 3	Note 3	Note 3	Note 3

Unterstützte ASA-Plattformkombinationen für den Umstieg

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für ASA Systeme aufgeführt.

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

Wählen Sie Ihr Übergangsverfahren

Sie müssen ein Migrationsverfahren je nach Ihrer bestehenden MetroCluster FC-Konfiguration auswählen.

Ein Migrationsverfahren ersetzt das Back-End FC Switch Fabric oder die FC-VI-Verbindung durch ein IP Switch-Netzwerk. Die genaue Vorgehensweise hängt von Ihrer Startkonfiguration ab.

Die ursprünglichen Plattformen und FC Switches (falls vorhanden) werden am Ende des Umstiegsverfahrens außer Betrieb genommen.

Konfiguration wird gestartet	Unterbrechungsfrei oder unterbrechungsfrei	Anforderungen	Verfahren
Vier oder acht Nodes	Unterbrechungsfrei	Unterstützung neuer Storage Shelfs auf neuen Plattformen	"Link zum Verfahren"
Zwei Nodes	Unterbrechungen	Neue Storage Shelves werden sowohl auf ursprünglichen als auch auf neuen Plattformen unterstützt.	"Link zum Verfahren"
Zwei Nodes	Unterbrechungen	Neue Storage Shelves werden sowohl auf ursprünglichen als auch auf neuen Plattformen unterstützt. Alte Storage-Shelves müssen außer Betrieb genommen werden.	"Link zum Verfahren"

Zwei Nodes	Unterbrechungen	Alte Storage-Shelves werden auf neuen Plattformen nicht unterstützt. Alte Storage-Shelves müssen außer Betrieb genommen werden.	"Link zum Verfahren"

Unterbrechungsfreier Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration (ONTAP 9.8 und höher)

Unterbrechungsfreier Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration (ONTAP 9.8 und höher)

Sie können unterbrechungsfreie Übergänge von Workloads und Daten von einer bestehenden MetroCluster FC Konfiguration in eine neue MetroCluster IP Konfiguration durchführen.

Ab ONTAP 9.13.1 wird dieses Verfahren in MetroCluster IP-Konfigurationen unterstützt, bei denen die MetroCluster und die Festplatten-Shelfs mit denselben IP-Switches verbunden sind (eine Konfiguration mit einem Shared Storage Switch).

Ab ONTAP 9.13.1 lassen sich Workloads und Daten unterbrechungsfrei von einer bestehenden MetroCluster FC Konfiguration mit acht Nodes auf eine neue MetroCluster IP Konfiguration übertragen.

Ab ONTAP 9.8 lassen sich unterbrechungsfreie Workloads und Daten von einer bestehenden MetroCluster FC Konfiguration mit vier Nodes auf eine neue MetroCluster IP Konfiguration übertragen.

- Dieses Verfahren ist unterbrechungsfrei.

  Die MetroCluster Konfiguration kann während des Vorgangs weiterhin Daten bereitstellen.

- Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen mit vier und acht Nodes.

  Wenn Sie über eine MetroCluster-FC-Konfiguration mit zwei Nodes verfügen, finden Sie Informationen unter "Auswahl des Migrationsverfahrens".

- In diesem Verfahren werden die Schritte beschrieben, die für den Übergang einer FC-DR-Gruppe mit vier Nodes erforderlich sind. Wenn Sie über eine Konfiguration mit acht Nodes (zwei FC DR-Gruppen) verfügen, müssen Sie den gesamten Vorgang für jede FC DR-Gruppe wiederholen.
- Sie müssen alle Anforderungen erfüllen und alle Schritte des Verfahrens befolgen.

Wichtige Informationen

Während der Umstellungs-, Aktualisierungs- und Erweiterungsvorgänge können Sie Ihrer MetroCluster-Konfiguration ein neues Plattformmodell hinzufügen. Wenn Ihre vorhandene MetroCluster-Konfiguration zu irgendeinem Zeitpunkt eine Plattform mit **gemeinsamen Cluster-/HA-Ports** enthält, können Sie der Konfiguration keine Plattform mit **gemeinsamen MetroCluster-/HA-Ports** hinzufügen, ohne Ihre ONTAP-Version auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher zu aktualisieren.

Bevor Sie sich für dieses Verfahren entscheiden, lesen Sie die Informationen in der folgenden Tabelle sorgfältig durch. Wenn Ihre vorhandene Plattform in der ersten Spalte und die Plattform, die Sie der Konfiguration hinzufügen möchten, in der zweiten Spalte aufgeführt ist, müssen alle Knoten in der Konfiguration ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen, um dieses Verfahren zu unterstützen.

> Sowohl die vorhandene Plattform als auch die Plattform, die Sie der Konfiguration hinzufügen möchten, müssen ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen.

Wenn Ihr vorhandener MetroCluster Folgendes enthält:		**Und die Plattform, die Sie hinzufügen, ist …**		**Dann…**
Ein AFF-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	Ein FAS-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • FAS50 • FAS70 • FAS90	Ein AFF-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	Ein FAS-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500	Bevor Sie die neue Plattform zu Ihrer vorhandenen MetroCluster-Konfiguration hinzufügen, aktualisieren Sie alle Knoten in der vorhandenen und neuen Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher.

Vorbereitung auf den Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration

Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie diese Aufgabe ausführen.

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Anforderungen für einen unterbrechungsfreien FC-to-IP Umstieg

Vergewissern Sie sich vor Beginn des Wechsels, dass die Konfiguration den Anforderungen entspricht.

Sie können einen unterbrechungsfreien FC-zu-IP-Übergang durchführen, wenn Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Bei einer Konfiguration mit acht Nodes werden auf allen Nodes ONTAP 9.13.1 oder höher ausgeführt.
- Bei einer Konfiguration mit vier Nodes werden auf allen Nodes ONTAP 9.8 oder höher ausgeführt.
- Die bestehenden und neuen Plattformen sind eine unterstützte Kombination für den Übergang.

  "Unterstützte Plattformen für unterbrechungsfreien Übergang"

- Ihre Konfiguration unterstützt eine Cluster-Konfiguration mit Switches.

  "Hardware Universe"

> Bei Verwendung von Shared Storage MetroCluster Switches können Sie nur zu einer MetroCluster IP-Konfiguration mit vier Nodes wechseln. Der Übergang zu einer MetroCluster IP-Konfiguration mit acht Nodes unter Verwendung von MetroCluster-Switches für gemeinsamen Storage wird nicht unterstützt. Nachdem Sie den Übergang zu einer MetroCluster IP-Konfiguration mit vier Knoten abgeschlossen haben, können Sie "Erweitern Sie auf eine MetroCluster IP-Konfiguration mit acht Nodes".

- Ihre Konfiguration erfüllt alle Anforderungen und ist gemäß den folgenden *MetroCluster-Installations- und -Konfigurations* -Verfahren verkabelt.

  "Installation und Konfiguration von Fabric-Attached MetroCluster"

  "Installation und Konfiguration von Stretch MetroCluster"

Auswirkungen der Transition auf die Hardwarekomponenten von MetroCluster

Nach Abschluss des Umstiegverfahrens wurden wichtige Komponenten der bestehenden MetroCluster Konfiguration ersetzt oder neu konfiguriert.

- **Controller-Module**

  Die vorhandenen Controller-Module werden durch neue Controller-Module ersetzt. Die vorhandenen Controller-Module werden am Ende des Umstiegsprozesse deaktiviert.

- **Lagerregale**

  Die Daten werden von den alten Shelfs in die neuen Shelfs verschoben. Die alten Shelfs werden am Ende des Umstiegs deaktiviert.

- **MetroCluster (Back-End) und Cluster-Switches**

  Die Back-End-Switch-Funktion wird durch das IP Switch Fabric ersetzt. Wenn zur MetroCluster FC-Konfiguration FC-Switches und FC-to-SAS-Bridges verwendet wurden, werden sie am Ende dieses Verfahrens deaktiviert.

  Wenn die MetroCluster FC-Konfiguration Cluster Switches für den Cluster Interconnect verwendet hat, können sie in einigen Fällen wiederverwendet werden, um für das Back-End IP Switch Fabric zu sorgen. Zudem müssen wiederverwendet werden Cluster Switches mit Plattform- und Switch-spezifischen RCFs neu konfiguriert werden. Verfahren.

  Wenn die MetroCluster FC-Konfiguration keine Cluster Switches verwendet, werden neue IP-Switches hinzugefügt, um die Back-End Switch Fabric zu schaffen.

  "Überlegungen zu IP-Switches"

- **Cluster Peering Netzwerk**

  Das vom Kunden bereitgestellte Cluster-Peering-Netzwerk kann für die neue MetroCluster IP-Konfiguration verwendet werden. Cluster-Peering wird auf den MetroCluster IP Nodes im Rahmen des Übergangverfahrens konfiguriert.

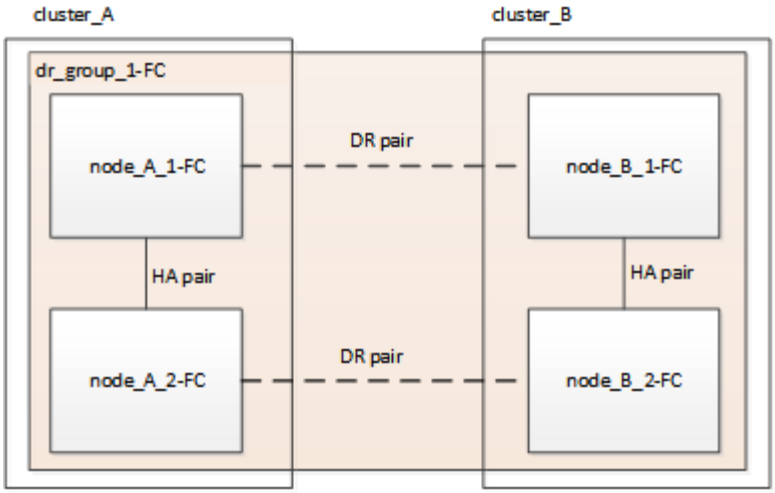
Workflow für unterbrechungsfreie MetroCluster Transition

Um einen erfolgreichen unterbrechungsfreien Übergang zu gewährleisten, müssen Sie die jeweiligen Workflows beachten. Wählen Sie den Workflow für Ihre Konfiguration aus:

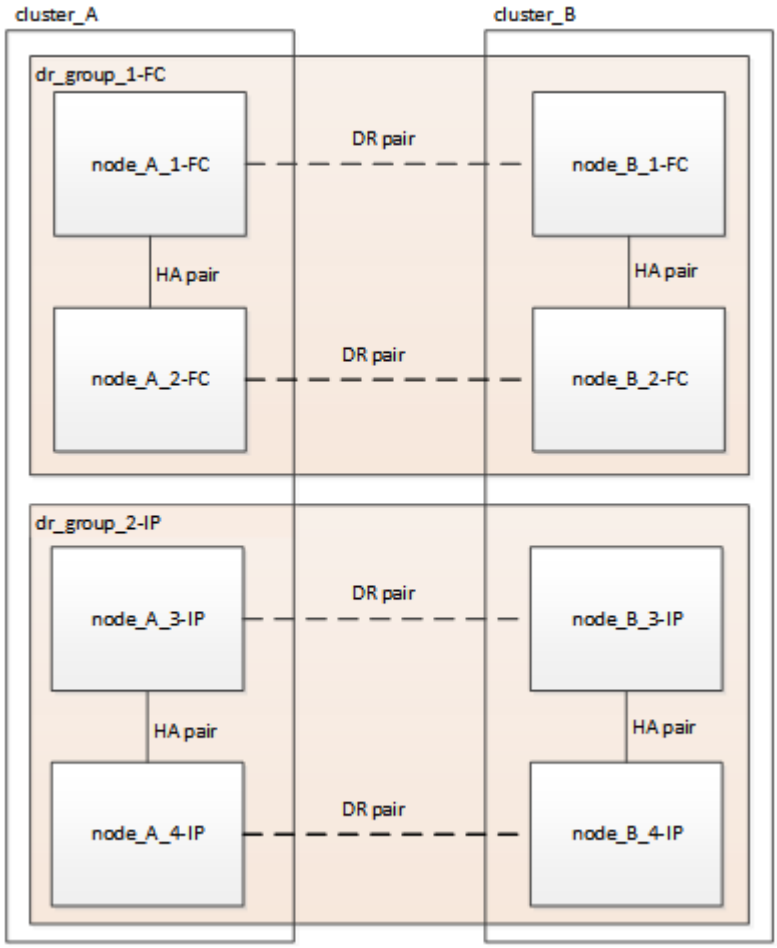
- Workflow zur Migration der FC-Konfiguration mit vier Nodes
- Workflow zur Migration der FC-Konfiguration mit acht Nodes

Workflow zur Migration der FC-Konfiguration mit vier Nodes

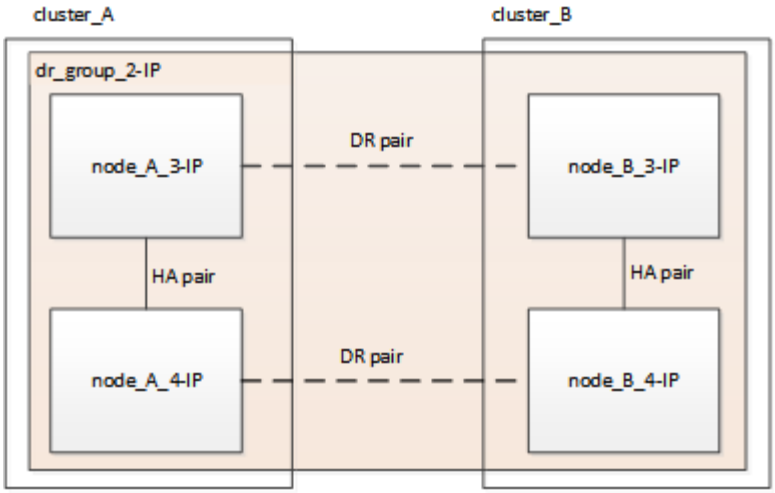
Der Umstellungsprozess beginnt mit einer soliden MetroCluster FC-Konfiguration mit vier Nodes.



Die neuen MetroCluster IP Knoten werden als zweite DR-Gruppe hinzugefügt.

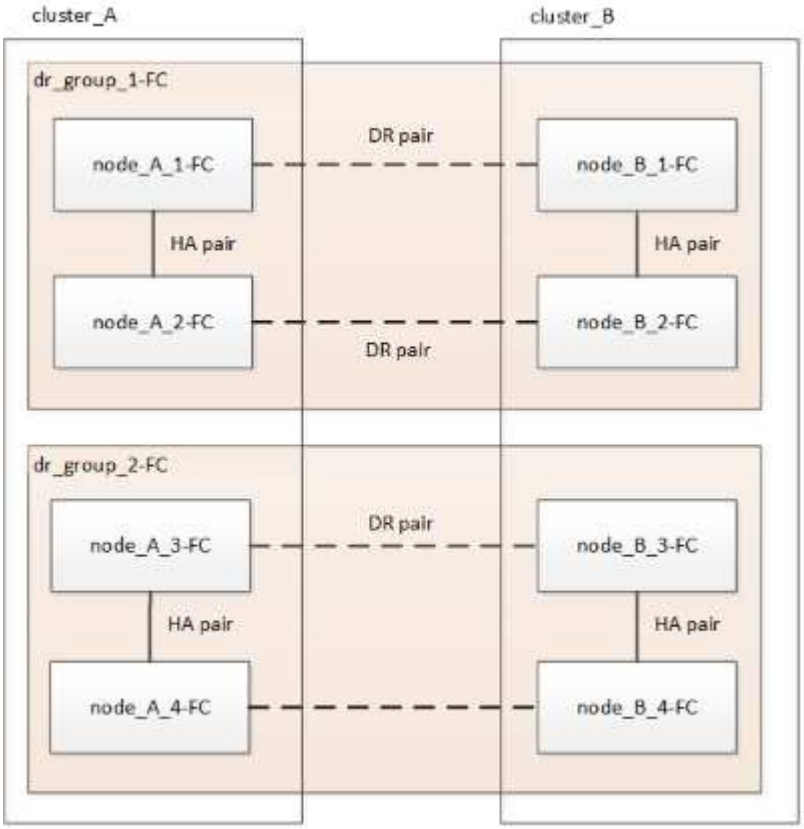


Die Daten werden von der alten DR-Gruppe zur neuen DR-Gruppe übertragen, gefolgt von den alten Nodes und ihrem Storage werden aus der Konfiguration entfernt und stillgelegt. Der Prozess endet mit einer MetroCluster IP-Konfiguration mit vier Nodes.

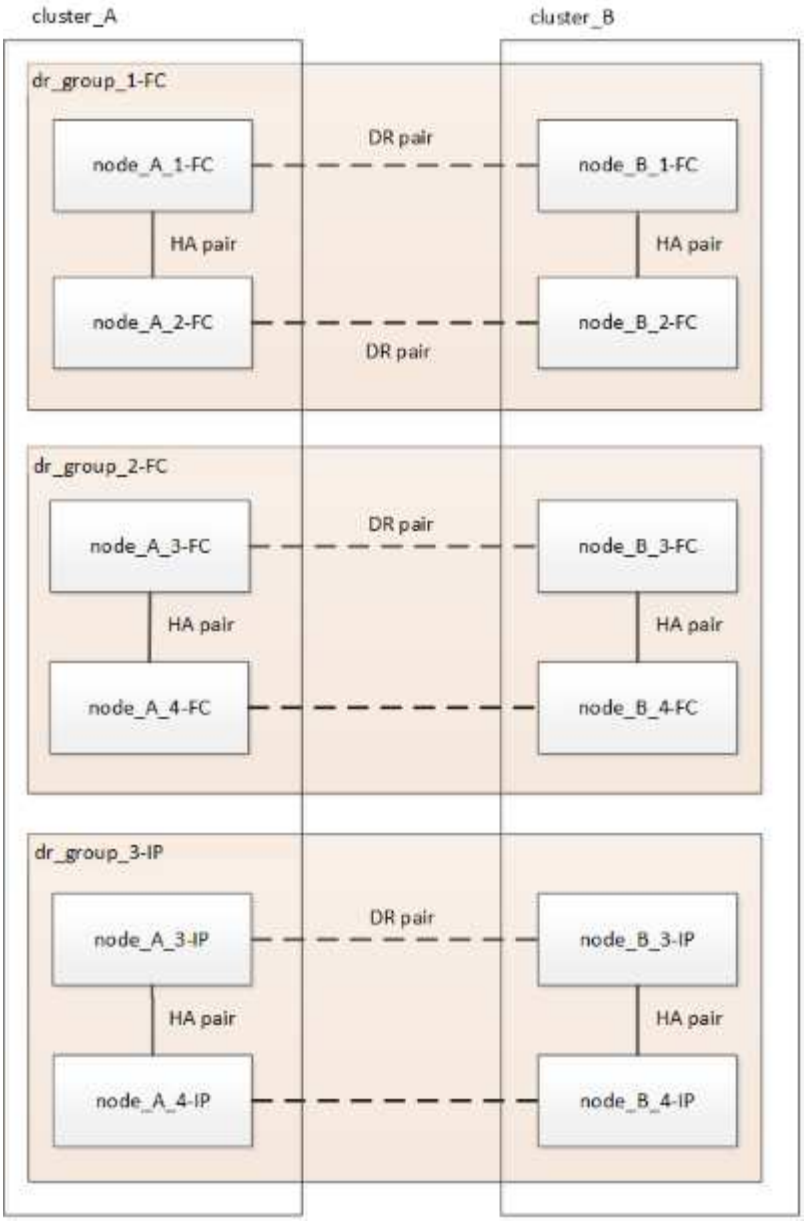


Workflow zur Migration der FC-Konfiguration mit acht Nodes

Der Wechsel beginnt mit einer funktionierenden MetroCluster FC-Konfiguration mit acht Nodes.

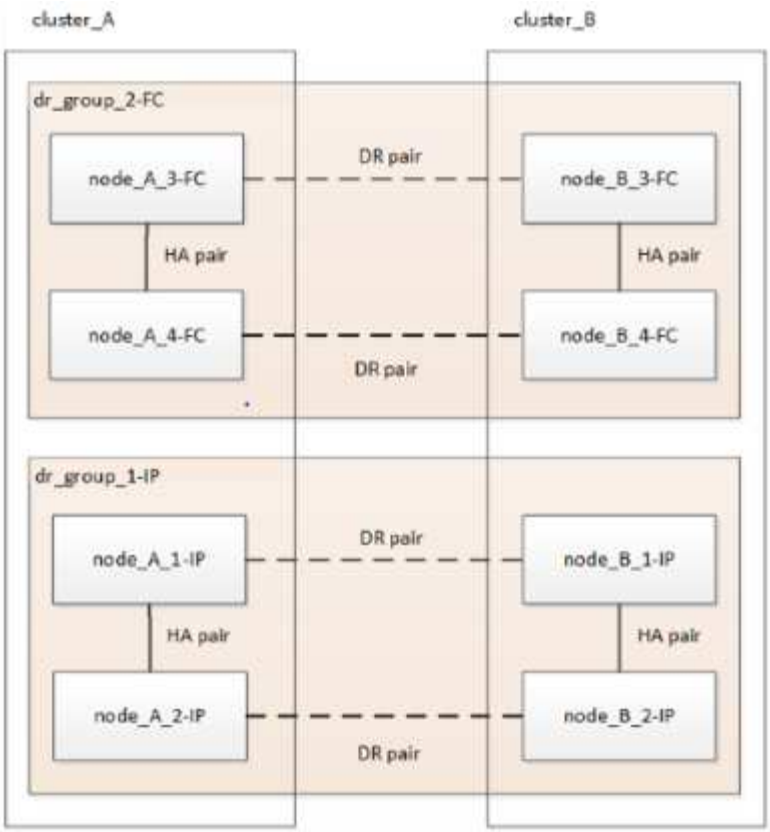


Die neuen MetroCluster IP Nodes werden als dritte DR-Gruppe hinzugefügt.

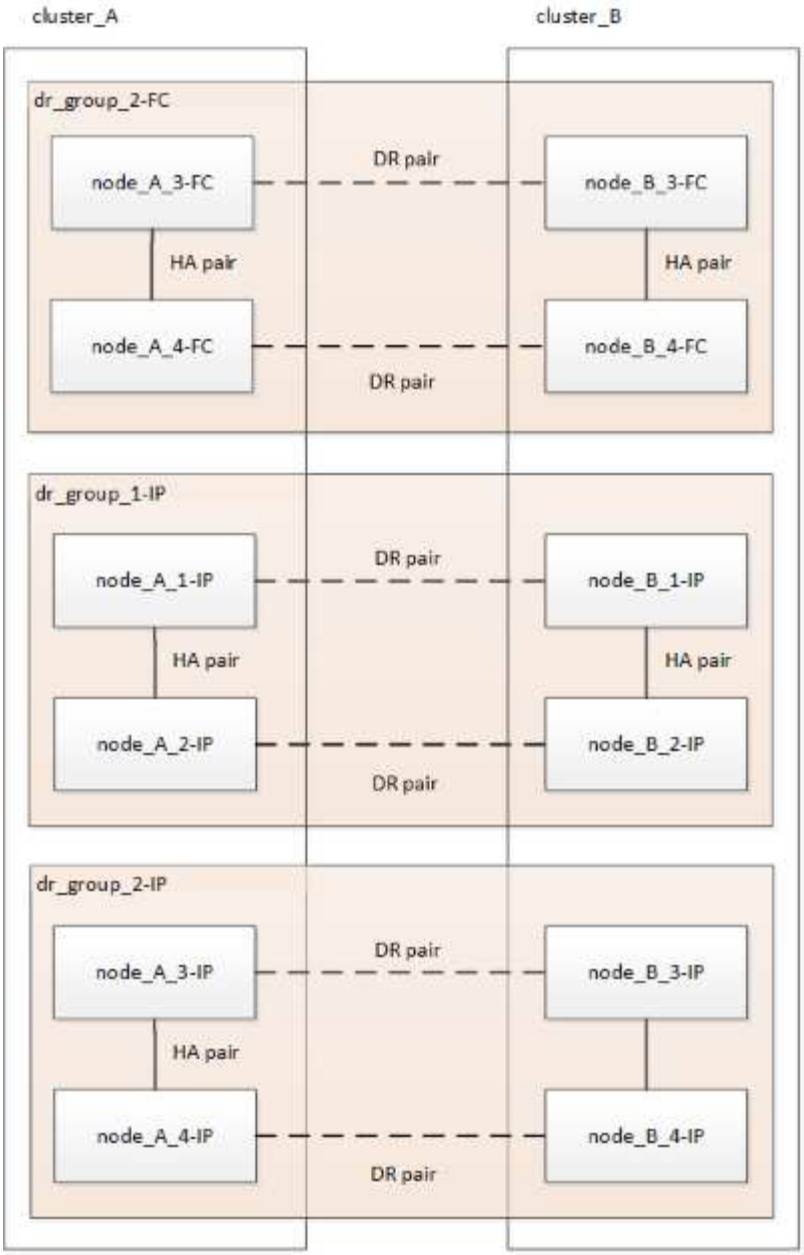


Die Daten werden von DR_Group_1-FC zu DR_Group_1-IP übertragen und anschließend die alten Knoten und deren Speicher aus der Konfiguration entfernt und außer Betrieb genommen.

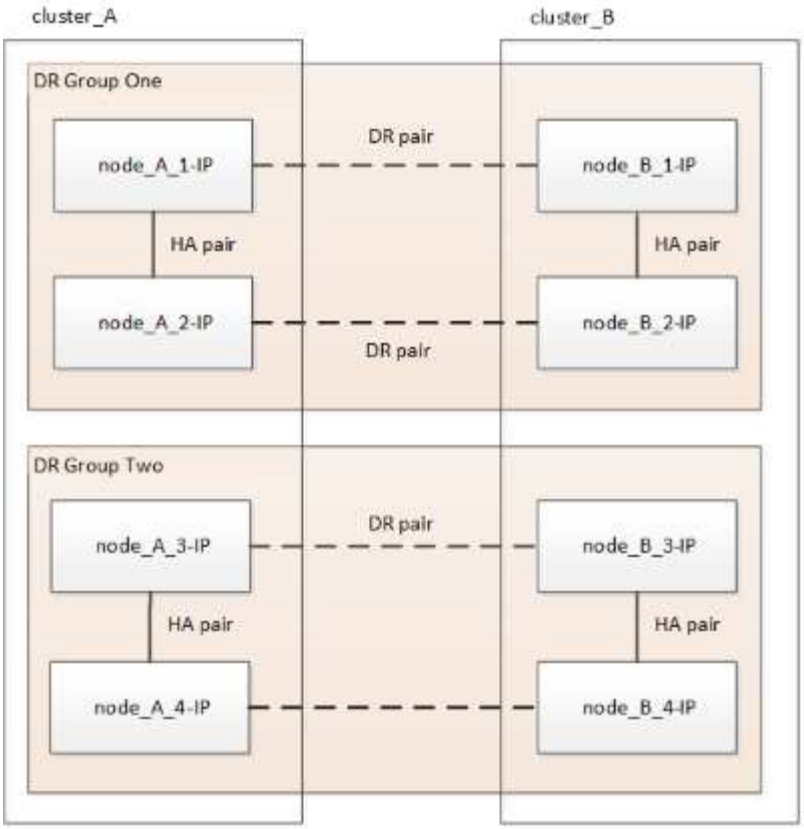
> Wenn Sie von einer FC-Konfiguration mit acht Knoten auf eine IP-Konfiguration mit vier Knoten umstellen möchten, müssen Sie alle Daten in DR_Group_1-FC und DR_Group_2-FC auf die neue IP DR-Gruppe (DR_Group_1-IP) übertragen. Sie können dann beide FC DR-Gruppen außer Betrieb nehmen. Nachdem die FC DR-Gruppen entfernt wurden, endet der Prozess mit einer MetroCluster IP Konfiguration mit vier Nodes.



Fügen Sie der vorhandenen MetroCluster-Konfiguration die verbleibenden MetroCluster IP-Nodes hinzu. Wiederholen Sie den Vorgang, um Daten von den DR_Group_2-FC-Nodes auf die DR_Group_2-IP-Nodes zu übertragen.

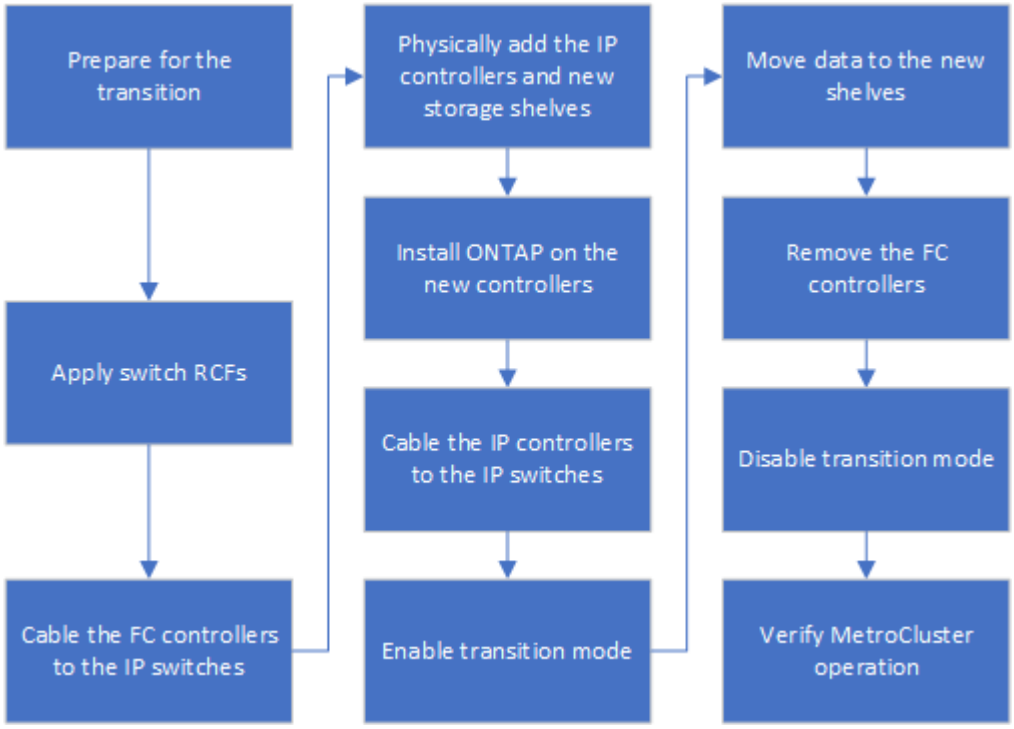


Nach dem Entfernen von DR_Group_2-FC endet der Prozess mit einer MetroCluster IP-Konfiguration mit acht Knoten.



Workflow für den Umstellungsprozess

Sie verwenden den folgenden Workflow, um die MetroCluster Konfiguration zu wechseln.



Überlegungen zu IP-Switches

Sie müssen sicherstellen, dass die IP-Switches unterstützt werden. Wenn das

vorhandene Switch-Modell sowohl von der ursprünglichen MetroCluster FC-Konfiguration als auch von der neuen MetroCluster IP-Konfiguration unterstützt wird, können die vorhandenen Switches wiederverwendet werden.

Unterstützte Switches

Sie müssen von NetApp bereitgestellte Switches verwenden.

- Die Verwendung von MetroCluster-konformen Switches (Switches, die nicht von NetApp validiert und bereitgestellt werden) wird für die Transition nicht unterstützt.
- Die IP-Switches müssen von der MetroCluster FC-Konfiguration und der MetroCluster IP-Konfiguration als Cluster-Switch unterstützt werden.
- Die IP-Switches können in der neuen MetroCluster IP-Konfiguration wiederverwendet werden, wenn MetroCluster FC ein Switch-Cluster ist und die IP-Cluster-Switches von der MetroCluster IP-Konfiguration unterstützt werden.
- Neue IP-Schalter werden in der Regel in folgenden Fällen verwendet:
  - Die MetroCluster FC-Plattform ist ein Cluster ohne Switches, sodass neue Switches erforderlich sind.
  - Die MetroCluster FC ist ein Switch-basiertes Cluster, die bestehenden IP-Switches werden jedoch in der MetroCluster IP-Konfiguration nicht unterstützt.
  - Sie möchten verschiedene Switches für die MetroCluster IP-Konfiguration verwenden.

> Bei Verwendung von Shared Storage MetroCluster Switches können Sie nur zu einer MetroCluster IP-Konfiguration mit vier Nodes wechseln. Der Übergang zu einer MetroCluster IP-Konfiguration mit acht Nodes unter Verwendung von MetroCluster-Switches für gemeinsamen Storage wird nicht unterstützt. Nachdem Sie den Übergang zu einer MetroCluster IP-Konfiguration mit vier Knoten abgeschlossen haben, können Sie "Erweitern Sie auf eine MetroCluster IP-Konfiguration mit acht Nodes".

Informationen zu Plattformmodellen und Switch-Unterstützung finden Sie im "Hardware Universe".

Umschaltung, Reparatur und Wechsel zwischen den Abläufen während des unterbrechungsfreien Übergangs

Je nach Phase des Übergangs verwenden die MetroCluster Switchover-, Healing- und Switchback-Vorgänge entweder den MetroCluster FC- oder MetroCluster IP-Workflow.

Die folgende Tabelle zeigt, welche Workflows in verschiedenen Phasen des Wechsels zum Einsatz kommen. In einigen Phasen werden Umschaltung und zurückwechseln nicht unterstützt.

- Im MetroCluster FC-Workflow werden die Schritte Switchover, Healing und Switchback von einer MetroCluster FC-Konfiguration verwendet.
- Im MetroCluster IP-Workflow werden die Schritte Switchover, Healing und Switchback von einer MetroCluster IP-Konfiguration verwendet.
- Wenn im einheitlichen Workflow sowohl die FC- als auch die IP-Knoten konfiguriert sind, hängen die Schritte davon ab, ob NSO oder USO ausgeführt wird. Die Details sind in der Tabelle aufgeführt.

Informationen zu den MetroCluster FC- und IP-Workflows für Switchover, Healing und Switchback finden Sie unter "MetroCluster Datensicherung und Disaster Recovery verstehen".

Während des Umstiegs ist keine automatische, ungeplante Umschaltung verfügbar.

Phase des Übergangs	Die ausgehandelte Umschaltung nutzt diesen Workflow…	Ungeplante Umschaltung nutzt diesen Workflow…
Bevor die MetroCluster IP-Knoten dem Cluster beigetreten sind	MetroCluster FC	MetroCluster FC
Nachdem die MetroCluster-IP-Nodes dem Cluster beigetreten sind, bevor der `metrocluster configure` Befehl wird ausgeführt	Nicht unterstützt	MetroCluster FC
Nach dem `metrocluster configure` Befehl wurde ausgegeben. Die Volume-Verschiebung kann ausgeführt werden.	Unified: Alle Nodes an Remote-Standorten bleiben aktiviert, und die Reparatur erfolgt automatisch	Vereinheitlicht: • Gespiegelte Aggregate des MetroCluster FC-Node werden gespiegelt, wenn der Storage verfügbar ist. Nach der Umschaltung werden alle anderen Aggregate herabgestuft. • Alle Nodes am Remote-Standort können gestartet werden. • Der `heal aggregate` Und `heal root` Sie müssen Befehle manuell ausführen.
Die MetroCluster FC-Nodes wurden nicht konfiguriert.	Nicht unterstützt	MetroCluster IP
Der `cluster unjoin` Der Befehl wurde auf den MetroCluster FC-Knoten ausgeführt.	MetroCluster IP	MetroCluster IP

Warnmeldungen und Tool-Unterstützung während der Transition

Sie können während der Umstellung Warnmeldungen bemerken. Diese Warnmeldungen können ohne Bedenken ignoriert werden. Außerdem stehen einige Tools während der Transition nicht zur Verfügung.

- ARS können während des Übergangs warnen.

  Diese Warnmeldungen können ignoriert werden und sollten nach Abschluss der Transition verschwinden.

- OnCommand Unified Manager gibt während der Transition möglicherweise eine Warnmeldung aus.

  Diese Warnmeldungen können ignoriert werden und sollten nach Abschluss der Transition verschwinden.

- Config Advisor wird während der Umstellung nicht unterstützt.

- System Manager wird während der Umstellung nicht unterstützt.

Beispiel für die Benennung in diesem Verfahren

Bei diesem Verfahren werden durchgängig Beispielnamen verwendet, um die involvierten DR-Gruppen, Nodes und Switches zu identifizieren.

DR-Gruppen	Cluster_A an Standort_A	Cluster_B an Standort_B
dr_Group_1-FC	• Node_A_1-FC • Node_A_2-FC	• Node_B_1-FC • Node_B_2-FC
dr_Group_2-IP	• Node_A_3-IP • Node_A_4-IP	• Node_B_3-IP • Node_B_4-IP
Schalter	Initial Switches (bei Fabric-Attached-Konfiguration:) • Switch_A_1-FC • Switch_A_2-FC MetroCluster IP-Switches: • Switch_A_1-IP • Switch_A_2-IP	Initial Switches (bei Fabric-Attached-Konfiguration): • Switch_B_1-FC • Switch_B_2-FC MetroCluster IP-Switches: • Switch_B_1-IP • Switch_B_2-IP

Umstellung von MetroCluster FC- auf MetroCluster IP-Konfigurationen

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie müssen den Zustand und die Konnektivität der MetroCluster Konfiguration vor der Durchführung der Transition überprüfen

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:`node run -node node-name sysconfig -a`
   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen: `system health alert show`
   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus: `metrocluster show`
   d. Durchführen einer MetroCluster-Prüfung: `metrocluster check run`
   e. Ergebnisse der MetroCluster-Prüfung anzeigen: `metrocluster check show`
   f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden): `storage switch show`
   g. Nutzen Sie Config Advisor.

      "NetApp Downloads: Config Advisor"

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

2. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet: `cluster show`

```
cluster_A::> cluster show
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1_FC    true    true          false
node_A_2_FC    true    true          false

cluster_A::>
```

3. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind: `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1_FC

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind: `network interface show -vserver cluster`

   Jede Cluster-LIF sollte „true“ für „is Home“ und „up/up“ für „Status Admin/Oper“ anzeigen.

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A-1_FC_clus1
                       up/up      169.254.209.69/16  node_A-1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Vergewissern Sie sich, dass die automatische Umrüstung auf allen Cluster-LIFs aktiviert ist: `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1_FC_clus1
                        true
           node_A_1_FC_clus2
                        true
           node_A_2_FC_clus1
                        true
           node_A_2_FC_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "Entfernen von MetroCluster-Konfigurationen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Erstellen und Anwenden von RCFs auf die neuen IP-Switches

Wenn Sie neue IP-Schalter für die MetroCluster IP-Konfiguration verwenden, müssen Sie die Switches mit einer benutzerdefinierten RCF-Datei konfigurieren.

Diese Aufgabe ist erforderlich, wenn Sie neue Switches verwenden.

Wenn Sie vorhandene Switches verwenden, fahren Sie mit fort "Verschieben der lokalen Cluster-Verbindungen".

1. Installieren und Rack der neuen IP-Switches.
2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

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

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

3. Aktualisieren Sie die Firmware auf dem Switch auf eine unterstützte Version, falls erforderlich.
4. Verwenden Sie das RCF-Generator-Tool, um die RCF-Datei abhängig vom Switch-Anbieter und den Plattformmodellen zu erstellen und dann die Switches mit der Datei zu aktualisieren.

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

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

Verschieben Sie die lokalen Cluster-Verbindungen

Verschieben Sie die Clusterschnittstellen der MetroCluster FC-Konfiguration zu den IP-Switches.

Schritt 1: Verschieben Sie die Clusterverbindungen auf den MetroCluster FC-Knoten

Verschieben Sie die Clusterverbindungen der MetroCluster FC-Knoten zu den IP-Switches. Die Schritte hängen davon ab, ob Sie vorhandene oder neue IP-Switches verwenden.

Über diese Aufgabe

- Sie führen diese Aufgabe auf beiden MetroCluster-Sites aus.

Welche Verbindungen zu verschieben sind

Die folgende Aufgabe geht davon aus, dass ein Controllermodul zwei Ports für die Clusterverbindungen verwendet. Einige Controller-Modulmodelle verwenden vier oder mehr Ports für die Cluster-Verbindung. In diesem Beispiel sind die Ports in zwei Gruppen unterteilt, wobei die Ports zwischen den beiden Gruppen abwechselnd verwendet werden.

In der folgenden Tabelle sind die Beispielports aufgeführt, die in dieser Aufgabe verwendet werden.

Anzahl der Cluster-Verbindungen am Controller-Modul	Ports gruppieren	Gruppen-B-Ports
Zwei	e0a	e0b
Vier	e0a, e0c	e0b, e0d

- Ports gruppieren A verbinden sich mit lokalem Switch_x_1-IP.
- Gruppen-B-Ports verbinden sich mit dem lokalen Switch_x_2-IP.

In der folgenden Tabelle wird gezeigt, mit welchen Switch-Ports die FC-Nodes verbunden werden. Für den Broadcom BES-53248-Switch hängt die Portnutzung vom Modell der MetroCluster-IP-Nodes ab.

Switch-Modell	MetroCluster IP-Node-Modell	Switch-Port(e)	Stellt eine Verbindung her
Cisco 3132Q-V	Alle	5, 6	Lokale Cluster-Schnittstelle am FC-Node
Cisco 9336C-FX2 (12 Ports)	Alle	3,4 oder 11,12 **Hinweis:** Um die Switch-Ports 11 und 12 zu verwenden, müssen Sie zwei Geschwindigkeitsmodi auswählen.	Lokale Cluster-Schnittstelle am FC-Node
Cisco 3232C oder 9336C-FX2 (36 Ports)	Alle	5, 6 oder 13, 14 **Hinweis:** Um die Switch-Ports 13 und 14 zu verwenden, müssen Sie zwei Geschwindigkeitsmodi auswählen.	Lokale Cluster-Schnittstelle am FC-Node
Cisco 9336C-FX2 gemeinsam genutzt (36-Port)	Alle	3,4 oder 11,12 **Hinweis:** Um die Switch-Ports 11 und 12 zu verwenden, müssen Sie zwei Geschwindigkeitsmodi auswählen.	Lokale Cluster-Schnittstelle am FC-Node
Broadcom BES-53248	FAS500f/A250	1 - 6	Lokale Cluster-Schnittstelle am FC-Node
	FAS8200/A300	3, 4, 9, 10, 11 12	Lokale Cluster-Schnittstelle am FC-Node
	FAS8300/A400/FAS8700	1 - 6	Lokale Cluster-Schnittstelle am FC-Node
NVIDIA SN2100	Alle	5,6 oder 11,12 **Hinweis:** Um die Switch-Ports 11 und 12 zu verwenden, müssen Sie zwei Geschwindigkeitsmodi auswählen.	Lokale Cluster-Schnittstelle am FC-Node

Verschieben der lokalen Clusterverbindungen bei Verwendung neuer IP-Switches

Wenn Sie neue IP-Switches verwenden, verschieben Sie die Clusterverbindungen der vorhandenen MetroCluster FC-Knoten physisch auf die neuen Switches.

Schritte

1. Verschieben Sie die Cluster-Verbindungen der MetroCluster-FC-Node-Gruppe A zu den neuen IP-Switches.

   Verwenden Sie die in beschriebenen Ports Welche Verbindungen zu verschieben sind.

   a. Trennen Sie alle Ports der Gruppe A vom Switch, oder trennen Sie die Ports der MetroCluster-FC-Konfiguration als Switch-freien Cluster vom Partner-Node.
   b. Trennen Sie die Ports der Gruppe A von Node_A_1-FC und Node_A_2-FC.
   c. Verbinden Sie die Ports der Gruppe A von Node_A_1-FC mit den Switch-Ports für den FC-Node auf Switch_A_1-IP
   d. Verbinden Sie die Gruppen-A-Ports von Node_A_2-FC mit den Switch-Ports für den FC-Node auf Switch_A_1-IP

2. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

   ```
   network port show -ipspace Cluster
   ```

   ```
   cluster_A::*> network port show -ipspace Cluster

   Node: node_A_1-FC

                                                       Speed(Mbps) Health
   Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
   --------- ------------ ---------------- ---- ---- ----------- --------
   e0a       Cluster      Cluster          up   9000  auto/10000 healthy
   e0b       Cluster      Cluster          up   9000  auto/10000 healthy

   Node: node_A_2-FC

                                                       Speed(Mbps) Health
   Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
   --------- ------------ ---------------- ---- ---- ----------- --------
   e0a       Cluster      Cluster          up   9000  auto/10000 healthy
   e0b       Cluster      Cluster          up   9000  auto/10000 healthy

   4 entries were displayed.

   cluster_A::*>
   ```

3. Stellen Sie sicher, dass die Inter-Switch Links (ISLs) zwischen Standorten verfügbar sind und die Port-Kanäle betriebsbereit sind:

```
show interface brief
```

Im folgenden Beispiel werden ISL-Ports „eth1/15“ zu „eth1/20“ als „Po10“ für die Remote-Site-Verbindung konfiguriert und „eth1/7“ bis „eth1/8“ als „PO1“ für den lokalen Cluster ISL konfiguriert. Der Zustand von „eth1/15“ bis „eth1/20“, „eth1/7“ bis „eth1/8“, „Po10“ und „PO1“ sollte „up“ sein.

```
IP_switch_A_1# show interface brief

--------------------------------------------------------------
Port   VRF          Status   IP Address        Speed      MTU
--------------------------------------------------------------
mgmt0  --            up        100.10.200.20    1000      1500
-------------------------------------------------------------------------
--------
Ethernet     VLAN   Type Mode    Status     Reason              Speed
Port
Interface                                    Ch #
-------------------------------------------------------------------------
--------

...

Eth1/7        1     eth  trunk    up        none                100G(D)
1
Eth1/8        1     eth  trunk    up        none                100G(D)
1

...

Eth1/15       1     eth  trunk    up        none                100G(D)
10
Eth1/16       1     eth  trunk    up        none                100G(D)
10
Eth1/17       1     eth  trunk    up        none                100G(D)
10
Eth1/18       1     eth  trunk    up        none                100G(D)
10
Eth1/19       1     eth  trunk    up        none                100G(D)
10
Eth1/20       1     eth  trunk    up        none                100G(D)
10

-------------------------------------------------------------------------
--------
Port-channel VLAN  Type Mode   Status   Reason         Speed    Protocol
Interface
-------------------------------------------------------------------------
```

```
--------
Po1          1     eth  trunk   up      none            a-100G(D) lacp
Po10         1     eth  trunk   up      none            a-100G(D) lacp
Po11         1     eth  trunk   down    No operational  auto(D)   lacp
                                         members
IP_switch_A_1#
```

4. Vergewissern Sie sich, dass in der Spalte „`is Home`“ alle Schnittstellen wahr angezeigt werden:

   `network interface show -vserver cluster`

   Dies kann einige Minuten dauern.

```
cluster_A::*> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1-FC_clus2
                       up/up      169.254.49.125/16  node_A_1-FC   e0b
true
            node_A_2-FC_clus1
                       up/up      169.254.47.194/16  node_A_2-FC   e0a
true
            node_A_2-FC_clus2
                       up/up      169.254.19.183/16  node_A_2-FC   e0b
true

4 entries were displayed.

cluster_A::*>
```

5. Führen Sie die oben genannten Schritte auf beiden Knoten (Node_A_1-FC und Node_A_2-FC) durch, um die Gruppen-B-Ports der Clusterschnittstellen zu verschieben.
6. Wiederholen Sie die oben genannten Schritte im Partner-Cluster „`Cluster_B`“.

Verschieben Sie die lokalen Clusterverbindungen, wenn Sie vorhandene IP-Switches wiederverwenden

Wenn Sie vorhandene IP-Switches wiederverwenden, aktualisieren Sie die Firmware, konfigurieren die Switches mit den richtigen Referenzkonfigurationsdateien (RCFs) neu und verschieben die Verbindungen Switch für Switch auf die richtigen Ports.

Über diese Aufgabe

Diese Aufgabe ist nur erforderlich, wenn die FC-Knoten mit vorhandenen IP-Switches verbunden sind und Sie die Switches erneut verwenden.

Schritte

1. Trennen Sie die lokalen Cluster-Verbindungen, die sich mit Switch_A_1_IP verbinden

   a. Trennen Sie die Ports der Gruppe A vom vorhandenen IP-Switch.

   b. Trennen Sie die ISL-Ports auf Switch_A_1_IP.

      Sie finden die Installations- und Setup-Anleitung für die Plattform, um die Verwendung des Cluster-Ports anzuzeigen.

      "AFF A320-Systeme: Installation und Einrichtung"

      "Installations- und Setup-Anleitung für AFF A220/FAS2700 Systeme"

      "Installations- und Setup-Anleitung für AFF A800 Systeme"

      "Installations- und Setup-Anleitung für AFF A300 Systeme"

   "FAS8200 Systems Installation and Setup instructions"

2. Konfigurieren Sie Switch_A_1_IP mit RCF-Dateien neu, die für die Kombination und den Übergang Ihrer Plattform generiert wurden.

   Befolgen Sie die Schritte im Verfahren für Ihren Switch-Anbieter von *MetroCluster IP Installation and Configuration*:

   "Installation und Konfiguration von MetroCluster IP"

   a. Laden Sie bei Bedarf die neue Switch-Firmware herunter und installieren Sie sie.

      Sie sollten die neueste Firmware verwenden, die die MetroCluster IP Nodes unterstützen.

      - "Laden Sie die Broadcom-Switch-EFOS-Software herunter, und installieren Sie sie"
      - "Laden Sie die Cisco Switch NX-OS-Software herunter, und installieren Sie sie"
      - "Laden Sie die NVIDIA Cumulus-Software herunter und installieren Sie sie"

   b. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

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

   c. Laden Sie die IP RCF-Datei je nach Switch-Anbieter herunter und installieren Sie sie.

      - "Herunterladen und Installieren der Broadcom IP RCF-Dateien"

- "Herunterladen und Installieren der Cisco IP RCF-Dateien"
- "Laden Sie die NVIDIA RCF-Dateien herunter, und installieren Sie sie"

3. Schließen Sie die Ports der Gruppe A wieder an Switch_A_1_IP an.

   Verwenden Sie die in beschriebenen Ports Welche Verbindungen zu verschieben sind.

4. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

   ```
   network port show -ipspace cluster
   ```

   ```
   Cluster-A::*> network port show -ipspace cluster

   Node: node_A_1_FC

                                                        Speed(Mbps) Health
   Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
   --------- ------------ ---------------- ---- ---- ----------- --------
   e0a       Cluster      Cluster          up   9000  auto/10000 healthy
   e0b       Cluster      Cluster          up   9000  auto/10000 healthy

   Node: node_A_2_FC

                                                        Speed(Mbps) Health
   Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
   --------- ------------ ---------------- ---- ---- ----------- --------
   e0a       Cluster      Cluster          up   9000  auto/10000 healthy
   e0b       Cluster      Cluster          up   9000  auto/10000 healthy

   4 entries were displayed.

   Cluster-A::*>
   ```

5. Vergewissern Sie sich, dass sich alle Schnittstellen auf ihrem Home-Port befinden:

   ```
   network interface show -vserver Cluster
   ```

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

6. Wiederholen Sie alle vorherigen Schritte auf Switch_A_2_IP.
7. Schließen Sie die lokalen Cluster-ISL-Ports wieder an.
8. Wiederholen Sie die oben genannten Schritte an Standort_B für Schalter B_1_IP und Schalter B_2_IP.
9. Verbinden Sie die Remote-ISLs zwischen den Standorten.

Schritt 2: Überprüfen, ob die Clusterverbindungen verschoben wurden und der Cluster fehlerfrei ist

Um sicherzustellen, dass die Konnektivität ordnungsgemäß ist und die Konfiguration für den Übergangsprozess bereit ist, überprüfen Sie, ob die Clusterverbindungen richtig verschoben wurden, die Cluster-Switches erkannt werden und der Cluster fehlerfrei ist.

Schritte

1. Vergewissern Sie sich, dass alle Cluster-Ports betriebsbereit sind:

   ```
   network port show -ipspace Cluster
   ```

```
Cluster-A::*> network port show -ipspace Cluster

Node: Node-A-1-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: Node-A-2-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

2. Vergewissern Sie sich, dass sich alle Schnittstellen auf ihrem Home-Port befinden:

   `network interface show -vserver Cluster`

   Dies kann einige Minuten dauern.

   Das folgende Beispiel zeigt, dass alle Schnittstellen in der Spalte „`is Home`“ den Status „true“ aufweisen.

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            Node-A-1_FC_clus1
                       up/up      169.254.209.69/16  Node-A-1_FC   e0a
true
            Node-A-1-FC_clus2
                       up/up      169.254.49.125/16  Node-A-1-FC   e0b
true
            Node-A-2-FC_clus1
                       up/up      169.254.47.194/16  Node-A-2-FC   e0a
true
            Node-A-2-FC_clus2
                       up/up      169.254.19.183/16  Node-A-2-FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

3. Vergewissern Sie sich, dass die beiden lokalen IP-Switches von den Knoten erkannt werden:

   `network device-discovery show -protocol cdp`

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
Node-A-1-FC
           /cdp
            e0a    Switch-A-3-IP             1/5/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/5/1             N3K-
C3232C
Node-A-2-FC
           /cdp
            e0a    Switch-A-3-IP             1/6/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/6/1             N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. Überprüfen Sie am IP-Switch, ob die MetroCluster-IP-Knoten von beiden lokalen IP-Switches erkannt wurden:

   `show cdp neighbors`

   Sie müssen diesen Schritt bei jedem Schalter ausführen.

   In diesem Beispiel wird gezeigt, wie Sie überprüfen, ob die Knoten auf Switch-A-3-IP erkannt werden.

```
(Switch-A-3-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0a
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0a
Switch-A-4-IP(FDO220329A4)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-4-IP(FDO220329A4)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-3-IP(FDO220329B3)
                    Eth1/20        173    R S I s   N3K-C3232C
Eth1/20
Switch-B-3-IP(FDO220329B3)
                    Eth1/21        173    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-3-IP)#
```

In diesem Beispiel wird gezeigt, wie Sie überprüfen, ob die Knoten bei Switch-A-4-IP erkannt werden.

```
(Switch-A-4-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0b
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0b
Switch-A-3-IP(FDO220329A3)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-3-IP(FDO220329A3)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-4-IP(FDO220329B4)
                    Eth1/20        169    R S I s   N3K-C3232C
Eth1/20
Switch-B-4-IP(FDO220329B4)
                    Eth1/21        169    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP)#
```

Vorbereiten der MetroCluster IP-Controller

Sie müssen die vier neuen MetroCluster IP-Knoten vorbereiten und die korrekte ONTAP-Version installieren.

Diese Aufgabe muss auf jedem der neuen Knoten ausgeführt werden:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

Löschen Sie in diesen Schritten die Konfiguration auf den Knoten und löschen Sie den Mailbox-Bereich auf neuen Laufwerken.

1. Rack für die neuen Controller für die MetroCluster IP-Konfiguration

   Die MetroCluster-FC-Nodes (Node_A_x-FC und Node_B_x-FC) bleiben derzeit verkabelt.

2. Verkabeln Sie die MetroCluster IP-Knoten wie im gezeigt mit den IP-Switches "Verkabeln der IP-Switches".

3. Konfigurieren Sie die MetroCluster IP-Knoten unter Verwendung der folgenden Abschnitte:
   a. "Sammeln Sie die erforderlichen Informationen"
   b. "Systemstandardwerte auf einem Controller-Modul wiederherstellen"
   c. "Überprüfen Sie den Status der HA-Konfiguration der Komponenten"
   d. "Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.4 und höher)"
4. Geben Sie im Wartungsmodus den Befehl stop ein, um den Wartungsmodus zu beenden, und geben Sie dann den Boot_ontap-Befehl aus, um das System zu booten und zum Cluster-Setup zu gelangen.

   Schließen Sie derzeit den Cluster-Assistenten oder den Node-Assistenten nicht ab.

5. Wiederholen Sie diese Schritte auf den anderen MetroCluster IP-Knoten.

MetroCluster für Transition konfigurieren

Um die Konfiguration für den Umstieg vorzubereiten, fügen Sie die neuen Nodes zur bestehenden MetroCluster Konfiguration hinzu und verschieben Sie dann Daten zu den neuen Nodes.

Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung

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

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung durchgeführt wird:

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

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

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

2. Wiederholen Sie den Befehl im Partner-Cluster.

Aktivieren des Übergangsmodus und Deaktivieren von Cluster HA

Sie müssen den MetroCluster Transition-Modus aktivieren, damit die alten und neuen Nodes in der MetroCluster Konfiguration gemeinsam arbeiten und die Cluster HA deaktivieren können.

1. Übergang ermöglichen:

   a. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

b. Übergangsmodus aktivieren:

```
metrocluster transition enable -transition-mode non-disruptive
```

> Führen Sie diesen Befehl nur auf einem Cluster aus.

```
cluster_A::*> metrocluster transition enable -transition-mode non-
disruptive

Warning: This command enables the start of a "non-disruptive"
MetroCluster
         FC-to-IP transition. It allows the addition of hardware for
another DR
         group that uses IP fabrics, and the removal of a DR group that
uses FC
         fabrics. Clients will continue to access their data during a
         non-disruptive transition.

         Automatic unplanned switchover will also be disabled by this
command.
Do you want to continue? {y|n}: y

cluster_A::*>
```

a. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Vergewissern Sie sich, dass die Transition auf beiden Clustern aktiviert ist.

```
cluster_A::> metrocluster transition show-mode
Transition Mode

non-disruptive

cluster_A::*>


cluster_B::*> metrocluster transition show-mode
Transition Mode

non-disruptive

Cluster_B::>
```

3. Deaktivieren Sie Cluster HA.

   Sie müssen diesen Befehl auf beiden Clustern ausführen.

```
cluster_A::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_A::*>


cluster_B::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_B::*>
```

4. Vergewissern Sie sich, dass Cluster HA deaktiviert ist.

   Sie müssen diesen Befehl auf beiden Clustern ausführen.

```
cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>
```

Verbinden der MetroCluster IP-Nodes mit den Clustern

Sie müssen die vier neuen MetroCluster IP-Nodes der bestehenden MetroCluster-Konfiguration hinzufügen.

Über diese Aufgabe

Sie müssen diese Aufgabe für beide Cluster ausführen.

Schritte

1. Fügen Sie die MetroCluster IP-Knoten zur bestehenden MetroCluster-Konfiguration hinzu.
   a. Schließen Sie den ersten MetroCluster-IP-Knoten (Node_A_3-IP) an die vorhandene MetroCluster-FC-Konfiguration an.

```
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: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:

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


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Fügen Sie den zweiten MetroCluster IP-Knoten (Node_A_4-IP) der bestehenden MetroCluster FC-

Konfiguration hinzu.

2. Wiederholen Sie diese Schritte, um Node_B_3-IP und Node_B_4-IP zu Cluster_B. zu verbinden

Konfigurieren von Intercluster-LIFs, Erstellen der MetroCluster-Schnittstellen und Spiegeln von Root-Aggregaten

Sie müssen Cluster-Peering-LIFs erstellen, die MetroCluster-Schnittstellen auf den neuen MetroCluster IP-Nodes erstellen.

Über diese Aufgabe

Der in den Beispielen verwendete Home-Port ist plattformspezifisch. Sie sollten den entsprechenden Home Port für die MetroCluster IP-Node-Plattform verwenden.

Schritte

1. Auf den neuen MetroCluster IP-Knoten "Konfigurieren Sie die Intercluster LIFs".
2. Vergewissern Sie sich an jedem Standort, dass Cluster-Peering konfiguriert ist:

   ```
   cluster peer show
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A 1-80-000011 Available ok
   ```

3. Konfigurieren Sie die DR-Gruppe für die MetroCluster IP-Knoten:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   ```
   cluster_A::> metrocluster configuration-settings dr-group create
   -partner-cluster
   cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
   [Job 259] Job succeeded: DR Group Create is successful.
   cluster_A::>
   ```

4. Vergewissern Sie sich, dass die DR-Gruppe erstellt wird.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
2           cluster_A
                                       node_A_3-IP        node_B_3-IP
                                       node_A_4-IP        node_B_4-IP
            cluster_B
                                       node_B_3-IP        node_A_3-IP
                                       node_B_4-IP        node_A_4-IP

4 entries were displayed.

cluster_A::>
```

   Sie werden feststellen, dass die DR-Gruppe für die alten MetroCluster FC-Knoten (DR-Gruppe 1) nicht aufgeführt ist, wenn Sie die ausführen `metrocluster configuration-settings dr-group show` Befehl.

   Verwenden Sie können `metrocluster node show` Führen Sie einen Befehl auf beiden Seiten aus, um alle Nodes aufzulisten.

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
      cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
2     cluster_A
              node_A_3-IP      ready to configure
                                                 -         -
              node_A_4-IP      ready to configure
                                                 -         -

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
      cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
2     cluster_B
              node_B_3-IP      ready to configure
                                                 -         -
              node_B_4-IP      ready to configure
                                                 -         -
```

5. Konfigurieren Sie die MetroCluster IP-Schnittstellen für die neu verbundenen MetroCluster IP-Knoten:

> Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

```
metrocluster configuration-settings interface create -cluster-name
```

Siehe "Konfigurieren und Anschließen der MetroCluster IP-Schnittstellen" Überlegungen bei der Konfiguration der IP-Schnittstellen.

Sie können die MetroCluster-IP-Schnittstellen von beiden Clustern konfigurieren.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Überprüfen Sie, ob die MetroCluster-IP-Schnittstellen erstellt wurden:

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

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
2     cluster_A
             node_A_3-IP
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-IP
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Verbinden Sie die MetroCluster IP-Schnittstellen:

```
metrocluster configuration-settings connection connect
```

Dieser Befehl kann einige Minuten dauern.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Überprüfen Sie, ob die Verbindungen ordnungsgemäß aufgebaut sind:

   `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_3-IP**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
```

```
                     172.17.26.11    172.17.26.12    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.10    HA Partner
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.13    DR Partner
completed
                Home Port: e1b
                     172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                   Source          Destination
Group Cluster Node   Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_4-IP
                Home Port: e1a
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_3-IP
                Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
```

```
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.10    DR Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. Überprüfen der automatischen Zuweisung und Partitionierung der Festplatte:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.
cluster_A::>
```

Bei Systemen, die für Advanced Drive Partitioning (ADP) konfiguriert sind, ist der Containertyp „shared“ und nicht „Remote“, wie in der Beispielausgabe dargestellt.

10. Root-Aggregate spiegeln:

```
storage aggregate mirror -aggregate aggr0_node_A_3_IP
```

Diesen Schritt müssen Sie bei jedem MetroCluster IP Node abschließen.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3_IP

Info: Disks would be added to aggregate "aggr0_node_A_3_IP"on node
"node_A_3-IP"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available for volume use would be 467.6GB.

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

cluster_A::>
```

11. Überprüfen Sie, ob die Root-Aggregate gespiegelt wurden:

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1_FC
           349.0GB   16.84GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2_FC
           349.0GB   16.84GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3_IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_4_IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-FC
raid_dp,

mirrored,
```

Abschließen des Hinzufügung der MetroCluster IP-Nodes

Sie müssen die neue DR-Gruppe in die MetroCluster Konfiguration einbinden und gespiegelte Datenaggregate auf den neuen Nodes erstellen.

Schritte

1. Konfigurieren Sie den MetroCluster, je nachdem, ob auf beiden Clustern ein einzelnes oder mehrere Datenaggregate vorhanden sind:

Wenn Ihre MetroCluster Konfiguration…	Dann tun Sie das…

Mehrere Datenaggregate auf beiden Clustern	Konfigurieren Sie an der Eingabeaufforderung eines beliebigen Nodes MetroCluster: `metrocluster configure <node-name>` Sie müssen ausführen `metrocluster configure` Und **nicht** `metrocluster configure -refresh true`

Ein einzelnes gespiegeltes Datenaggregat auf beiden Clustern	a. Ändern Sie von der Eingabeaufforderung eines beliebigen Node auf die erweiterte Berechtigungsebene:
	
	`set -privilege advanced`
	
	Sie müssen mit antworten `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus (*>) angezeigt.
	
	b. Konfigurieren Sie die MetroCluster mit dem `-allow-with-one-aggregate true` Parameter:
	
	`metrocluster configure -allow-with -one-aggregate true -node-name <node-name>`
	
	c. Zurück zur Administratorberechtigungsebene:
	
	`set -privilege admin`

Als Best Practice empfiehlt sich die Nutzung mehrerer gespiegelter Datenaggregate. Wenn nur ein gespiegeltes Aggregat verfügbar ist, ist weniger Schutz da sich die Metadaten-Volumes auf demselben Aggregat anstatt auf separaten Aggregaten befinden.

2. Starten Sie jeden der neuen Nodes neu:

```
node reboot -node <node_name> -inhibit-takeover true
```

Die Nodes müssen nicht in einer bestimmten Reihenfolge neu gebootet werden. Sie sollten jedoch warten, bis ein Node vollständig gebootet wurde und alle Verbindungen hergestellt sind, bevor Sie den nächsten Node neu booten.

3. Vergewissern Sie sich, dass die Nodes zu ihrer DR-Gruppe hinzugefügt werden:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node-A-1-FC        configured     enabled   normal
              node-A-2-FC        configured     enabled   normal
      Cluster-B
              node-B-1-FC        configured     enabled   normal
              node-B-2-FC        configured     enabled   normal
2     cluster_A
              node-A-3-IP        configured     enabled   normal
              node-A-4-IP        configured     enabled   normal
      Cluster-B
              node-B-3-IP        configured     enabled   normal
              node-B-4-IP        configured     enabled   normal
8 entries were displayed.

cluster_A::>
```

4. Erstellen von gespiegelten Datenaggregaten auf jedem der neuen MetroCluster Nodes:

   `storage aggregate create -aggregate aggregate-name -node node-name -diskcount no-of-disks -mirror true`

   > Sie müssen mindestens ein gespiegeltes Datenaggregat pro Standort erstellen. Es wird empfohlen, zwei gespiegelte Datenaggregate pro Standort auf MetroCluster IP-Knoten zu haben, um die MDV-Volumes zu hosten. Allerdings wird ein einzelnes Aggregat pro Standort unterstützt (jedoch nicht empfohlen). Es ist akzeptabel, dass ein Standort der MetroCluster ein einziges gespiegeltes Datenaggregat hat und der andere Standort mehr als ein gespiegeltes Datenaggregat hat.

   Das folgende Beispiel zeigt die Erstellung eines Aggregats auf Node_A_3-IP.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_3-
IP -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_3-IP" would be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
```

```
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

5. Überprüfen Sie, ob alle Nodes im Cluster ordnungsgemäß sind:

```
cluster show
```

Die Ausgabe sollte angezeigt werden `true` Für das `health` Feld für alle Knoten.

6. Mit dem folgenden Befehl auf beiden Clustern bestätigen Sie, dass ein Takeover möglich ist und die Nodes verbunden sind:

   `storage failover show`

   ```
   cluster_A::> storage failover show
                                          Takeover
   Node           Partner                 Possible    State Description
   -------------- --------------------- ---------   ------------------
   Node_FC_1      Node_FC_2               true      Connected to Node_FC_2
   Node_FC_2      Node_FC_1               true      Connected to Node_FC_1
   Node_IP_1      Node_IP_2               true      Connected to Node_IP_2
   Node_IP_2      Node_IP_1               true      Connected to Node_IP_1
   ```

7. Vergewissern Sie sich, dass alle Festplatten vorhanden sind, die mit den neu verbundenen MetroCluster-IP-Nodes verbunden sind:

   `disk show`

8. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration, indem Sie die folgenden Befehle ausführen:

   a. `metrocluster check run`

   b. `metrocluster check show`

   c. `metrocluster interconnect mirror show`

   d. `metrocluster interconnect adapter show`

9. Verschieben Sie die MDV_CRS-Volumes von den alten Knoten auf die neuen Knoten in der erweiterten Berechtigung.

   a. Anzeigen der Volumes zur Identifizierung der MDV-Volumes:

   > Wenn Sie ein einzelnes gespiegeltes Datenaggregat pro Standort haben, dann verschieben Sie beide MDV-Volumen zu diesem einzigen Aggregat. Wenn Sie zwei oder mehr gespiegelte Datenaggregate haben, dann verschieben Sie jedes MDV-Volume zu einem anderen Aggregat.

   Das folgende Beispiel zeigt die MDV-Volumes in der Ausgabe der Volume show:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Legen Sie die erweiterte Berechtigungsebene fest:

```
set -privilege advanced
```

c. Verschieben Sie die MDV-Volumes nacheinander:

```
volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name
```

Das folgende Beispiel zeigt den Befehl und die Ausgabe für das Verschieben von MDV_CRS_d6b313ff5611e9837100a098544e51_A, um Daten_a3 auf Node_A_3 zu aggregieren.

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Überprüfen Sie mit dem Befehl Volume show, ob das MDV-Volume erfolgreich verschoben wurde:

```
volume show mdv-name
```

Die folgende Ausgabe zeigt, dass das MDV-Volume erfolgreich verschoben wurde.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

a. Zurück zum Admin-Modus:

```
set -privilege admin
```

Die Daten werden auf die neuen Festplatten-Shelfs verschoben

Während der Umstellung werden die Daten von den Laufwerk-Shelfs in der MetroCluster FC-Konfiguration auf die neue MetroCluster IP-Konfiguration verschoben.

Bevor Sie beginnen

Sie sollten neue SAN-LIFs auf den Ziel- oder IP-Nodes erstellen und Hosts verbinden, bevor Sie Volumes zu den neuen Aggregaten verschieben.

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.

a. Geben Sie den folgenden Befehl ein: `system node autosupport invoke -node * -type all -message MAINT=end`

b. Wiederholen Sie den Befehl im Partner-Cluster.

2. Verschieben Sie die Daten-Volumes zu Aggregaten auf den neuen Controllern, jeweils ein Volume.

   Verwenden Sie das Verfahren unter "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes".

3. Erstellen Sie SAN-LIFs auf den kürzlich hinzugefügten Nodes.

   Gehen Sie wie folgt vor "LUN-Pfade für die neuen Nodes werden aktualisiert".

4. Prüfen Sie, ob auf den FC-Nodes gesperrte Lizenzen für Nodes vorhanden sind. Falls vorhanden, müssen sie den neu hinzugefügten Nodes hinzugefügt werden.

   Gehen Sie wie folgt vor "Hinzufügen von Node-gesperrten Lizenzen".

5. Migrieren der Daten-LIFs

   Verwenden Sie das Verfahren unter "Die verschieben von LIFs für nicht-SAN-Daten und LIFs für das Cluster-Management auf die neuen Nodes" Führen Sie aber die letzten beiden Schritte durch, um LIFs für das Cluster-Management zu migrieren.

> - Sie können keine LIF migrieren, die für Copy-Offload-Vorgänge verwendet wird – mit VMware vStorage APIs for Array Integration (VAAI).
> - Nach dem Abschluss der Umstellung Ihrer MetroCluster Nodes von FC zu IP müssen Sie eventuell Ihre iSCSI Host-Verbindungen zu den neuen Nodes von finden Sie unter "Verschieben von Linux iSCSI-Hosts von MetroCluster-FC- zu MetroCluster-IP-Knoten."

Entfernen der MetroCluster FC-Controller

Sie müssen eine Bereinigung durchführen und die alten Controller-Module aus der MetroCluster-Konfiguration entfernen.

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit die Wartung läuft.

   a. Geben Sie den folgenden Befehl ein: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      Maintenance-Fenster in Stunden gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Wiederholen Sie den Befehl im Partner-Cluster.

2. Legen Sie die Aggregate fest, die auf der MetroCluster FC-Konfiguration gehostet werden sollen, die gelöscht werden müssen.

   In diesem Beispiel werden die folgenden Datenaggregate vom MetroCluster FC Cluster_B gehostet und müssen gelöscht werden: aggr_Data_a1 und aggr_Data_a2.

Sie müssen die Schritte durchführen, um die Datenaggregate auf beiden Clustern zu identifizieren, offline und zu löschen. Das Beispiel gilt nur für ein Cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.83GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.02TB    0% online       0 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
```

```
            1.02TB    1.02TB    0% online       0 node_A_2-FC
raid_dp,

mirrored,

normal
aggr_data_a3
            1.37TB    1.35TB    1% online       3 node_A_3-IP
raid_dp,

mirrored,

normal
aggr_data_a4
            1.25TB    1.24TB    1% online       2 node_A_4-IP
raid_dp,

mirrored,

normal
8 entries were displayed.

cluster_B::>
```

3. Überprüfen Sie, ob die Datenaggregate auf den FC-Knoten über MDV_aud-Volumes verfügen und löschen Sie sie vor dem Löschen der Aggregate.

   Sie müssen die MDV_aud-Volumes löschen, da sie nicht verschoben werden können.

4. Nehmen Sie alle Datenaggregate offline und löschen Sie sie anschließend:

   a. Versetzen Sie das Aggregat in den Offline-Modus: `storage aggregate offline -aggregate aggregate-name`

      Das folgende Beispiel zeigt, dass das Aggregat aggr_Data_a1 offline geschaltet wird:

      ```
      cluster_B::> storage aggregate offline -aggregate aggr_data_a1

      Aggregate offline successful on aggregate: aggr_data_a1
      ```

   b. Löschen Sie das Aggregat: `storage aggregate delete -aggregate aggregate-name`

      Sie können den Plex zerstören, wenn Sie dazu aufgefordert werden.

      Das folgende Beispiel zeigt, dass das Aggregat aggr_Data_a1 gelöscht wird.

```
cluster_B::> storage aggregate delete -aggregate aggr_data_a1
Warning: Are you sure you want to destroy aggregate "aggr_data_a1"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

5. Identifizieren Sie die MetroCluster FC DR-Gruppe, die entfernt werden muss.

   Im folgenden Beispiel befinden sich die MetroCluster FC Nodes in der DR-Gruppe '1', und dies ist die DR-Gruppe, die entfernt werden muss.

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        configured     enabled   normal
              node_A_2-FC        configured     enabled   normal
      cluster_B
              node_B_1-FC        configured     enabled   normal
              node_B_2-FC        configured     enabled   normal
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_3-IP        configured     enabled   normal
8 entries were displayed.

cluster_B::>
```

6. Verschieben Sie die Cluster-Management-LIF von einem MetroCluster FC Node zu einem MetroCluster IP Node: `cluster_B::> network interface migrate -vserver svm-name -lif cluster_mgmt -destination-node node-in-metrocluster-ip-dr-group -destination-port available-port`
7. Ändern Sie den Home Node und den Home Port der Cluster-Management-LIF: `cluster_B::> network interface modify -vserver svm-name -lif cluster_mgmt -service-policy default-management -home-node node-in-metrocluster-ip-dr-group -home-port lif-port`
8. Verschieben Sie Epsilon von einem MetroCluster-FC-Node auf einen MetroCluster-IP-Node:
   a. Identifizieren Sie, welcher Knoten derzeit über Epsilon verfügt: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      true
node_A_2-FC      false
node_A_1-IP      false
node_A_2-IP      false
4 entries were displayed.
```

b. Setzen Sie Epsilon auf „false“ auf den MetroCluster-FC-Node (Node_A_1-FC): `cluster modify -node fc-node -epsilon false`

c. Setzen Sie das Epsilon auf „true“ auf dem MetroCluster-IP-Knoten (Node_A_1-IP): `cluster modify -node ip-node -epsilon true`

d. Vergewissern Sie sich, dass sich das Epsilon auf den richtigen Knoten bewegt hat: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      false
node_A_2-FC      false
node_A_1-IP      true
node_A_2-IP      false
4 entries were displayed.
```

9. Ändern Sie die IP-Adresse für den Cluster-Peer der migrierten IP-Nodes für jedes Cluster:

a. Identifizieren Sie den Cluster_A-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

i. Peer-IP-Adresse „Cluster_A“ ändern:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

b. Identifizieren Sie den Cluster_B-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

i. Peer-IP-Adresse für Cluster_B ändern:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

c. Überprüfen Sie, ob die Cluster-Peer-IP-Adresse für jedes Cluster aktualisiert wurde:

i. Überprüfen Sie mithilfe der, ob die IP-Adresse für jedes Cluster aktualisiert wurde `cluster peer show -instance` Befehl.

Der `Remote Intercluster Addresses` In den folgenden Beispielen wird die aktualisierte IP-Adresse angezeigt.

Beispiel für Cluster_A:

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

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                      Remote Cluster Name: cluster_B
                      Active IP Addresses: 172.21.178.212,
172.21.178.204
                    Cluster Serial Number: 1-80-000011
                     Remote Cluster Nodes: node_B_3-IP,
                                           node_B_4-IP
                    Remote Cluster Health: true
                  Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+
Beispiel für „Cluster_B“

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

                      Peer Cluster Name: cluster_A
           Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                        Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. Entfernen Sie auf jedem Cluster die DR-Gruppe, die die alten Nodes enthält, aus der MetroCluster-FC-Konfiguration.

    Sie müssen diesen Schritt nacheinander für beide Cluster ausführen.

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B" to remove the remote nodes in the
DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed ifthe preparation steps are not completed on
the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_B::>
```

11. Vergewissern Sie sich, dass die Nodes bereit sind, aus den Clustern zu entfernen.

    Sie müssen diesen Schritt auf beiden Clustern durchführen.

    > An diesem Punkt, der `metrocluster node show` Mit dem Befehl werden nur die lokalen MetroCluster FC-Nodes angezeigt und nicht mehr die Nodes angezeigt, die Teil des Partner-Clusters sind.

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        ready to configure
                                                -         -
              node_A_2-FC        ready to configure
                                                -         -
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_4-IP        configured     enabled   normal
6 entries were displayed.

cluster_B::>
```

12. Deaktivieren Sie das Storage-Failover für die MetroCluster-FC-Nodes.

    Sie müssen diesen Schritt für jeden Knoten durchführen.

```
cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>
```

13. Heben Sie die Verbindung der MetroCluster FC-Nodes vom Cluster ab: `cluster unjoin -node node-name`

    Sie müssen diesen Schritt für jeden Knoten durchführen.

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC"from the cluster.
You must
         remove the failover partner as well. After the node is removed,
erase
         its configuration and initialize all disks by usingthe "Clean
         configuration and initialize all disks (4)" option from the
boot menu.
Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

14. Wenn in der Konfiguration FC-to-SAS-Bridges oder FC-Back-End-Switches verwendet werden, trennen und entfernen Sie diese.

Entfernen Sie FC-to-SAS-Bridges

a. Identifizieren Sie die Brücken:

```
system bridge show
```

b. Entfernen Sie die Brücken:

```
system bridge remove -name <bridge_name>
```

c. Vergewissern Sie sich, dass die Brücken entfernt wurden:

```
system bridge show
```

Das folgende Beispiel zeigt, dass die Brücken entfernt werden:

Beispiel

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is        Monitor
    Bridge     Symbolic Name Vendor  Model     Bridge WWN
Monitored Status
    ---------- ------------- ------- --------- ----------------
--------- -------
    ATTO_FibreBridge6500N_1
               Bridge Number 16
                             Atto    FibreBridge 6500N
                                                 2000001086603824
false     -
    ATTO_FibreBridge6500N_2
               Not Set       Atto    FibreBridge 6500N
                                                 20000010866037e8
false     -
    ATTO_FibreBridge6500N_3
               Not Set       Atto    FibreBridge 6500N
                                                 2000001086609e0e
false     -
    ATTO_FibreBridge6500N_4
               Not Set       Atto    FibreBridge 6500N
                                                 2000001086609c06
false     -
    4 entries were displayed.
```

Entfernen Sie die FC-Switches

a. Identifizieren Sie die Switches:

```
system switch fibre-channel show
```

b. Entfernen Sie die Schalter:

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. Vergewissern Sie sich, dass die Schalter entfernt wurden:

```
system switch fibre-channel show
```

Beispiel

```
cluster1::> system switch fibre-channel show
                Symbolic                                      Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    Cisco_10.226.197.34
                mcc-cisco-8Gb-fab-4
                         Cisco   DS-C9148-16P-K9
                                            2000547fee78f088
true      ok
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed.
cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                Symbolic                                      Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    mcc-cisco-8Gb-fab-4
                mcc-cisco-8Gb-fab-4
                         Cisco
                                 -          -
false     -
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
```

```
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed
cluster1::>
```

15. Schalten Sie die MetroCluster FC Controller-Module und Storage Shelfs aus.
16. Trennen Sie die MetroCluster FC-Controller-Module und Storage-Shelfs, und entfernen Sie sie.

Abschluss der Transition

Zum Abschluss der Umstellung müssen Sie den Betrieb der neuen MetroCluster IP-Konfiguration überprüfen.

1. Überprüfen Sie die MetroCluster IP-Konfiguration.

   Sie müssen diesen Schritt auf jedem Cluster im erweiterten Berechtigungsmodus ausführen.

   Im folgenden Beispiel wird die Ausgabe für „Cluster_A“ angezeigt

```
cluster_A::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_A_1-IP          true    true          false
node_A_2-IP          true    true          false
2 entries were displayed.

cluster_A::>
```

   Im folgenden Beispiel wird die Ausgabe für „Cluster_B“ angezeigt

```
cluster_B::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_B_1-IP          true    true          false
node_B_2-IP          true    true          false
2 entries were displayed.

cluster_B::>
```

2. Aktivieren von Cluster-HA und Storage-Failover

   Sie müssen diesen Schritt für jedes Cluster durchführen.

3. Vergewissern Sie sich, dass die Cluster-HA-Funktion aktiviert ist.

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>


cluster_A::> storage  failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1-IP    node_A_2-IP    true     Connected to node_A_2-IP
node_A_2-IP    node_A_1-IP    true     Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. Deaktivieren Sie den MetroCluster-Übergangsmodus.

   a. Ändern Sie die erweiterte Berechtigungsebene: `set -privilege advanced`
   b. Übergangsmodus deaktivieren:`metrocluster transition disable`
   c. Zurück zur Administratorberechtigungsebene: `set -privilege admin`

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. Vergewissern Sie sich, dass die Transition deaktiviert ist:`metrocluster transition show-mode`

   Sie müssen diese Schritte auf beiden Clustern durchführen.

```
cluster_A::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_A::>
```

```
cluster_B::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_B::>
```

6. Wenn Sie über eine Konfiguration mit acht Nodes verfügen, müssen Sie den gesamten Vorgang ab wiederholen "Vorbereitung auf den Übergang von einer MetroCluster FC- zu einer MetroCluster IP-Konfiguration" Für jede der FC DR-Gruppen.

Senden einer benutzerdefinierten AutoSupport Meldung nach der Wartung

Nach Abschluss des Übergangs sollten Sie eine AutoSupport-Nachricht mit dem Ende der Wartung senden, damit die automatische Case-Erstellung fortgesetzt werden kann.

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Wiederherstellen der Tiebreaker- oder Mediator-Überwachung

Nach Abschluss der MetroCluster Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

1. Verwenden Sie das entsprechende Verfahren für Ihre Konfiguration.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen"
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration"

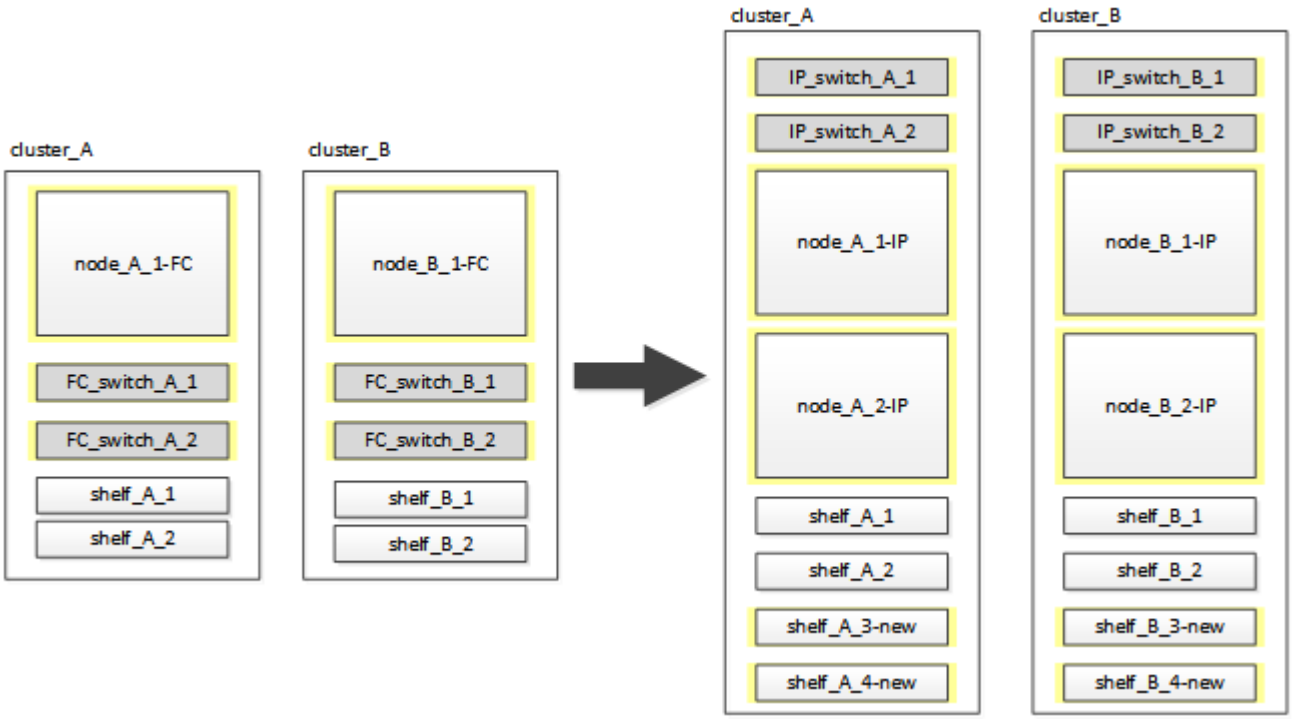
Unterbrechungsfreier Übergang von einer MetroCluster FC Konfiguration mit zwei Nodes auf eine MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher)

Unterbrechungsfreie Umstellung von einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher)

Ab ONTAP 9.8 können Sie Workloads und Daten von einer bestehenden MetroCluster FC Konfiguration mit zwei Nodes auf eine neue MetroCluster IP-Konfiguration mit vier

Nodes umstellen. Festplatten-Shelfs der MetroCluster FC-Nodes werden zu IP-Nodes verschoben.

Die folgende Abbildung bietet eine vereinfachte Ansicht der Konfiguration vor und nach diesem Migrationsvorgang.



- Dieses Verfahren wird auf Systemen mit ONTAP 9.8 und höher unterstützt.
- Dieser Vorgang ist störend.
- Dieses Verfahren gilt nur für eine MetroCluster FC-Konfiguration mit zwei Nodes.

  Wenn Sie über eine MetroCluster-FC-Konfiguration mit vier Nodes verfügen, finden Sie Informationen unter "Auswahl des Migrationsverfahrens".

- ADP wird in der mit diesem Verfahren erstellten vier-Knoten-MetroCluster-IP-Konfiguration nicht unterstützt.
- Sie müssen alle Anforderungen erfüllen und alle Schritte des Verfahrens befolgen.
- Die vorhandenen Storage-Shelves werden auf die neuen MetroCluster IP-Knoten verschoben.
- Bei Bedarf können der Konfiguration zusätzliche Storage Shelves hinzugefügt werden.

  Siehe "Wiederverwendung von Festplatten-Shelfs und Festplattenanforderungen für einen unterbrechungsfreien Wechsel von FC zu IP".

Beispiel für die Benennung in diesem Verfahren

Bei diesem Verfahren werden durchgängig Beispielnamen verwendet, um die involvierten DR-Gruppen, Nodes und Switches zu identifizieren.

Die Nodes in der ursprünglichen Konfiguration verfügen über das Suffix -FC und geben an, dass sie sich in einer Fabric-Attached- oder Stretch-MetroCluster-Konfiguration befinden.

Komponenten	Cluster_A an Standort_A	Cluster_B an Standort_B
dr_Group_1-FC	• Node_A_1-FC • Shelf_A_1 • Shelf_A_2	• Node_B_1-FC • Shelf_B_1 • Shelf_B_2
dr_Group_2-IP	• Node_A_1-IP • Node_A_2-IP • Shelf_A_1 • Shelf_A_2 • Shelf_A_3-neu • Shelf_A_4-neu	• Node_B_1-IP • Node_B_2-IP • Shelf_B_1 • Shelf_B_2 • Shelf_B_3-neu • Shelf_B_4-neu
Schalter	• Switch_A_1-FC • Switch_A_2-FC • Switch_A_1-IP • Switch_A_2-IP	• Switch_B_1-FC • Switch_B_2-FC • Switch_B_1-IP • Switch_B_2-IP

Vorbereitung auf den Umstieg mit FC-to-IP und Störungen

Bevor Sie mit dem Umstieg beginnen, müssen Sie sicherstellen, dass die Konfiguration die Anforderungen erfüllt.

Aktivieren Sie die Konsolenprotokollierung

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Allgemeine Anforderungen für die disruptive FC-to-IP Umstellung

Die vorhandene MetroCluster FC-Konfiguration muss die folgenden Anforderungen erfüllen:

- Die Konfiguration muss zwei Nodes sein, und alle Nodes müssen ONTAP 9.8 oder höher ausführen.

  Dabei kann es sich um eine Fabric-Attached oder eine Stretch-MetroCluster mit zwei Nodes handelt.

- Er muss alle Anforderungen und Verkabelung erfüllen, wie in den Verfahren *MetroCluster Installation and Configuration* beschrieben.

  "Installation und Konfiguration von Fabric-Attached MetroCluster"

  "Installation und Konfiguration von Stretch MetroCluster"

- Es kann nicht mit NetApp Storage Encryption (NSE) konfiguriert werden.
- Die MDV-Volumes können nicht verschlüsselt werden.

Sie müssen über Remote-Konsolenzugriff für alle sechs Nodes von einem MetroCluster Standort aus verfügen oder Reisen zwischen den Standorten planen, wie im Verfahren erforderlich.

Wiederverwendung von Festplatten-Shelfs und Festplattenanforderungen für einen unterbrechungsfreien Wechsel von FC zu IP

Es muss sichergestellt werden, dass auf den Storage-Shelves ausreichend freie Laufwerke und Root-Aggregatspeicherplatz zur Verfügung stehen.

Wiederverwendung der vorhandenen Storage Shelfs

Bei Verwendung dieses Verfahrens werden die vorhandenen Storage-Shelfs zur Verwendung durch die neue Konfiguration beibehalten. Wenn Node_A_1-FC und Node_B_1-FC entfernt werden, werden die vorhandenen Laufwerk-Shelfs auf Cluster_A_1-IP und Node_A_2-IP auf Cluster_A sowie Node_B_1-IP und Node_B_2-IP auf Cluster_B verbunden

- Die vorhandenen Storage-Shelfs (diejenigen, die an Node_A_1-FC und Node_B_1-FC angeschlossen sind) müssen von den neuen Plattformmodellen unterstützt werden.

  Wenn die vorhandenen Shelfs nicht von den neuen Plattformmodellen unterstützt werden, finden Sie unter "Unterbrechungsfreie Transition, wenn vorhandene Shelfs nicht auf neuen Controllern unterstützt werden (ONTAP 9.8 und höher)".

- Sie müssen sicherstellen, dass Sie die Plattformgrenzen für Laufwerke usw. nicht überschreiten

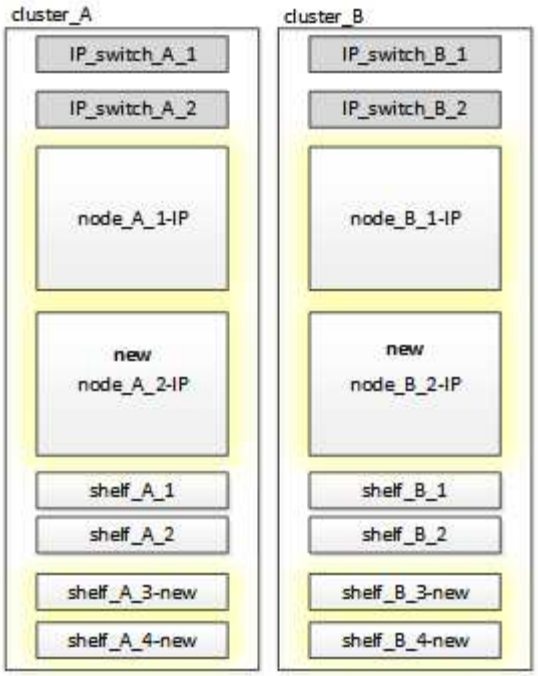
  "NetApp Hardware Universe"

Storage-Anforderungen für die zusätzlichen Controller

Falls erforderlich muss zusätzlicher Storage hinzugefügt werden, um die beiden zusätzlichen Controller unterzubringen (Node_A_2-IP und Node_B_2-ip), da die Konfiguration von einer Anordnung mit zwei Nodes auf vier Nodes geändert wird.

- Je nach den in den vorhandenen Shelves verfügbaren Spare-Laufwerken müssen zusätzliche Laufwerke hinzugefügt werden, um die zusätzlichen Controller in der Konfiguration zu unterstützen.

  Dies erfordert möglicherweise zusätzliche Storage Shelves, wie in der folgenden Abbildung dargestellt.



Sie benötigen weitere 14 bis 18 Laufwerke für die dritte und vierte Controller (Node_A_2-IP und Node_B_2-IP):

- Drei Pool0-Laufwerke
- Drei Pool1-Laufwerke
- Zwei Ersatzlaufwerke
- Sechs bis zehn Laufwerke für das System-Volume

- Sie müssen sicherstellen, dass die Konfiguration, einschließlich der neuen Nodes, die Plattformlimits für die Konfiguration nicht überschreitet, einschließlich Laufwerksanzahl, Root-Aggregatgröße usw.

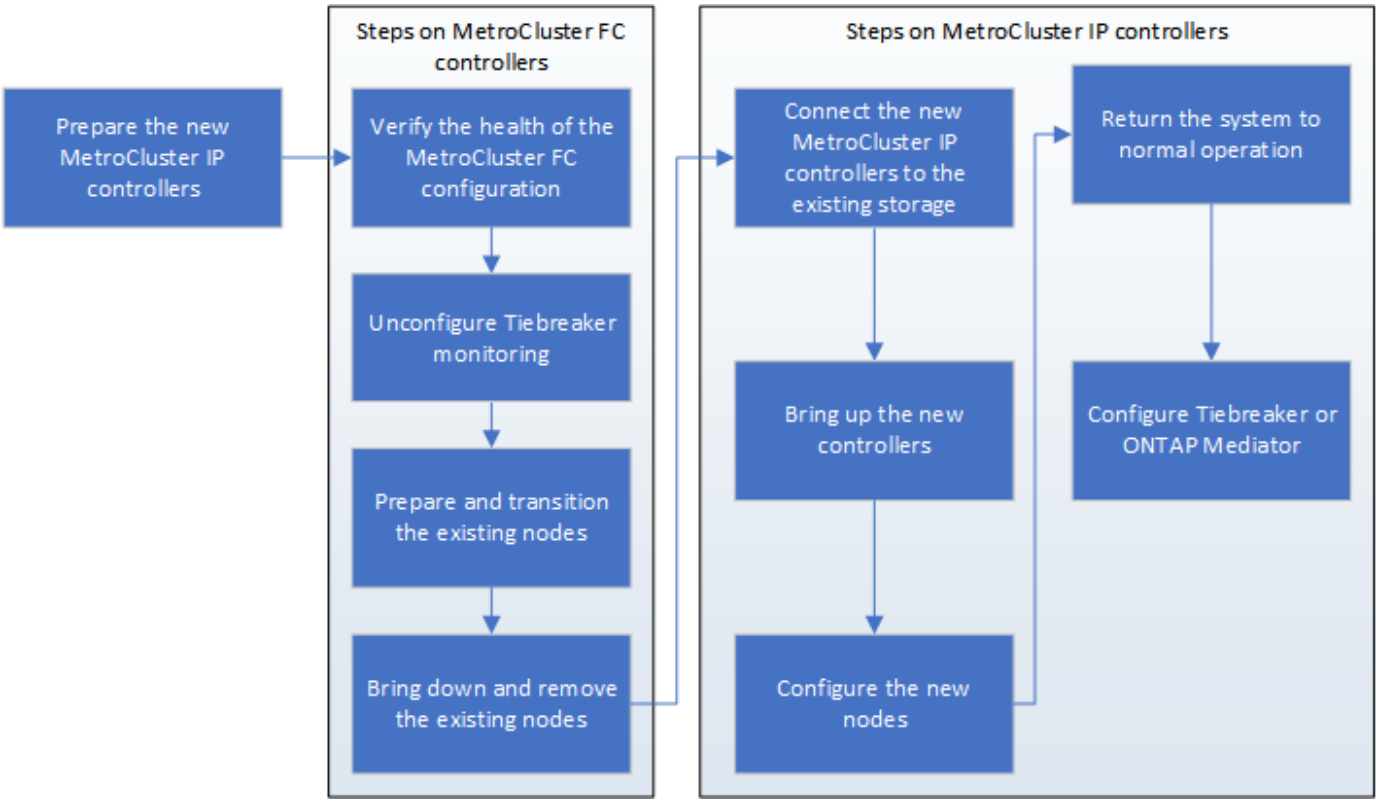
  Diese Informationen sind für jedes Plattformmodell bei *NetApp Hardware Universe* verfügbar.

  "NetApp Hardware Universe"

Workflow für Unterbrechungen

Um eine erfolgreiche Umstellung sicherzustellen, müssen Sie den spezifischen Workflow einhalten.

Planen Sie bei der Vorbereitung der Transition die Reise zwischen den Standorten ein. Beachten Sie, dass Sie nach dem Rack und verkabelt der Remote-Nodes seriellen Zugriff auf die Nodes benötigen. Der Service-Prozessor-Zugriff ist erst verfügbar, wenn die Nodes konfiguriert sind.



Zuordnen von Ports von den MetroCluster FC-Nodes zu den MetroCluster IP-Nodes

Sie müssen die Port- und LIF-Konfiguration des MetroCluster FC-Node anpassen, damit er mit dem MetroCluster IP-Node kompatibel ist, der den Node ersetzt.

Über diese Aufgabe

Wenn die neuen Nodes zum ersten Mal während des Upgrades gebootet werden, verwendet jeder Node die aktuellste Konfiguration des Node, der ausgetauscht wird. Wenn Sie Node_A_1-IP booten, versucht ONTAP, LIFs auf denselben Ports zu hosten, die auf Node_A_1-FC verwendet wurden.

Während des Übergangs führen Sie sowohl für die alten als auch für die neuen Nodes Schritte durch, um eine korrekte Cluster-, Management- und Daten-LIF-Konfiguration sicherzustellen.

Schritte

1. Identifizieren Sie alle Konflikte zwischen der vorhandenen MetroCluster FC-Port-Nutzung und der Portnutzung für die MetroCluster IP-Schnittstellen auf den neuen Nodes.

   Sie müssen die MetroCluster IP-Ports auf den neuen MetroCluster IP Controllern mithilfe der folgenden Tabelle identifizieren. Überprüfen und protokollieren Sie dann, ob Daten-LIFs oder Cluster-LIFs auf den Ports auf den MetroCluster FC-Nodes vorhanden sind.

   Diese gegensätzlichen Daten-LIFs oder Cluster-LIFs auf den MetroCluster FC Nodes werden beim entsprechenden Schritt beim Migrationsvorgang verschoben.

   In der folgenden Tabelle werden die MetroCluster IP-Ports nach Plattformmodell aufgeführt. Sie können die Spalte VLAN-ID ignorieren.

Modell der Plattform	MetroCluster-IP-Port	VLAN-ID	

AFF A800	e0b	Nicht verwendet	
	e1b		
AFF A700 UND FAS9000	e5a		
	E5b		
AFF A320	e0g.		
	e0h		
AFF A300 UND FAS8200	e1a		
	e1b		
FAS8300/A400/FAS8700	e1a	10	
	e1b	20	
AFF A250 und FAS500f	e0c	10	
	e0b	20	

Sie können die folgende Tabelle ausfüllen und später im Migrationsverfahren nachschlagen.

Ports	Entsprechende MetroCluster IP-Schnittstellen-Ports (aus Tabelle oben)	LIFs auf diesen Ports auf den MetroCluster FC-Nodes sind widersprüchlich
Erster MetroCluster-IP-Port auf Node_A_1-FC		
Zweiter MetroCluster-IP-Port auf Node_A_1-FC		
Erster MetroCluster-IP-Port auf Node_B_1-FC		
Zweiter MetroCluster-IP-Port auf Node_B_1-FC		

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

   Die Port-Nutzung des Controllers hängt vom Plattformmodell und dem IP-Switch-Modell ab, das Sie in der MetroCluster IP-Konfiguration verwenden werden. Sie können die Port-Nutzung der neuen Plattformen von

NetApp Hardware Universe erfassen.

"NetApp Hardware Universe"

3. Notieren Sie bei Bedarf die Portinformationen für Node_A_1-FC und Node_A_1-IP.

   Bei der Durchführung des Übergangsverfahrens wird auf die Tabelle verwiesen.

   Fügen Sie in den Spalten für Node_A_1-IP die physischen Ports für das neue Controller-Modul hinzu und planen Sie die IPspaces und Broadcast-Domänen für den neuen Knoten.

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

4. Notieren Sie ggf. alle Portinformationen für Node_B_1-FC.

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

   Fügen Sie in den Spalten für Node_B_1-IP die physischen Ports für das neue Controller-Modul hinzu und planen Sie die Verwendung des LIF-Ports, IPspaces und Broadcast-Domänen für den neuen Knoten.

	Node_B_1-FC			Node_B_1-IP		
LIF	Physische Ports	IPspaces	Broadcast-Domänen	Physische Ports	IPspaces	Broadcast-Domänen
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node-Management						
Cluster-Management						
Daten 1						
Daten 2						
Daten 3						
Daten 4						
San						
Intercluster-Port						

Vorbereiten der MetroCluster IP-Controller

Sie müssen die vier neuen MetroCluster IP-Knoten vorbereiten und die korrekte ONTAP-Version installieren.

Über diese Aufgabe

Diese Aufgabe muss auf jedem der neuen Knoten ausgeführt werden:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

Die Nodes sollten mit jedem **neuen** Storage-Shelf verbunden sein. Sie müssen **nicht** an die vorhandenen Storage Shelfs mit Daten angeschlossen sein.

Diese Schritte können Sie jetzt oder später bei der Ablage der Controller und Shelfs durchführen. In jedem Fall

müssen Sie sicherstellen, dass Sie die Konfiguration löschen und die Knoten **vorbereiten, bevor** sie mit den vorhandenen Speicher-Shelfs verbinden und **bevor** Änderungen an der Konfiguration an den MetroCluster FC Nodes vornehmen.

> Führen Sie diese Schritte nicht durch, wenn die MetroCluster IP-Controller mit den vorhandenen Storage-Shelfs verbunden sind, die mit den MetroCluster FC-Controllern verbunden waren.

Löschen Sie in diesen Schritten die Konfiguration auf den Knoten und löschen Sie den Mailbox-Bereich auf neuen Laufwerken.

Schritte

1. Verbinden Sie die Controller-Module mit den neuen Storage Shelfs.
2. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte „`mccip`“ sein.

3. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

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

4. Beenden des Wartungsmodus:

   ```
   halt
   ```

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

5. Wiederholen Sie die folgenden Teilschritte auf allen vier Knoten, um die Konfiguration zu löschen:

   a. Legen Sie die Umgebungsvariablen auf Standardwerte fest:

      ```
      set-defaults
      ```

   b. Umgebung speichern:

      ```
      saveenv
      ```

   ```
   bye
   ```

6. Wiederholen Sie die folgenden Teilschritte, um alle vier Knoten mit der Option 9a im Startmenü zu booten.

   a. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

      ```
      boot_ontap menu
      ```

   b. Wählen Sie im Startmenü die Option „`9a`“, um den Controller neu zu booten.

7. Starten Sie jeden der vier Knoten in den Wartungsmodus mit der Option „`5`“ im Startmenü.
8. Notieren Sie die System-ID und von jedem der vier Knoten:

```
sysconfig
```

9. Wiederholen Sie die folgenden Schritte auf Node_A_1-IP und Node_B_1-IP.
   a. Weisen Sie jedem Standort das Eigentum aller lokalen Festplatten zu:

      ```
      disk assign adapter.xx.*
      ```

   b. Wiederholen Sie den vorherigen Schritt für jeden HBA mit angeschlossenen Laufwerk-Shelfs auf Node_A_1-IP und Node_B_1-IP.
10. Wiederholen Sie die folgenden Schritte auf Node_A_1-IP und Node_B_1-IP, um den Mailbox-Bereich auf jeder lokalen Festplatte zu löschen.
    a. Zerstören Sie den Mailbox-Bereich auf jeder Festplatte:

       ```
       mailbox destroy local``mailbox destroy partner
       ```

11. Beenden aller vier Controller:

    ```
    halt
    ```

12. Zeigen Sie auf jedem Controller das Startmenü an:

    ```
    boot_ontap menu
    ```

13. Löschen Sie bei jedem der vier Controller die Konfiguration:

    ```
    wipeconfig
    ```

    Wenn der Wipeconfig-Vorgang abgeschlossen ist, kehrt der Knoten automatisch zum Boot-Menü zurück.

14. Wiederholen Sie die folgenden Teilschritte, um alle vier Knoten mithilfe der Option 9a im Startmenü erneut zu booten.
    a. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

       ```
       boot_ontap menu
       ```

    b. Wählen Sie im Startmenü die Option „`9a`“, um den Controller neu zu booten.
    c. Lassen Sie das Controller-Modul vor dem Wechsel zum nächsten Controller-Modul booten.

    Nach Abschluss von „`9a`“ kehren die Nodes automatisch zum Startmenü zurück.

15. Schalten Sie die Controller aus.

Überprüfen des Systemzustands der MetroCluster FC-Konfiguration

Sie müssen vor der Umstellung den Zustand und die Konnektivität der MetroCluster FC-Konfiguration überprüfen

Diese Aufgabe wird in der MetroCluster FC-Konfiguration ausgeführt.

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

```
node run -node node-name sysconfig -a
```

b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

```
system health alert show
```

c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

d. Durchführen einer MetroCluster-Prüfung:

```
metrocluster check run
```

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

f. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

g. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

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

2. Vergewissern Sie sich, dass sich die Nodes im Non-HA-Modus befinden:

```
storage failover show
```

Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "Entfernen von MetroCluster-Konfigurationen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Umstellung der MetroCluster FC Nodes

Sie müssen Informationen von den vorhandenen MetroCluster FC Nodes erfassen, eine AutoSupport-Meldung mit Beginn der Wartung senden und die Nodes wechseln.

Sammeln von Informationen aus den vorhandenen Controller-Modulen vor dem Umstieg

Vor dem Übergang müssen Sie Informationen für jeden der Nodes erfassen.

Diese Aufgabe wird auf den vorhandenen Knoten durchgeführt:

- Node_A_1-FC
- Node_B_1-FC

a. Sammeln Sie die Ausgabe für die Befehle in der folgenden Tabelle.

Kategorie	Befehle	Hinweise
Lizenz	Systemlizenz anzeigen	
Shelfs und Anzahl von Festplatten in jedem Shelf und Flash Storage sowie Arbeitsspeicher, NVRAM und Netzwerkkarten	Auf dem System-Node wird -Node_Name sysconfig ausgeführt	
LIFs für das Cluster-Netzwerk- und Node-Management	System Node Run -Node_Name sysconfig Netzwerkschnittstelle show -role „Cluster,Node-mgmt,Daten“	
SVM-Informationen	vserver zeigen	
Protokollinformationen	nfs zeigen iscsi zeigen cifs zeigen	
Physische Ports	Netzwerk-Port show -Node_Name -type physischer Netzwerk-Port wird angezeigt	
Failover-Gruppen	Failover-Gruppen für Netzwerkschnittstellen zeigen -vserver vserver_Name	Notieren Sie die Namen und Ports der Failover-Gruppen, die nicht clusterweit sind.
VLAN-Konfiguration	Netzwerk-Port-vlan show -Node_Name	Zeichnen Sie die Paarung jedes Netzwerkports und jeder VLAN-ID auf.
Konfiguration der Schnittstellengruppe	Netzwerkport iffrp show -Node Node_Name -instance	Notieren Sie die Namen der Schnittstellengruppen und der ihnen zugewiesenen Ports.
Broadcast-Domänen	Netzwerk-Port Broadcast-Domain anzeigen	
IP-Bereich	Netzwerk-ipspace wird angezeigt	
Volume-Infos	Volume show und Volume show -fields verschlüsseln	
Info Zu Aggregaten	Storage Aggregat show und Storage aggr Encryption show andStorage aggregate object Store show	

Kategorie	Befehle	Hinweise
Festplattenbesitzer	Storage Aggregat show und Storage aggr Encryption show andStorage aggregate object Store show	
Verschlüsselung	Speicherplatz-Failover-Mailbox-Disk show und Security Key-Manager-Backup zeigen	Bewahren Sie auch die Passphrase auf, die zum Aktivieren des Schlüsselmanagers verwendet wird. Bei einem externen Schlüsselmanager benötigen Sie die Authentifizierungsinformationen für den Client und Server.
Verschlüsselung	Security Key-Manager zeigen	
Verschlüsselung	Externe Sicherheitstaste-Manager-Show	
Verschlüsselung	Systemell lokale kenv kmip.init.ipaddr ip-Adresse	
Verschlüsselung	Systemshell lokale kenv kmip.init.netmask Netzmaske	
Verschlüsselung	Systemshell lokale kenv kmip.init.gateway Gateway	
Verschlüsselung	Systemshell lokale kenv kmip.init.interface-Schnittstelle	

Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Dadurch wird verhindert, dass ein Fall unter der Annahme eröffnet wird, dass eine Störung aufgetreten ist.

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit die Wartung läuft.
   a. Geben Sie den folgenden Befehl ein: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      Maintenance-Fenster in Stunden gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Wiederholen Sie den Befehl im Partner-Cluster.

Umstiegs-, Herunterfahren und Entfernen der MetroCluster FC-Nodes

Zusätzlich zum Ausgeben von Befehlen an den MetroCluster FC-Knoten umfasst diese Aufgabe das physische Funktioneln und Entfernen der Controller-Module an jedem Standort.

Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden:

- Node_A_1-FC
- Node_B_1-FC

Schritte

1. Beenden Sie den gesamten Client-Datenverkehr.
2. Aktivieren Sie auf einem der MetroCluster FC-Nodes, z. B. Node_A_1-FC, die Transition.
   a. Legen Sie die erweiterte Berechtigungsebene fest: `set -priv advanced`
   b. Übergang ermöglichen: `metrocluster transition enable -transition-mode disruptive`
   c. Zurück zum Admin-Modus: `set -priv admin`
3. Heben Sie das Root-Aggregat auf, indem Sie den Remote Plex der Root-Aggregate löschen.
   a. Root-Aggregate ermitteln: `storage aggregate show -root true`
   b. Zeigen Sie die Pool1-Aggregate an: `storage aggregate plex show -pool 1`
   c. Offline und löschen Sie den Remote-Plex des Root-Aggregats:
      `aggr plex offline <root-aggregate> -plex <remote-plex-for-root-aggregate>`

      `aggr plex delete <root-aggregate> -plex <remote-plex-for-root-aggregate>`

      Beispiel:

```
# aggr plex offline aggr0_node_A_1-FC_01 -plex remoteplex4
```

+

```
# aggr plex delete aggr0_node_A_1-FC_01 -plex remoteplex4
```

4. Bestätigen Sie die Mailbox-Anzahl, die automatische Zuordnung der Festplatte und den Übergangsmodus, bevor Sie mit den folgenden Befehlen an jedem Controller fortfahren:
   a. Legen Sie die erweiterte Berechtigungsebene fest: `set -priv advanced`
   b. Vergewissern Sie sich, dass für jedes Controller-Modul nur drei Mailbox-Laufwerke angezeigt werden: `storage failover mailbox-disk show`
   c. Zurück zum Admin-Modus: `set -priv admin`
   d. Vergewissern Sie sich, dass der Umstiegmodus störend ist: MetroCluster Transition show
5. Prüfen Sie auf defekte Festplatten: `disk show -broken`
6. Entfernen oder ersetzen Sie alle defekten Festplatten
7. Überprüfen Sie, ob sich Aggregate in einem ordnungsgemäßen Zustand befinden, indem Sie die folgenden Befehle auf Node_A_1-FC und Node_B_1-FC verwenden:

   `storage aggregate show`

```
storage aggregate plex show
```

Der Befehl Storage Aggregate show gibt an, dass das Root-Aggregat nicht gespiegelt ist.

8. VLANs oder Schnittstellengruppen prüfen:

```
network port ifgrp show
```

```
network port vlan show
```

Wenn keine vorhanden sind, überspringen Sie die folgenden beiden Schritte.

9. Zeigen Sie die Liste der LIFs mithilfe von VLANs oder ifgrps an:

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

```
network port show -type if-group | vlan
```

10. Entfernen Sie alle VLANs und Schnittstellengruppen.

Sie müssen diese Schritte für alle LIFs in allen SVMs durchführen, einschließlich der SVMs mit dem -mc -Suffix.

a. Verschieben Sie alle LIFs über VLANs oder Schnittstellengruppen zu einem verfügbaren Port: `network interface modify -vserver vserver-name -lif lif_name -home- port port`
b. Zeigen Sie die LIFs an, die sich nicht an ihren Home-Ports befinden: `network interface show -is-home false`
c. Alle LIFs auf die jeweiligen Home-Ports zurücksetzen: `network interface revert -vserver vserver_name -lif lif_name`
d. Vergewissern Sie sich, dass sich alle LIFs auf ihren Home-Ports befinden: `network interface show -is-home false`

   Es sollten keine LIFs in der Ausgabe angezeigt werden.

e. VLAN- und ifgrp-Ports aus Broadcast-Domäne entfernen: `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`
f. Vergewissern Sie sich, dass nicht alle vlan- und ifgrp-Ports einer Broadcast-Domäne zugeordnet sind: `network port show -type if-group | vlan`
g. Alle VLANs löschen: `network port vlan delete -node nodename -vlan-name vlan-name`
h. Löschen von Schnittstellengruppen: `network port ifgrp delete -node nodename -ifgrp ifgrp-name`

11. Verschieben Sie alle LIFs nach Bedarf, um Konflikte mit den MetroCluster IP-Schnittstellen-Ports zu lösen.

Sie müssen die in Schritt 1 von identifizierten LIFs verschieben "Zuordnen von Ports von den MetroCluster FC-Nodes zu den MetroCluster IP-Nodes".

a. Verschieben Sie alle LIFs, die auf dem gewünschten Port gehostet werden, zu einem anderen Port: `network interface modify -lif lifname -vserver vserver-name -home-port new-`

`homeport``network interface revert -lif lifname -vserver vservername`

b. Bewegen Sie den Zielanschluss gegebenenfalls in einen entsprechenden IPspace und Broadcast-Domäne. `network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast-domain current-broadcast-domain -ports controller-name:current-port``network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port`

12. Beenden Sie die MetroCluster FC-Controller (Node_A_1-FC und Node_B_1-FC): `system node halt`
13. Synchronisieren Sie an der LOADER-Eingabeaufforderung die Hardware-Uhren zwischen den FC- und IP-Controller-Modulen.
    a. Zeigen Sie auf dem alten MetroCluster FC-Knoten (Node_A_1-FC) das Datum an: `show date`
    b. Legen Sie auf den neuen MetroCluster IP-Controllern (Node_A_1-IP und Node_B_1-IP) das am ursprünglichen Controller angezeigte Datum fest: `set date mm/dd/yy`
    c. Überprüfen Sie auf den neuen MetroCluster IP-Controllern (Node_A_1-IP und Node_B_1-IP) das Datum: `show date`
14. Anhalten und Abschalten der MetroCluster FC-Controller-Module (Node_A_1-FC und Node_B_1-FC), FC-to-SAS-Bridges (falls vorhanden), FC-Switches (falls vorhanden) und jedes mit diesen Nodes verbundene Storage-Shelf
15. Trennen Sie die Shelfs von den MetroCluster FC Controllern und dokumentieren Sie, welche Shelfs für jedes Cluster lokal sind.
16. Wenn in der Konfiguration FC-to-SAS-Bridges oder FC-Back-End-Switches verwendet werden, trennen und entfernen Sie diese.

Entfernen Sie FC-to-SAS-Bridges

a. Identifizieren Sie die Brücken:

```
system bridge show
```

b. Entfernen Sie die Brücken:

```
system bridge remove -name <bridge_name>
```

c. Vergewissern Sie sich, dass die Brücken entfernt wurden:

```
system bridge show
```

Das folgende Beispiel zeigt, dass die Brücken entfernt werden:

Beispiel

```
cluster1::> system bridge remove -name ATTO_10.226.197.16
cluster1::> system bridge show

Is        Monitor
    Bridge     Symbolic Name Vendor  Model     Bridge WWN
Monitored Status
    ---------- ------------- ------- --------- ----------------
--------- -------
    ATTO_FibreBridge6500N_1
               Bridge Number 16
                             Atto    FibreBridge 6500N
                                                 2000001086603824
false     -
    ATTO_FibreBridge6500N_2
               Not Set       Atto    FibreBridge 6500N
                                                 20000010866037e8
false     -
    ATTO_FibreBridge6500N_3
               Not Set       Atto    FibreBridge 6500N
                                                 2000001086609e0e
false     -
    ATTO_FibreBridge6500N_4
               Not Set       Atto    FibreBridge 6500N
                                                 2000001086609c06
false     -
    4 entries were displayed.
```

Entfernen Sie die FC-Switches

a. Identifizieren Sie die Switches:

```
system switch fibre-channel show
```

b. Entfernen Sie die Schalter:

```
system switch fibre-channel remove -switch-name <switch_name>
```

c. Vergewissern Sie sich, dass die Schalter entfernt wurden:

```
system switch fibre-channel show
```

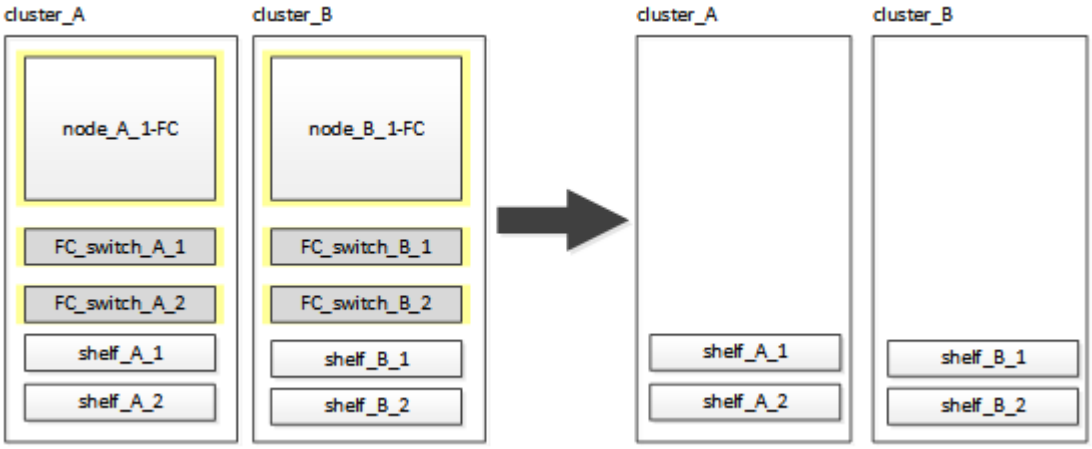
Beispiel

```
cluster1::> system switch fibre-channel show
                Symbolic                                      Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    Cisco_10.226.197.34
                mcc-cisco-8Gb-fab-4
                         Cisco   DS-C9148-16P-K9
                                            2000547fee78f088
true      ok
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed.
cluster1::> system switch fibre-channel remove -switch-name
Cisco_10.226.197.34
cluster1::> system switch fibre-channel show
                Symbolic                                      Is
Monitor
    Switch      Name     Vendor  Model      Switch WWN
Monitored Status
    ----------- -------- ------- ---------- ----------------
--------- -------
    mcc-cisco-8Gb-fab-4
                mcc-cisco-8Gb-fab-4
                         Cisco
                                 -          -
false     -
    mcc-cisco-8Gb-fab-1
                mcc-cisco-8Gb-fab-1
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-2
```

```
                mcc-cisco-8Gb-fab-2
                         Cisco   -          -
false     -
    mcc-cisco-8Gb-fab-3
                mcc-cisco-8Gb-fab-3
                         Cisco   -          -
false     -
    4 entries were displayed
cluster1::>
```

17. Vergewissern Sie sich im Wartungsmodus auf den MetroCluster FC Nodes (Node_A_1-FC und Node_B_1-FC), dass keine Festplatten verbunden sind: `disk show -v`
18. Schalten Sie die MetroCluster FC-Nodes aus und entfernen Sie sie.

An diesem Punkt wurden die MetroCluster FC Controller entfernt und die Shelves werden von allen Controllern getrennt.



Anschließen der MetroCluster IP-Controller-Module

Die Konfiguration muss die vier neuen Controller-Module und alle zusätzlichen Storage Shelfs enthalten. Die neuen Controller-Module werden zwei Mal hinzugefügt.

Einrichten der neuen Controller

Sie müssen die neuen MetroCluster IP Controller in einem Rack unterbringen und mit den zuvor mit den MetroCluster FC-Controllern verbundenen Storage-Shelfs verkabeln.

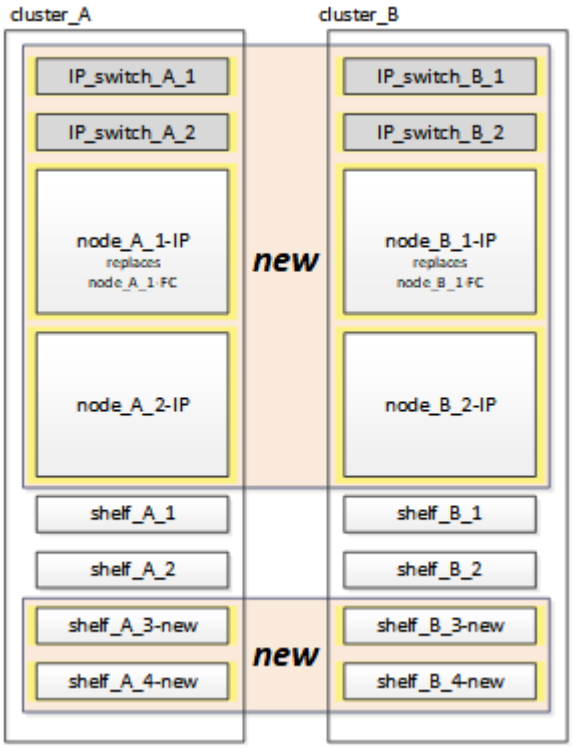
Über diese Aufgabe

Diese Schritte müssen auf jedem der MetroCluster IP Knoten durchgeführt werden.

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP

- Node_B_2-IP

Im folgenden Beispiel werden an jedem Standort zwei zusätzliche Storage Shelfs hinzugefügt, um den Storage für die neuen Controller-Module bereitzustellen.



Schritte

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

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

2. Richtig gemahlen.
3. Rack-Fläche für neue Geräte: Controller, Storage Shelfs und IP Switches.

   Verkabeln Sie jetzt nicht die Storage-Shelfs oder IP-Switches.

4. Schließen Sie die Stromkabel und die Verbindung der Managementkonsole an die Controller an.
5. Vergewissern Sie sich, dass alle Storage-Shelfs ausgeschaltet sind.
6. Stellen Sie sicher, dass keine Laufwerke verbunden sind, indem Sie die folgenden Schritte auf allen vier Nodes ausführen:

   a. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

      ```
      boot_ontap maint
      ```

   b. Vergewissern Sie sich, dass keine Laufwerke angeschlossen sind:

      ```
      disk show -v
      ```

   Die Ausgabe sollte keine Laufwerke anzeigen.

a. Stoppen Sie den Knoten:

```
halt
```

7. Starten Sie alle vier Knoten mit der Option 9a im Startmenü.

   a. Starten Sie an der LOADER-Eingabeaufforderung das Boot-Menü:

   ```
   boot_ontap menu
   ```

   b. Wählen Sie im Startmenü die Option „`9a`“, um den Controller neu zu booten.

   c. Lassen Sie das Controller-Modul vor dem Wechsel zum nächsten Controller-Modul booten.

   Nach Abschluss von „`9a`“ kehren die Nodes automatisch zum Startmenü zurück.

8. Die Storage-Shelfs verkabeln.

   Informationen zur Verkabelung finden Sie in den Verfahren zur Controller-Installation und -Einrichtung des Modells.

   "Dokumentation zu ONTAP Hardwaresystemen"

9. Verbinden Sie die Controller mit den IP-Switches, wie in beschrieben "Verkabeln der IP-Switches".
10. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

    Befolgen Sie die Schritte für Ihren Switch-Anbieter:

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

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

    Befolgen Sie die Schritte für Ihren Switch-Anbieter:

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

12. Schalten Sie den ersten neuen Controller (Node_A_1-IP) ein und drücken Sie Strg-C, um den Boot-Prozess zu unterbrechen und die LOADER-Eingabeaufforderung anzuzeigen.
13. Booten des Controllers in den Wartungsmodus:

    ```
    boot_ontap_maint
    ```

14. Zeigen Sie die System-ID für den Controller an:

    ```
    sysconfig -v
    ```

15. Vergewissern Sie sich, dass die Shelfs der vorhandenen Konfiguration über den neuen MetroCluster IP-Node sichtbar sind:

    ```
    storage show shelf``disk show -v
    ```

16. Stoppen Sie den Knoten:

    ```
    halt
    ```

17. Wiederholen Sie die vorherigen Schritte auf dem anderen Node am Partnerstandort (Site_B).

Verbinden und Booten von Node_A_1-IP und Node_B_1-IP

Nach dem Anschließen der MetroCluster-IP-Controller und IP-Switches wechseln und starten Sie Node_A_1-IP und Node_B_1-IP.

Node_A_1-IP wird wieder aktiv

Sie müssen den Node mit der richtigen Übergangsoption booten.

Schritte

1. Boot Node_A_1-IP zum Boot-Menü:

    ```
    boot_ontap menu
    ```

2. Geben Sie den folgenden Befehl an der Eingabeaufforderung des Startmenüs ein, um den Übergang zu initiieren:

    ```
    boot_after_mcc_transition
    ```

    - Mit diesem Befehl werden alle Festplatten, die sich im Besitz von Node_A_1-FC befinden, zu Node_A_1-IP neu zugewiesen.
      - Node_A_1-FC-Festplatten sind Node_A_1-IP zugewiesen
      - Node_B_1-FC-Festplatten sind Node_B_1-IP zugewiesen
    - Der Befehl führt auch automatisch andere erforderliche System-ID-Zuordnungen durch, damit die MetroCluster IP-Knoten an der ONTAP-Eingabeaufforderung booten können.
    - Wenn der Befehl Boot_after_mcc_Transition aus irgendeinem Grund ausfällt, sollte er über das Startmenü erneut ausgeführt werden.

    > - Wenn die folgende Eingabeaufforderung angezeigt wird, geben Sie Strg-C ein, um fortzufahren. MCC DR-Status wird überprüft… [Strg-C (Lebenslauf), S(Status), L(Link)]_ eingeben
    > - Wenn das Root-Volume verschlüsselt war, stoppt der Node mit der folgenden Meldung. Beenden des Systems, da das Root-Volume verschlüsselt ist (NetApp Volume Encryption) und der Schlüssel-Import fehlgeschlagen ist. Überprüfen Sie den Systemzustand der Schlüsselserver, wenn dieses Cluster mit einem externen (KMIP) Schlüsselmanager konfiguriert ist.

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning. Selection (1-9)?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-
FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of
MetroCluster FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
```

3. Wenn Daten-Volumes verschlüsselt sind, stellen Sie die Schlüssel mithilfe des richtigen Befehls für Ihre Schlüsselverwaltungskonfiguration wieder her.

Sie verwenden…	Befehl
• Onboard-Verschlüsselungsmanagement*	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Schlüsselmanagement	`security key-manager key query -node node-name` Weitere Informationen finden Sie unter "Wiederherstellen der externen Schlüssel für das Verschlüsselungsmanagement".

4. Wenn das Root-Volume verschlüsselt ist, verwenden Sie das Verfahren unter "Wiederherstellung des Verschlüsselungsmanagements bei Verschlüsselung des Root-Volumes".

Wiederherstellung des Verschlüsselungsmanagements bei Verschlüsselung des Root-Volumes

Wenn das Root-Volume verschlüsselt ist, müssen Sie spezielle Boot-Befehle verwenden, um das Verschlüsselungsmanagement wiederherzustellen.

Bevor Sie beginnen

Sie müssen die Passphrases früher gesammelt haben.

Schritte

1. Wenn die integrierte Schlüsselverwaltung verwendet wird, führen Sie die folgenden Teilschritte durch, um die Konfiguration wiederherzustellen.

   a. Zeigen Sie von der LOADER-Eingabeaufforderung das Boot-Menü an:

   ```
   boot_ontap menu
   ```

   b. Wählen Sie im Startmenü die Option „`(10) Set Onboard Key Management Recovery Secrets`“.

   Gehen Sie bei Bedarf auf die Eingabeaufforderungen ein:

   ```
   This option must be used only in disaster recovery procedures. Are
   you sure? (y or n): y
   Enter the passphrase for onboard key management: passphrase
   Enter the passphrase again to confirm: passphrase

   Enter the backup data: backup-key
   ```

   Das System startet zum Startmenü.

   c. Geben Sie im Startmenü die Option „`6`“ ein.

   Gehen Sie bei Bedarf auf die Eingabeaufforderungen ein:

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

   Following this, the system will reboot a few times and the following
   prompt will be available continue by saying y

   WARNING: System ID mismatch. This usually occurs when replacing a
   boot device or NVRAM cards!
   Override system ID? {y|n} y
   ```

   Nach dem Neubooten erhält das System die LOADER-Eingabeaufforderung.

   d. Zeigen Sie von der LOADER-Eingabeaufforderung das Boot-Menü an:

```
boot_ontap menu
```

e. Wählen Sie wieder Option „`(10) set Onboard Key Management Recovery Secrets`“ aus dem Boot Menu aus.

   Gehen Sie bei Bedarf auf die Eingabeaufforderungen ein:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

   Das System startet zum Startmenü.

f. Geben Sie im Startmenü die Option „`1`“ ein.

   Wenn die folgende Eingabeaufforderung angezeigt wird, können Sie Strg+C drücken, um den Vorgang fortzusetzen.

```
Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
```

   Das System bootet zur ONTAP-Eingabeaufforderung.

g. Wiederherstellung des Onboard-Verschlüsselungsmanagement:

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

   Beantworten Sie die Eingabeaufforderungen entsprechend mit der zuvor erfassten Passphrase:

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster_A":: passphrase
```

2. Wenn die externe Schlüsselverwaltung verwendet wird, führen Sie die folgenden Teilschritte durch, um die Konfiguration wiederherzustellen.

   a. Legen Sie die erforderlichen Bootargs fest:

```
setenv bootarg.kmip.init.ipaddr ip-address

setenv bootarg.kmip.init.netmask netmask

setenv bootarg.kmip.init.gateway gateway-address

setenv bootarg.kmip.init.interface interface-id
```

b. Zeigen Sie von der LOADER-Eingabeaufforderung das Boot-Menü an:

```
boot_ontap menu
```

c. Wählen Sie im Startmenü die Option „`(11) Knoten für externes Verschlüsselungsmanagement` konfigurieren.

Das System startet zum Startmenü.

d. Geben Sie im Startmenü die Option „`6`“ ein.

Das System bootet mehrmals. Sie können bestätigen, wenn Sie dazu aufgefordert werden, den Bootvorgang fortzusetzen.

Nach dem Neubooten erhält das System die LOADER-Eingabeaufforderung.

e. Legen Sie die erforderlichen Bootargs fest:

```
setenv bootarg.kmip.init.ipaddr ip-address

setenv bootarg.kmip.init.netmask netmask

setenv bootarg.kmip.init.gateway gateway-address

setenv bootarg.kmip.init.interface interface-id
```

a. Zeigen Sie von der LOADER-Eingabeaufforderung das Boot-Menü an:

```
boot_ontap menu
```

b. Wählen Sie erneut im Startmenü die Option „`(11) Knoten für die Verwaltung externer Schlüssel konfigurieren`“ aus, und reagieren Sie auf die Eingabeaufforderungen, falls erforderlich.

Das System startet zum Startmenü.

c. Stellen Sie das externe Schlüsselmanagement wieder her:

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

Erstellen der Netzwerkkonfiguration

Sie müssen eine Netzwerkkonfiguration erstellen, die der Konfiguration auf den FC-Nodes entspricht. Dies liegt daran ONTAP, dass der MetroCluster IP-Node beim Booten die gleiche Konfiguration wiedergibt. Dies bedeutet, dass Node_A_1-IP und Node_B_1-IP Boot versuchen wird, LIFs auf denselben Ports zu hosten, die auf Node_A_1-FC und Node_B_1-FC verwendet wurden.

Über diese Aufgabe

Verwenden Sie beim Erstellen der Netzwerkkonfiguration den in erstellten Plan "Zuordnen von Ports von den MetroCluster FC-Nodes zu den MetroCluster IP-Nodes" Um Ihnen zu helfen.

> Nach der Konfiguration der MetroCluster IP-Nodes ist möglicherweise eine zusätzliche Konfiguration erforderlich, um die Daten-LIFs anzuzeigen.

Schritte

1. Vergewissern Sie sich, dass sich alle Cluster-Ports in der entsprechenden Broadcast-Domäne befinden:

   Zum Erstellen von Cluster-LIFs sind der Cluster-IPspace und die Cluster-Broadcast-Domäne erforderlich

   a. IP-Bereiche anzeigen:

      ```
      network ipspace show
      ```

   b. Erstellen Sie IP-Leerzeichen und weisen Sie nach Bedarf Cluster-Ports zu.

      "Konfigurieren von IPspaces (nur Cluster-Administratoren)"

   c. Broadcast-Domänen anzeigen:

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

   d. Fügen Sie je nach Bedarf beliebige Cluster-Ports zu einer Broadcast-Domäne hinzu.

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

   e. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

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

      "Erstellen eines VLANs"

   "Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

2. Überprüfen Sie, ob die MTU-Einstellungen für die Ports und die Broadcast-Domäne korrekt eingestellt sind, und nehmen Sie mithilfe der folgenden Befehle Änderungen vor:

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

   ```
   network port broadcast-domain modify -broadcast-domain bcastdomainname -mtu
   mtu-value
   ```

Einrichten von Cluster-Ports und Cluster-LIFs

Sie müssen Cluster-Ports und LIFs einrichten. Die folgenden Schritte müssen an dem Standort Eine Node ausgeführt werden, die mit Root-Aggregaten gestartet wurden.

Schritte

1. Identifizieren Sie die Liste der LIFs mithilfe des gewünschten Cluster-Ports:

   ```
   network interface show -curr-port portname
   ```

   ```
   network interface show -home-port portname
   ```

2. Ändern Sie für jeden Cluster-Port den Home-Port einer der LIFs auf diesem Port in einen anderen Port,

   a. Rufen Sie den erweiterten Berechtigungsmodus auf, und geben Sie „`y`“ ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set priv advanced
```

b. Wenn das bearbeitete LIF eine Daten-LIF ist:

```
vserver config override -command "network interface modify -lif lifname
-vserver vservername -home-port new-datahomeport"
```

c. Wenn das LIF keine Daten-LIF ist:

```
network interface modify -lif lifname -vserver vservername -home-port new-
datahomeport
```

d. Zurücksetzen der geänderten LIFs auf ihren Home-Port:

```
network interface revert * -vserver vserver_name
```

e. Vergewissern Sie sich, dass am Cluster-Port keine LIFs vorhanden sind:

```
network interface show -curr-port portname
```

```
network interface show -home-port portname
```

a. Entfernen Sie den Port aus der aktuellen Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace ipspacename -broadcast
-domain bcastdomainname -ports node_name:port_name
```

b. Fügen Sie den Port dem Cluster-IPspace und der Broadcast-Domäne hinzu:

```
network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain
Cluster -ports node_name:port_name
```

c. Vergewissern Sie sich, dass sich die Portrolle geändert hat: `network port show`

d. Wiederholen Sie diese Teilschritte für jeden Cluster-Port.

e. Zurück zum Admin-Modus:

```
set priv admin
```

3. Erstellen von Cluster-LIFs an den neuen Cluster-Ports:

a. Verwenden Sie den folgenden Befehl, um eine automatische Konfiguration mithilfe der Link-lokalen Adresse für Cluster-LIF zu erstellen:

```
network interface create -vserver Cluster -lif cluster_lifname -service
-policy default-cluster -home-node a1name -home-port clusterport -auto true
```

b. Verwenden Sie den folgenden Befehl, um eine statische IP-Adresse für die Cluster-LIF zuzuweisen:

```
network interface create -vserver Cluster -lif cluster_lifname -service
-policy default-cluster -home-node a1name -home-port clusterport -address
ip-address -netmask netmask -status-admin up
```

LIF-Konfiguration wird überprüft

Nach der Verschiebung des Storage vom alten Controller bleiben die Node-Management-LIF, die Cluster-Management-LIF und das Intercluster LIF weiterhin vorhanden. Falls erforderlich, müssen Sie LIFs an die entsprechenden Ports verschieben.

Schritte

1. Überprüfen Sie, ob sich die Management-LIF und Cluster-Management-LIFs bereits auf dem gewünschten Port befinden:

   ```
   network interface show -service-policy default-management
   ```

   ```
   network interface show -service-policy default-intercluster
   ```

   Wenn sich die LIFs auf den gewünschten Ports befinden, können Sie die restlichen Schritte dieser Aufgabe überspringen und mit der nächsten Aufgabe fortfahren.

2. Ändern Sie für jeden Node, Cluster-Management oder Intercluster-LIFs, die sich nicht am gewünschten Port befinden, den Home Port einer der LIFs auf diesem Port in einen anderen Port.

   a. Umwidmung des gewünschten Ports durch Verschieben jeder auf dem gewünschten Port gehosteten LIFs zu einem anderen Port:

      ```
      vserver config override -command "network interface modify -lif lifname
      -vserver vservername -home-port new-datahomeport"
      ```

   b. Zurücksetzen der geänderten LIFs auf ihren neuen Home-Port:

      ```
      vserver config override -command "network interface revert -lif lifname
      -vserver _vservername"
      ```

   c. Wenn sich der gewünschte Port nicht im richtigen IPspace und Broadcast-Domäne befindet, entfernen Sie den Port aus dem aktuellen IPspace und Broadcast-Domain:

      ```
      network port broadcast-domain remove-ports -ipspace current-ipspace
      -broadcast-domain current-broadcast-domain -ports controller-name:current-
      port
      ```

   d. Verschieben Sie den gewünschten Port in den richtigen IPspace und Broadcast Domain:

      ```
      network port broadcast-domain add-ports -ipspace new-ipspace -broadcast
      -domain new-broadcast-domain -ports controller-name:new-port
      ```

   e. Vergewissern Sie sich, dass sich die Portrolle geändert hat:

      ```
      network port show
      ```

   f. Wiederholen Sie diese Teilschritte für jeden Port.

3. Verschieben Sie Node, Cluster-Management-LIFs und Intercluster-LIF zum gewünschten Port:

   a. Ändern Sie den Home-Port des LIF:

      ```
      network interface modify -vserver vserver -lif node_mgmt -home-port port
      -home-node homenode
      ```

b. Zurücksetzen des LIF auf seinen neuen Home Port:

```
network interface revert -lif node_mgmt -vserver vservername
```

c. Ändern Sie den Home-Port der Cluster-Management-LIF:

```
network interface modify -vserver vserver -lif cluster-mgmt-LIF-name -home
-port port -home-node homenode
```

d. Zurücksetzen der Cluster-Management-LIF auf seinen neuen Home-Port:

```
network interface revert -lif cluster-mgmt-LIF-name -vserver vservername
```

e. Ändern Sie den Home-Port des Intercluster LIF:

```
network interface modify -vserver vserver -lif intercluster-lif-name -home
-node nodename -home-port port
```

f. Zurücksetzen der Intercluster-LIF auf seinen neuen Home-Port:

```
network interface revert -lif intercluster-lif-name -vserver vservername
```

Node_A_2-IP und Node_B_2-IP werden heraufgebracht

Sie müssen den neuen MetroCluster IP Node an jedem Standort erzeugen und konfigurieren, sodass an jedem Standort ein HA-Paar erstellt wird.

Node_A_2-IP und Node_B_2-IP werden heraufgebracht

Sie müssen die neuen Controller-Module nacheinander mit der richtigen Option im Startmenü booten.

Über diese Aufgabe

In diesen Schritten booten Sie die beiden brandneuen Nodes und erweiterten die bislang eine Konfiguration mit zwei Nodes in eine Konfiguration mit vier Nodes.

Auf den folgenden Knoten werden diese Schritte durchgeführt:

- Node_A_2-IP
- Node_B_2-IP

Schritte

1. Starten Sie die neuen Nodes mithilfe der Boot-Option „`9c`“.

```
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)? 9c
```

Der Node initialisiert und bootet den Node-Setup-Assistenten, ähnlich wie folgt.

```
Welcome to node setup
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.
Any changes you made before quitting will be saved.
To accept a default or omit a question, do not enter a value. .
.
.
```

Wenn die Option „`9c`“ nicht erfolgreich ist, führen Sie die folgenden Schritte aus, um möglichen Datenverlust zu vermeiden:

- Versuchen Sie nicht, Option 9a auszuführen.
- Trennen Sie physisch die vorhandenen Shelfs, die Daten enthalten, von der ursprünglichen MetroCluster FC-Konfiguration (Shelf_A_1, Shelf_A_2, Shelf_B_1, Shelf_B_2).
- Wenden Sie sich an den technischen Support, und verweisen Sie auf den KB-Artikel "Übergang von MetroCluster FC zu IP – Option 9c schlägt fehl".

  "NetApp Support"

2. Aktivieren Sie das AutoSupport-Tool, indem Sie den Anweisungen des Assistenten folgen.
3. Befolgen Sie die Aufforderungen zur Konfiguration der Node-Managementoberfläche.

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Vergewissern Sie sich, dass der Storage Failover-Modus auf HA eingestellt ist:

   `storage failover show -fields mode`

   Wenn der Modus keine HA ist, setzen Sie ihn ein:

   `storage failover modify -mode ha -node localhost`

   Sie müssen dann den Node neu booten, damit die Änderung wirksam wird.

5. Liste der Ports im Cluster:

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

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

6. Beenden Sie den Knoten-Setup-Assistenten:

```
exit
```

7. Loggen Sie sich unter Verwendung des Admin-Benutzernamens beim Administratorkonto ein.
8. Schließen Sie den vorhandenen Cluster mit dem Cluster-Setup-Assistenten an.

```
:> cluster setup
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and "exit"
or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

9. Nachdem Sie den Cluster Setup-Assistenten abgeschlossen und den Vorgang beendet haben, vergewissern Sie sich, dass das Cluster aktiv ist und der Node sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

10. Automatische Zuordnung der Festplatte deaktivieren:

```
storage disk option modify -autoassign off -node node_A_2-IP
```

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

Sie verwenden…	Befehl
• Onboard-Verschlüsselungsmanagement*	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Schlüsselmanagement	`security key-manager key query -node` *`node-name`* Weitere Informationen finden Sie unter "Wiederherstellen der externen Schlüssel für das Verschlüsselungsmanagement".

12. Wiederholen Sie die oben genannten Schritte auf dem zweiten neuen Controller-Modul (Node_B_2-IP).

MTU-Einstellungen werden überprüft

Überprüfen Sie, ob die MTU-Einstellungen für die Ports und die Broadcast-Domäne korrekt eingestellt sind, und nehmen Sie Änderungen vor.

Schritte

1. Überprüfen Sie die in der Cluster Broadcast-Domäne verwendete MTU-Größe:

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

2. Bei Bedarf die MTU-Größe aktualisieren:

```
network port broadcast-domain modify -broadcast-domain bcast-domain-name -mtu
mtu-size
```

Konfigurieren von Intercluster-LIFs

Konfigurieren Sie die für Cluster-Peering erforderlichen Intercluster LIFs.

Diese Aufgabe muss an beiden neuen Knoten Node_A_2-IP und Node_B_2-IP ausgeführt werden.

Schritt

1. Konfigurieren Sie die Intercluster LIFs. Siehe "Konfigurieren von Intercluster-LIFs"

Cluster-Peering wird überprüft

Vergewissern Sie sich, dass Cluster_A und Cluster_B Peering durchgeführt und Nodes auf jedem Cluster miteinander kommunizieren können.

Schritte

1. Überprüfen Sie die Cluster-Peering-Beziehung:

   ```
   cluster peer health show
   ```

   ```
   cluster01::> cluster peer health show
   Node       cluster-Name                Node-Name
                Ping-Status               RDB-Health Cluster-Health  Avail…
   ---------- --------------------------- ---------  ---------------
   --------
   node_A_1-IP
              cluster_B                   node_B_1-IP
                Data: interface_reachable
                ICMP: interface_reachable true       true            true
                                          node_B_2-IP
                Data: interface_reachable
                ICMP: interface_reachable true       true            true
   node_A_2-IP
              cluster_B                   node_B_1-IP
                Data: interface_reachable
                ICMP: interface_reachable true       true            true
                                          node_B_2-IP
                Data: interface_reachable
                ICMP: interface_reachable true       true            true
   ```

2. Ping, um zu überprüfen, ob die Peer-Adressen erreichbar sind:

   ```
   cluster peer ping -originating-node local-node -destination-cluster remote-
   cluster-name
   ```

Konfiguration der neuen Nodes und Abschluss des Übergangs

Beim Hinzufügen der neuen Nodes müssen Sie die Umstiegschritte abschließen und die MetroCluster IP Nodes konfigurieren.

Konfigurieren der MetroCluster IP-Knoten und Deaktivieren des Übergangs

Sie müssen die MetroCluster IP-Verbindungen implementieren, die MetroCluster-Konfiguration aktualisieren und den Übergangsmodus deaktivieren.

Schritte

1. Geben Sie die folgenden Befehle von Controller Node_A_1-IP aus, um die neuen Nodes einer DR-Gruppe zu bilden:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   <peer_cluster_name> -local-node <local_controller_name> -remote-node
   <remote_controller_name>

   metrocluster configuration-settings dr-group show
   ```

2. MetroCluster-IP-Schnittstellen erstellen (Node_A_1-IP, Node_A_2-IP, Node_B_1-IP, Node_B_2-IP) — pro Controller müssen zwei Schnittstellen erstellt werden; insgesamt acht Schnittstellen:

> Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <controller_name> -home-port <port_name> -address
<ip_address> -netmask <netmask_address> -vlan-id <vlan_id>

metrocluster configuration-settings interface show
```

Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

Falls unterstützt, können Sie auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben. Verwenden Sie dazu den `-vlan-id` Parameter im `metrocluster configuration-settings interface create` Befehl.

Die folgenden Plattformen unterstützen **Not** den `-vlan-id` Parameter:

- FAS8200 UND AFF A300
- AFF A320
- FAS9000 und AFF A700
- AFF C800, ASA C800, AFF A800 und ASA A800

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

  Die Standard- und gültigen VLAN-Zuweisungen hängen davon ab, ob die Plattform den folgenden Parameter unterstützt `-vlan-id`:

Plattformen, die <code>-vlan-</code> unterstützen

Standard-VLAN:

- Wenn der `-vlan-id` Parameter nicht angegeben wird, werden die Schnittstellen mit VLAN 10 für die „A“-Ports und VLAN 20 für die „B“-Ports erstellt.
- Das angegebene VLAN muss mit dem im RCF ausgewählten VLAN übereinstimmen.

Gültige VLAN-Bereiche:

- Standard-VLAN 10 und 20
- VLANs 101 und höher (zwischen 101 und 4095)

Plattformen, die <code>-vlan-</code> nicht unterstützen

Standard-VLAN:

- Keine Angabe. Für die Schnittstelle muss kein VLAN auf der MetroCluster-Schnittstelle angegeben werden. Der Switch-Port definiert das verwendete VLAN.

Gültige VLAN-Bereiche:

- Alle VLANs werden beim Generieren der RCF nicht explizit ausgeschlossen. Die RCF warnt Sie, wenn das VLAN ungültig ist.

3. Führen Sie den MetroCluster Connect-Vorgang über den Controller Node_A_1-IP durch, um eine Verbindung zu den MetroCluster-Standorten herzustellen. Dieser Vorgang kann einige Minuten dauern:

   ```
   metrocluster configuration-settings connection connect
   ```

4. Stellen Sie sicher, dass die Remote-Cluster-Laufwerke von jedem Controller über die iSCSI-Verbindungen sichtbar sind:

   ```
   disk show
   ```

   Sie sollten die Remote-Festplatten sehen, die zu den anderen Knoten in der Konfiguration gehören.

5. Root-Aggregat für Node_A_1-IP und Node_B_1-IP spiegeln:

   ```
   aggregate mirror -aggregate root-aggr
   ```

6. Weisen Sie Festplatten für Node_A_2-IP und Node_B_2-IP zu.

   Pool 1-Festplattenzuordnungen, die bereits für Node_A_1-IP und Node_B_1-IP vorgenommen wurden, wenn der Befehl Boot_after_mcc_trantion im Startmenü ausgegeben wurde.

   a. Geben Sie die folgenden Befehle an Node_A_2-IP ein:

      ```
      disk assign disk1disk2disk3 … diskn -sysid node_B_2-IP-controller-sysid
      -pool 1 -force
      ```

   b. Geben Sie die folgenden Befehle an Node_B_2-IP ein:

      ```
      disk assign disk1disk2disk3 … diskn -sysid node_A_2-IP-controller-sysid
      ```

```
-pool 1 -force
```

7. Bestätigen Sie, dass das Eigentumsrecht für die Remote-Festplatten aktualisiert wurde:

```
disk show
```

8. Aktualisieren Sie bei Bedarf die Eigentümerinformationen mit den folgenden Befehlen:
   a. Wechseln Sie zum erweiterten Berechtigungsmodus, und geben Sie y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

      ```
      set priv advanced
      ```

   b. Aktualisierung der Festplatteneigentümer:

      ```
      disk refresh-ownership controller-name
      ```

   c. Zurück zum Admin-Modus:

      ```
      set priv admin
      ```

9. Root-Aggregate für Node_A_2-IP und Node_B_2-IP spiegeln:

```
aggregate mirror -aggregate root-aggr
```

10. Überprüfen Sie, ob die erneute Synchronisierung des Aggregats für Root- und Datenaggregate abgeschlossen wurde:

```
aggr show``aggr plex show
```

    Die Resynchronisierung kann einige Zeit in Anspruch nehmen, muss aber abgeschlossen sein, bevor Sie mit den folgenden Schritten fortfahren.

11. Aktualisieren Sie die MetroCluster Konfiguration, um die neuen Nodes einzubinden:
    a. Wechseln Sie zum erweiterten Berechtigungsmodus, und geben Sie y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

       ```
       set priv advanced
       ```

    b. Aktualisieren Sie die Konfiguration:

Wenn Sie konfiguriert haben…	Geben Sie diesen Befehl aus…
Ein einzelnes Aggregat pro Cluster:	`metrocluster configure -refresh true -allow-with-one-aggregate true`
Mehr als ein einzelnes Aggregat pro Cluster	`metrocluster configure -refresh true`

    c. Zurück zum Admin-Modus:

       ```
       set priv admin
       ```

12. Deaktivieren des MetroCluster-Übergangsmodus:

a. Rufen Sie den erweiterten Berechtigungsmodus auf, und geben Sie „y“ ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set priv advanced
```

b. Übergangsmodus deaktivieren:

```
metrocluster transition disable
```

c. Zurück zum Admin-Modus:

```
set priv admin
```

Einrichten von Daten-LIFs auf den neuen Nodes

Sie müssen Daten-LIFs auf den neuen Nodes konfigurieren, Node_A_2-IP und Node_B_2-IP.

Sie müssen neue, auf neuen Controllern verfügbare Ports einer Broadcast-Domäne hinzufügen, wenn diese nicht bereits einem zugewiesen ist. Erstellen Sie bei Bedarf VLANs oder Schnittstellengruppen auf den neuen Ports. Siehe "Netzwerkmanagement"

1. Identifizieren der aktuellen Port-Nutzung und der Broadcast-Domänen:

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

2. Fügen Sie bei Bedarf Ports zu Broadcast-Domänen und VLANs hinzu.

   a. IP-Bereiche anzeigen:

   ```
   network ipspace show
   ```

   b. Erstellen Sie IP-Leerzeichen und weisen Sie Datenports nach Bedarf zu.

   "Konfigurieren von IPspaces (nur Cluster-Administratoren)"

   c. Broadcast-Domänen anzeigen:

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

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

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

   e. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

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

   "Erstellen eines VLANs"

   "Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

3. Vergewissern Sie sich, dass die LIFs bei Bedarf auf dem entsprechenden Node und den entsprechenden Ports auf den MetroCluster IP Nodes (einschließlich SVM mit -mc vServer) gehostet werden.

Siehe die in erfassten Informationen "Erstellen der Netzwerkkonfiguration".

a. Überprüfen Sie den Startport der LIFs:

```
network interface show -field home-port
```

b. Gegebenenfalls ändern Sie die LIF-Konfiguration:

```
vserver config override -command "network interface modify -vserver
<svm_name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>
```

c. Zurücksetzen der LIFs auf ihre Home-Ports:

```
network interface revert * -vserver <svm_name>
```

Erweitern der SVMs

Aufgrund der Änderungen, wenn die LIF-Konfiguration durchgeführt wird, müssen Sie die SVMs auf den neuen Nodes neu starten.

Schritte

1. Den Status der SVMs überprüfen:

```
metrocluster vserver show
```

2. Starten Sie die SVMs auf Cluster_A neu, die kein „`-mc`“ Suffix haben:

```
vserver start -vserver <svm_name> -force true
```

3. Wiederholen Sie die vorherigen Schritte im Partner-Cluster.
4. Prüfen Sie, ob sich alle SVMs in einem ordnungsgemäßen Zustand befinden:

```
metrocluster vserver show
```

5. Vergewissern Sie sich, dass alle Daten-LIFs online sind:

```
network interface show
```

Verschieben eines System-Volumes zu den neuen Nodes

Zur Verbesserung der Ausfallsicherheit sollte ein System-Volume von Controller Node_A_1-IP zu Controller Node_A_2-IP und auch von Node_B_1-IP auf Node_B_2-IP verschoben werden. Sie müssen ein gespiegeltes Aggregat auf dem Ziel-Node für das System-Volume erstellen.

Über diese Aufgabe

Systemvolumes haben das Namensformular „`MDV_CRS_*_A`“ oder „`MDV_CRS_*_B.`“ Die Bezeichnungen „`_A`“ und „`_B`“ stehen in keinem Zusammenhang mit den in diesem Abschnitt verwendeten Site_A- und Site_B-Referenzen; z. B. ist MDV_CRS_*_A nicht mit Site_A verknüpft

Schritte

1. Weisen Sie je nach Bedarf mindestens drei Pool-0- und drei Pool-1-Laufwerke für Controller Node_A_2-IP

und Node_B_2-IP zu.

2. Aktivieren der automatischen Zuweisung der Festplatte
3. Verschieben Sie das _B-Systemvolume von Node_A_1-IP auf Node_A_2-IP, indem Sie die folgenden Schritte von Site_A ausführen

   a. Erstellen eines gespiegelten Aggregats auf Controller Node_A_2-IP, um das System-Volume festzuhalten:

      ```
      aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node node_A_2-IP
      ```

      ```
      aggr show
      ```

      Das gespiegelte Aggregat erfordert fünf Pool 0 und fünf Pool 1 Ersatzfestplatten des Controllers Node_A_2-IP.

      Die erweiterte Option „`-Force-small-Aggregate true`“ kann verwendet werden, um die Festplattenverwendung auf 3 Pool-0- und 3 Pool-1-Festplatten zu begrenzen, wenn die Datenträger knapp sind.

   b. Liste der mit der Administrator-SVM verknüpften System-Volumes:

      ```
      vserver show
      ```

      ```
      volume show -vserver <admin_svm_name>
      ```

   Sie sollten Volumes identifizieren, die von Site_A-Aggregaten enthalten sind Außerdem werden die Site_B-System-Volumes angezeigt.

4. Verschieben Sie das MDV_CRS_*_B-Systemvolume für Site_A in das auf Controller Node_A_2-IP erstellte gespiegelte Aggregat

   a. Prüfen Sie auf mögliche Zielaggregate:

      ```
      volume move target-aggr show -vserver <admin_svm_name> -volume MDV_CRS_*_B
      ```

      Das neu erstellte Aggregat auf Node_A_2-IP sollte aufgelistet werden.

   b. Verschieben Sie das Volume in das neu erstellte Aggregat der Node_A_2-IP:

      ```
      set advanced
      ```

      ```
      volume move start -vserver <admin_svm_name> -volume MDV_CRS_*_B -destination -aggregate new_node_A_2-IP_aggr -cutover-window 40
      ```

   c. Status für den Vorgang „Verschieben“ überprüfen:

      ```
      volume move show -vserver <admin_svm_name> -volume MDV_CRS_*_B
      ```

   d. Überprüfen Sie nach Abschluss des Move-Vorgangs, ob das MDV_CRS_*_B-System vom neuen Aggregat auf Node_A_2-IP enthalten ist:

      ```
      set admin
      ```

```
volume show -vserver <admin_svm_name>
```

5. Wiederholen Sie die oben genannten Schritte auf Site_B (Node_B_1-IP und Node_B_2-IP).

Stellt den normalen Betrieb des Systems wieder her

Sie müssen die abschließenden Konfigurationsschritte durchführen und die MetroCluster-Konfiguration in den normalen Betrieb bringen.

Überprüfung des MetroCluster-Betriebs und Zuweisung von Laufwerken nach dem Umstieg

Sie müssen überprüfen, ob die MetroCluster ordnungsgemäß funktioniert und dem zweiten Paar neuer Knoten Laufwerke zuweisen (Node_A_2-IP und Node_B_2-IP).

1. Vergewissern Sie sich, dass der MetroCluster-Konfigurationstyp IP-Fabric ist: `metrocluster show`
2. Führen Sie eine MetroCluster-Prüfung durch.
   a. Geben Sie den folgenden Befehl ein: `metrocluster check run`
   b. Ergebnisse der MetroCluster-Prüfung anzeigen: `metrocluster check show`
3. Vergewissern Sie sich, dass die DR-Gruppe mit den MetroCluster IP Nodes konfiguriert ist: `metrocluster node show`
4. Zusätzliche Datenaggregate können je nach Bedarf für Controller Node_A_2-IP und Node_B_2-IP an jedem Standort erstellt und gespiegelt werden.

Installieren von Lizenzen für das neue Controller-Modul

Lizenzen für das neue Controller-Modul müssen für alle ONTAP Services hinzugefügt werden, die Standard-Lizenzen (mit Nodes gesperrt) erfordern. Bei Standardlizenzen muss jeder Node im Cluster über seinen eigenen Schlüssel für die Funktion verfügen.

Ausführliche Informationen zur Lizenzierung finden Sie in der Knowledge Base-Artikel 3013749: Übersicht über die Data ONTAP 8.2 Lizenzierung und Referenzen auf der NetApp Support Site und *System Administration Reference*.

1. Falls erforderlich, beziehen Sie Lizenzschlüssel für den neuen Node auf der NetApp Support Site im Abschnitt „My Support“ unter „Software-Lizenzen“.

   Weitere Informationen zum Austausch von Lizenzen finden Sie im Knowledge Base-Artikel "Verfahren zum Austausch der Hauptplatine zur Aktualisierung der Lizenzierung auf einem All Flash FAS/FAS System"

2. Geben Sie den folgenden Befehl ein, um jeden Lizenzschlüssel zu installieren: `system license add -license-code license_key`

   Der Lizenzschlüssel ist 28 Ziffern lang.

   Wiederholen Sie diesen Schritt für jede erforderliche Standard-Lizenz (Node-locked).

Die Konfiguration der Nodes wird abgeschlossen

Vor dem Abschluss der Verfahren können verschiedene Konfigurationsschritte durchgeführt werden. Einige dieser Schritte sind optional.

1. Konfigurieren Sie den Service Processor: `system service-processor network modify`
2. AutoSupport auf den neuen Nodes einrichten: `system node autosupport modify`
3. Controller können optional im Rahmen der Transition umbenannt werden. Der folgende Befehl wird zum Umbenennen eines Controllers verwendet: `system node rename -node <old-name> -newname <new-name>`

   Die Umbenennung kann einige Minuten in Anspruch nehmen. Vergewissern Sie sich, dass alle Namensänderungen an jeden Knoten übertragen wurden, bevor Sie mit anderen Schritten mit dem Befehl „System show -fields Node“ fortfahren.

4. Konfigurieren Sie einen Überwachungsdienst nach Bedarf.

   "Überlegungen für Mediator"

   "Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung"

   "Installation und Konfiguration von Tiebreaker Software"

Senden einer benutzerdefinierten AutoSupport Meldung nach der Wartung

Nach Abschluss des Übergangs sollten Sie eine AutoSupport-Nachricht mit dem Ende der Wartung senden, damit die automatische Case-Erstellung fortgesetzt werden kann.

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Unterbrechungsfreier Übergang von MetroCluster FC auf MetroCluster IP beim Ausmustern von Storage Shelves (ONTAP 9.8 und höher)

Ab ONTAP 9.8 ist es möglich, eine MetroCluster FC-Konfiguration mit zwei Nodes unterbrechungsfrei auf eine MetroCluster IP-Konfiguration mit vier Nodes zu verschieben und die vorhandenen Storage Shelfs außer Betrieb zu nehmen. Verfahren umfasst Schritte zum Verschieben der Daten von den vorhandenen Festplatten-Shelfs zur neuen Konfiguration und anschließend zum Ausmustern der alten Shelfs.

- Diese Vorgehensweise wird verwendet, wenn Sie die vorhandenen Storage-Shelfs ausmustern und alle Daten auf die neuen Shelfs in der MetroCluster IP-Konfiguration verschieben möchten.
- Die bestehenden Storage Shelf-Modelle müssen von den neuen MetroCluster IP Nodes unterstützt werden.
- Dieses Verfahren wird auf Systemen mit ONTAP 9.8 und höher unterstützt.
- Dieser Vorgang ist störend.
- Dieses Verfahren gilt nur für eine MetroCluster FC-Konfiguration mit zwei Nodes.

Wenn Sie über eine MetroCluster-FC-Konfiguration mit vier Nodes verfügen, finden Sie Informationen unter "Auswahl des Migrationsverfahrens".

- Sie müssen alle Anforderungen erfüllen und alle Schritte des Verfahrens befolgen.

Aktivieren Sie die Konsolenprotokollierung

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Anforderungen für den Umstieg beim Ausmustern alter Shelfs

Bevor Sie mit dem Umstieg beginnen, müssen Sie sicherstellen, dass die vorhandene MetroCluster FC-Konfiguration die Anforderungen erfüllt.

- Es muss eine Fabric-Attached- oder Stretch-MetroCluster-Konfiguration mit zwei Nodes und auf allen Nodes ONTAP 9.8 oder höher ausgeführt werden.

  Die neuen MetroCluster IP Controller-Module sollten dieselbe Version von ONTAP 9.8 ausführen.

- Die bestehenden und neuen Plattformen müssen eine unterstützte Kombination für den Umstieg sein.

  "Unterstützte Plattformen für unterbrechungsfreien Übergang"

- Er muss alle Anforderungen und Verkabelung erfüllen, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

  "Installation und Konfiguration von Fabric-Attached MetroCluster"

Die neue Konfiguration muss auch die folgenden Anforderungen erfüllen:

- Die neuen MetroCluster IP Plattformmodelle müssen alte Storage Shelf-Modelle unterstützen.

  "NetApp Hardware Universe"

- Abhängig von den in den vorhandenen Shelves verfügbaren Spare-Festplatten müssen zusätzliche Festplatten hinzugefügt werden.

  Dafür könnten zusätzliche Festplatten-Shelfs erforderlich sein.

  Sie benötigen weitere 14 bis 18 Laufwerke für jeden Controller:

  - Drei Pool-Laufwerke: 0

    - Drei Pool-1-Laufwerke
    - Zwei Ersatzlaufwerke
    - Sechs bis zehn Laufwerke für das System-Volume
- Sie müssen sicherstellen, dass die Konfiguration, einschließlich der neuen Nodes, die Plattformlimits für die Konfiguration nicht überschreitet, einschließlich Laufwerksanzahl, Root-Aggregatgröße usw.

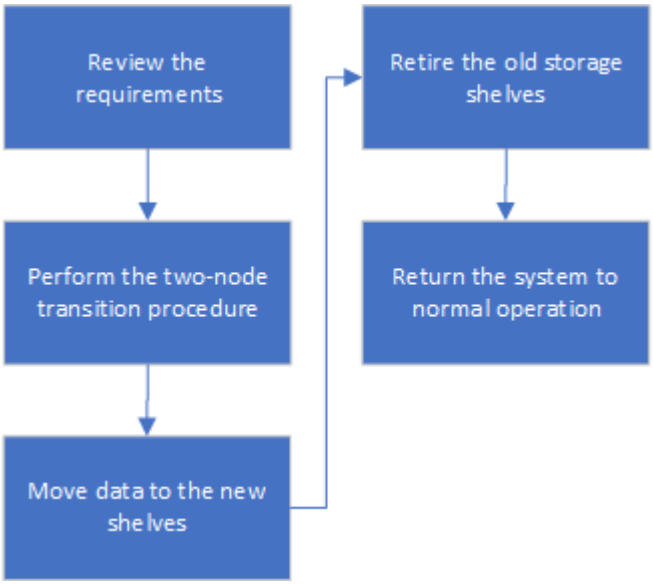
  Diese Informationen sind für jedes Plattformmodell bei verfügbar "NetApp Hardware Universe"

Sie müssen über Remote-Konsolenzugriff für alle sechs Nodes von einem MetroCluster Standort aus verfügen oder Reisen zwischen den Standorten planen, wie im Verfahren erforderlich.

Workflow für Unterbrechungen beim Verschieben von Daten und Aussortieren alter Storage Shelves

Um eine erfolgreiche Umstellung sicherzustellen, müssen Sie den spezifischen Workflow einhalten.

Planen Sie bei der Vorbereitung der Transition die Reise zwischen den Standorten ein. Beachten Sie, dass Sie nach dem Rack und verkabelt der Remote-Nodes seriellen Zugriff auf die Nodes benötigen. Der Service-Prozessor-Zugriff ist erst verfügbar, wenn die Nodes konfiguriert sind.



Umstellung der Konfiguration

Sie müssen das detaillierte Übergangsverfahren befolgen.

Über diese Aufgabe

In den folgenden Schritten werden Sie zu anderen Verfahren geleitet. Sie müssen die Schritte in jeder referenzierten Prozedur in der angegebenen Reihenfolge durchführen.

Schritte

1. Planen Sie die Port-Zuordnung mithilfe der Schritte in "Zuordnen von Ports von den MetroCluster FC-Nodes zu den MetroCluster IP-Nodes".
2. Bereiten Sie die MetroCluster IP-Controller mithilfe der Schritte in vor "Vorbereiten der MetroCluster IP-Controller".

3. Überprüfen Sie den Systemzustand der MetroCluster FC-Konfiguration.

   Führen Sie die Schritte unter aus "Überprüfen des Systemzustands der MetroCluster FC-Konfiguration".

4. Erfassen von Informationen aus der MetroCluster FC-Konfiguration

   Führen Sie die Schritte unter aus "Sammeln von Informationen aus den vorhandenen Controller-Modulen vor dem Umstieg".

5. Gegebenenfalls das Tiebreaker Monitoring entfernen.

   Führen Sie die Schritte unter aus "Entfernen der vorhandenen Konfiguration über den Tiebreaker oder eine andere Monitoring-Software".

6. Bereiten Sie die vorhandenen MetroCluster FC-Nodes vor und entfernen Sie sie.

   Führen Sie die Schritte unter aus "Umstellung der MetroCluster FC Nodes".

7. Verbinden Sie die neuen MetroCluster IP-Knoten.

   Führen Sie die Schritte unter aus "Anschließen der MetroCluster IP-Controller-Module".

8. Konfiguration der neuen MetroCluster IP-Knoten und vollständiger Übergang.

   Führen Sie die Schritte unter aus "Konfiguration der neuen Nodes und Abschluss des Übergangs".

Migration der Root-Aggregate

Migrieren Sie nach Abschluss der Transition die bestehenden Stammaggregate von der MetroCluster FC-Konfiguration auf neue Shelfs in der MetroCluster IP-Konfiguration.

Über diese Aufgabe

Mit dieser Aufgabe werden die Root-Aggregate für Node_A_1-FC und Node_B_1-FC auf Festplatten-Shelfs verschoben, die sich im Besitz der neuen MetroCluster IP-Controller befinden:

Schritte

1. Weisen Sie dem Controller, der das Root migriert hat, Pool 0-Festplatten im neuen lokalen Storage Shelf zu (z. B. wenn das Root von Node_A_1-FC migriert wird, weisen Sie Pool 0-Festplatten im neuen Shelf Node_A_1-IP zu).

   Beachten Sie, dass die Migration *entfernt und die Root-Spiegelung* nicht neu erstellt. Pool 1-Festplatten müssen daher erst zugewiesen werden, wenn Sie den Migrationsbefehl starten

2. Legen Sie den Berechtigungsmodus auf erweitert fest:

   ```
   set priv advanced
   ```

3. Migrieren des Root-Aggregats:

   ```
   system node migrate-root -node node-name -disklist disk-id1,disk-id2,diskn
   -raid-type raid-type
   ```

   - Der Node-Name ist der Node, auf den das Root-Aggregat migriert wird.

- Die Festplatten-id identifiziert die Pool-0-Festplatten auf dem neuen Shelf.
- Der RAID-Typ ist normalerweise der gleiche wie der RAID-Typ des bestehenden Root-Aggregats.
- Sie können den Befehl verwenden `job show -idjob-id-instance` Um den Migrationsstatus zu überprüfen, wobei Job-id der Wert ist, der beim Ausgeben des Befehls „Migration-Root“ angegeben wird.

  Wenn das Root-Aggregat für Node_A_1-FC beispielsweise aus drei Festplatten mit RAID_dp bestand, würde der folgende Befehl verwendet, um das Root zu einem neuen Shelf 11 zu migrieren:

```
system node migrate-root -node node_A_1-IP -disklist
3.11.0,3.11.1,3.11.2 -raid-type raid_dp
```

4. Warten Sie, bis der Migrationsvorgang abgeschlossen ist und der Node automatisch neu gebootet wird.
5. Weisen Sie Pool 1-Disks für das Root-Aggregat auf einem neuen Shelf zu, das direkt mit dem Remote-Cluster verbunden ist.
6. Spiegeln Sie das migrierte Root-Aggregat.
7. Warten Sie, bis das Root-Aggregat neu synchronisiert wurde.

   Mit dem Befehl „Storage Aggregate show“ können Sie den Synchronisierungsstatus der Aggregate überprüfen.

8. Wiederholen Sie diese Schritte für das andere Root-Aggregat.

Und die Daten-Aggregate migrieren

Erstellen Sie Datenaggregate auf den neuen Shelfs und verschieben Sie die Daten-Volumes von den alten Shelfs zu den Aggregaten auf den neuen Shelfs.

1. Verschieben Sie die Daten-Volumes zu Aggregaten auf den neuen Controllern, jeweils ein Volume.

   "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes"

Ausmustern von Shelfs, die von Node_A_1-FC und Node_A_2-FC verschoben wurden

Sie haben die alten Storage Shelfs aus der ursprünglichen MetroCluster FC-Konfiguration entfernt. Ursprünglich waren die Shelfs Node_A_1-FC und Node_A_2-FC im Besitz dieser Shelfs.

1. Ermitteln Sie die Aggregate auf den alten Shelfs auf Cluster_B, die gelöscht werden müssen.

   In diesem Beispiel werden die folgenden Datenaggregate vom MetroCluster FC Cluster_B gehostet und müssen gelöscht werden: aggr_Data_a1 und aggr_Data_a2.

   > Es müssen die Schritte ausgeführt werden, um die Datenaggregate auf den Shelfs zu identifizieren, offline und zu löschen. Das Beispiel gilt nur für ein Cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-IP
raid_dp,

mirrored,

normal
aggr0_node_A_2-IP
           349.0GB   16.83GB   95% online       1 node_A_2-IP
raid_dp,

mirrored,

normal
...
8 entries were displayed.

cluster_B::>
```

2. Überprüfen Sie, ob die Datenaggregate über MDV_aud-Volumes verfügen, und löschen Sie sie, bevor Sie die Aggregate löschen.

   Sie müssen die MDV_aud-Volumes löschen, da sie nicht verschoben werden können.

3. Nehmen Sie jedes Aggregat in den Offline-Modus und löschen Sie es anschließend:

   a. Versetzen Sie das Aggregat in den Offline-Modus:

      ```
      storage aggregate offline -aggregate aggregate-name
      ```

      Das folgende Beispiel zeigt, dass der aggregierte Node_B_1_aggr0 offline geschaltet wird:

      ```
      cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

      Aggregate offline successful on aggregate: node_B_1_aggr0
      ```

   b. Löschen Sie das Aggregat:

      ```
      storage aggregate delete -aggregate aggregate-name
      ```

      Sie können den Plex zerstören, wenn Sie dazu aufgefordert werden.

Das folgende Beispiel zeigt, dass der aggregierte Node_B_1_aggr0 gelöscht wird.

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. Nach dem Löschen aller Aggregate fahren Sie herunter, trennen die Shelfs und entfernen sie.
5. Wiederholen Sie die oben genannten Schritte, um das Cluster_A-Shelf außer Betrieb zu nehmen.

Übergang abschließen

Wenn die alten Controller-Module entfernt wurden, können Sie den Umstieg abschließen.

Schritt

1. Abschluss des Transitionsprozesses

   Führen Sie die Schritte unter aus "Stellt den normalen Betrieb des Systems wieder her".

Unterbrechungsfreie Transition, wenn vorhandene Shelfs nicht auf neuen Controllern unterstützt werden (ONTAP 9.8 und höher)

Ab ONTAP 9.8 können Sie eine MetroCluster FC-Konfiguration mit zwei Nodes unterbrechungsfrei verschieben und Daten von den vorhandenen Laufwerk-Shelfs verschieben, selbst wenn die vorhandenen Storage-Shelfs nicht von den neuen MetroCluster IP Nodes unterstützt werden.

- Dieses Verfahren sollte nur angewandt werden, wenn die vorhandenen Storage Shelf-Modelle nicht von den neuen MetroCluster IP-Plattformmodellen unterstützt werden.
- Dieses Verfahren wird auf Systemen mit ONTAP 9.8 und höher unterstützt.
- Dieser Vorgang ist störend.
- Dieses Verfahren gilt nur für eine MetroCluster FC-Konfiguration mit zwei Nodes.

  Wenn Sie über eine MetroCluster-FC-Konfiguration mit vier Nodes verfügen, finden Sie Informationen unter "Auswahl des Migrationsverfahrens".

- Sie müssen alle Anforderungen erfüllen und alle Schritte des Verfahrens befolgen.

Aktivieren Sie die Konsolenprotokollierung

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Anforderungen für den Umstieg, wenn Shelfs auf den neuen Nodes nicht unterstützt werden

Bevor Sie mit dem Umstieg beginnen, müssen Sie sicherstellen, dass die Konfiguration die Anforderungen erfüllt.

Bevor Sie beginnen

- Die vorhandene Konfiguration muss eine Fabric-Attached- oder Stretch-MetroCluster Konfiguration mit zwei Nodes und auf allen Nodes ONTAP 9.8 oder höher ausgeführt werden.

  Die neuen MetroCluster IP Controller-Module sollten dieselbe Version von ONTAP 9.8 ausführen.

- Die bestehenden und neuen Plattformen müssen eine unterstützte Kombination für den Umstieg sein.

  "Unterstützte Plattformen für unterbrechungsfreien Übergang"

- Es muss alle Anforderungen und Verkabelung erfüllen, wie in beschrieben "Installation und Konfiguration von Fabric-Attached MetroCluster".
- Neue mit den neuen Controllern bereitgestellte Storage-Shelfs (Node_A_1-IP, Node_A_2-IP, Node_B_1-IP und Node_B_2-IP) müssen von den alten Controllern (Node_A_1-FC und Node_B_1-FC) unterstützt werden.

  "NetApp Hardware Universe"

- Die alten Storage Shelves werden von den neuen MetroCluster IP Plattformmodellen * nicht unterstützt.

  "NetApp Hardware Universe"

- Abhängig von den in den vorhandenen Shelves verfügbaren Spare-Festplatten müssen zusätzliche Festplatten hinzugefügt werden.

  Dafür könnten zusätzliche Festplatten-Shelfs erforderlich sein.

  Sie benötigen weitere 14 bis 18 Laufwerke für jeden Controller:

  - Drei Pool0-Laufwerke
  - Drei Pool1-Laufwerke
  - Zwei Ersatzlaufwerke
  - Sechs bis zehn Laufwerke für das System-Volume
- Sie müssen sicherstellen, dass die Konfiguration, einschließlich der neuen Nodes, die Plattformlimits für die Konfiguration nicht überschreitet, einschließlich Laufwerksanzahl, Root-Aggregatgröße usw.

Diese Informationen sind für jedes Plattformmodell bei *NetApp Hardware Universe* verfügbar.

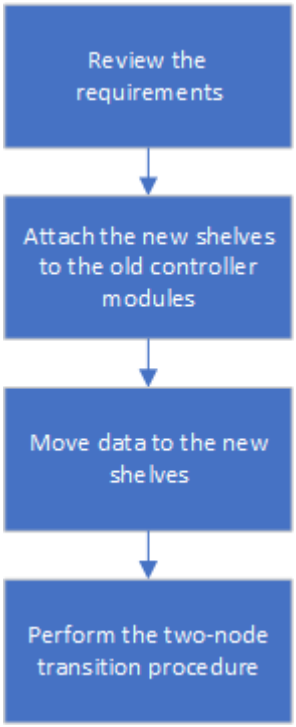
"NetApp Hardware Universe"

- Sie müssen über Remote-Konsolenzugriff für alle sechs Nodes von einem MetroCluster Standort aus verfügen oder Reisen zwischen den Standorten planen, wie im Verfahren erforderlich.

Workflow für Unterbrechungen beim Übergang, wenn Shelfs nicht von neuen Controllern unterstützt werden

Wenn die vorhandenen Shelf-Modelle von den neuen Plattformmodellen nicht unterstützt werden, müssen Sie die neuen Shelfs an die alte Konfiguration anbinden, die Daten in die neuen Shelfs verschieben und schließlich in die neue Konfiguration übergehen.

Planen Sie bei der Vorbereitung der Transition die Reise zwischen den Standorten ein. Beachten Sie, dass Sie nach dem Rack und verkabelt der Remote-Nodes seriellen Zugriff auf die Nodes benötigen. Der Service-Prozessor-Zugriff ist erst verfügbar, wenn die Nodes konfiguriert sind.



Vorbereiten der neuen Controller-Module

Sie müssen die Konfiguration und die Festplatteneigentümer für die neuen Controller-Module und die neuen Storage-Shelves löschen.

Schritte

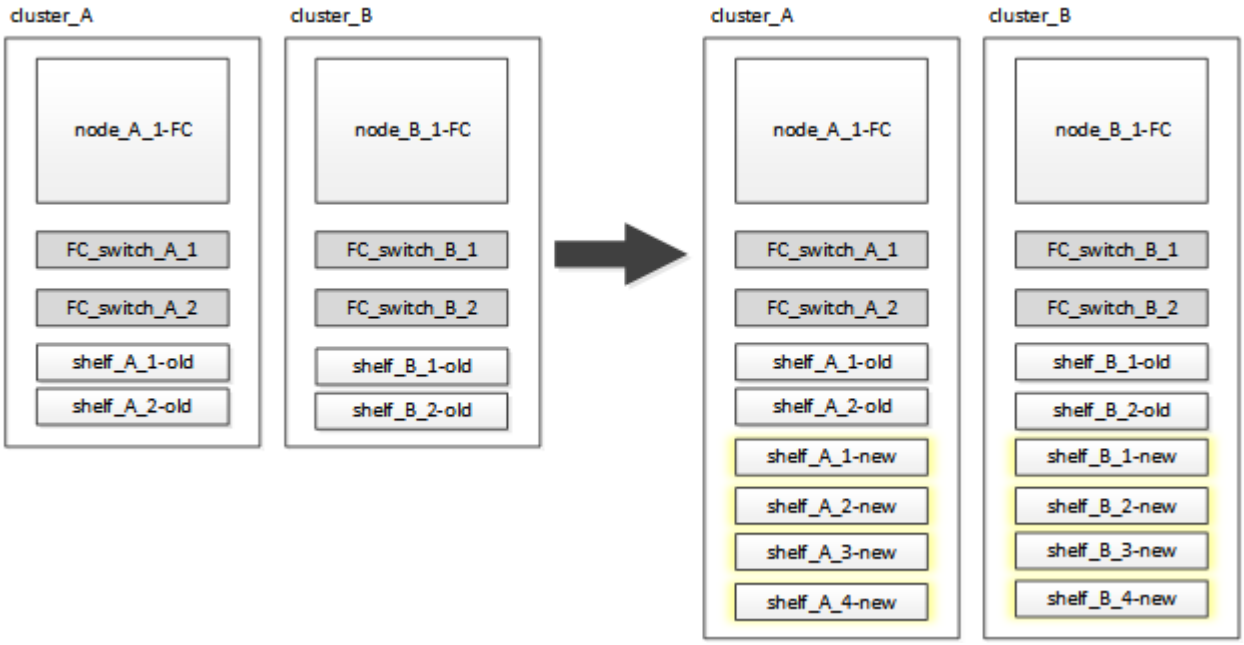
1. Führen Sie alle Schritte aus, die mit den neuen MetroCluster IP-Controller-Modulen verbunden sind "Vorbereiten der MetroCluster IP-Controller".
2. Trennen Sie die neuen Storage-Shelves von den neuen MetroCluster IP Controller-Modulen.

Anschließen der neuen Platten-Shelfs an die vorhandenen MetroCluster FC-Controller

Vor dem Wechsel zu einer MetroCluster IP-Konfiguration müssen Sie die neuen Festplatten-Shelfs an die vorhandenen Controller-Module anschließen.

Über diese Aufgabe

Die folgende Abbildung zeigt die neuen Shelves, die an die MetroCluster FC-Konfiguration angeschlossen sind.



Schritte

1. Deaktivieren der automatischen Zuordnung der Festplatte bei Node_A_1-FC und Node_A_2-FC:

   ```
   disk option modify -node node-name -autoassign off
   ```

   Dieser Befehl muss für jeden Node ausgestellt werden.

   Die automatische Zuweisung von Festplatten ist deaktiviert, um zu vermeiden, dass die Shelfs Node_A_1-FC und Node_B_1-FC hinzugefügt werden. Im Rahmen der Transition sind die Festplatten für die Knoten Node_A_1-IP und Node_B_2-IP erforderlich. Wenn die automatische Zuweisung zulässig ist, müssten die Festplattenbesitzer später entfernt werden, bevor Festplatten Node_A_1-IP und Node_B_2-IP zugewiesen werden konnten.

2. Verbinden Sie die neuen Shelfs ggf. mit den vorhandenen MetroCluster FC Nodes über FC-to-SAS-Bridges.

   Siehe Anforderungen und Verfahren in "Hot-adding von Speicher zu einer MetroCluster-FC-Konfiguration"

Migrieren Sie Root-Aggregate und verschieben Sie Daten in die neuen Platten-Shelves

Sie müssen die Root-Aggregate von den alten Laufwerk-Shelfs auf die neuen Festplatten-Shelfs verschieben, die von den MetroCluster IP-Nodes verwendet werden.

Über diese Aufgabe

Diese Aufgabe wird vor dem Übergang der vorhandenen Knoten durchgeführt (Node_A_1-FC und Node_B_1-FC).

Schritte

1. Durchführen einer ausgehandelten Umschaltung von Controller Node_B_1-FC:

   ```
   metrocluster switchover
   ```

2. Führen Sie die Heal-Aggregate aus und heilen Sie die Root-Schritte der Recovery von Node_B_1-FC:

   ```
   metrocluster heal -phase aggregates

   metrocluster heal -phase root-aggregates
   ```

3. Boot Controller Node_A_1-FC:

   ```
   boot_ontap
   ```

4. Weisen Sie die nicht im Besitz befindlichen Festplatten auf den neuen Shelfs den entsprechenden Pools für Controller Node_A_1-FC zu:

   a. Festplatten in den Shelfs identifizieren:

      ```
      disk show -shelf pool_0_shelf -fields container-type,diskpathnames

      disk show -shelf pool_1_shelf -fields container-type,diskpathnames
      ```

   b. Geben Sie den lokalen Modus ein, sodass die Befehle auf dem lokalen Knoten ausgeführt werden:

      ```
      run local
      ```

   c. Weisen Sie die Festplatten zu:

      ```
      disk assign disk1disk2disk3disk… -p 0

   disk assign disk4disk5disk6disk… -p 1
      ```

   a. Lokalen Modus beenden:

      ```
      exit
      ```

5. Erstellen Sie ein neues gespiegeltes Aggregat zum neuen Root-Aggregat für Controller Node_A_1-FC:

   a. Legen Sie den Berechtigungsmodus auf erweitert fest:

      ```
      set priv advanced
      ```

   b. Erstellen Sie das Aggregat:

      ```
      aggregate create -aggregate new_aggr -disklist disk1, disk2, disk3,… -mirror
      -disklist disk4disk5, disk6,… -raidtypesame-as-existing-root -force-small
      -aggregate true aggr show -aggregate new_aggr -fields percent-snapshot-space
      ```

Wenn der Prozentwert für Snapshot-Speicherplatz weniger als 5 Prozent beträgt, müssen Sie ihn auf einen Wert über 5 Prozent erhöhen:

```
aggr modify new_aggr -percent-snapshot-space 5
```

a. Setzen Sie den Berechtigungsebene-Modus zurück auf admin:

```
set priv admin
```

6. Vergewissern Sie sich, dass das neue Aggregat ordnungsgemäß erstellt wird:

```
node run -node local sysconfig -r
```

7. Erstellung von Backups der Konfiguration auf Node- und Cluster-Ebene:

> Wenn die Backups während des Switchover erstellt werden, erkennt das Cluster bei der Recovery den Switchover-Status. Sie müssen sicherstellen, dass die Sicherung und das Hochladen der Systemkonfiguration erfolgreich ist, da es ohne diese Sicherung nicht möglich ist, die MetroCluster-Konfiguration zwischen Clustern zu reformieren.

a. Erstellen Sie das Cluster-Backup:

```
system configuration backup create -node local -backup-type cluster -backup
-name cluster-backup-name
```

b. Überprüfen Sie die Erstellung von Cluster-Backups

```
job show -id job-idstatus
```

c. Erstellen Sie das Knoten-Backup:

```
system configuration backup create -node local -backup-type node -backup
-name node-backup-name
```

d. Prüfen Sie sowohl Cluster- als auch Node-Backups:

```
system configuration backup show
```

Sie können den Befehl wiederholen, bis in der Ausgabe beide Backups angezeigt werden.

8. Erstellung von Kopien der Backups

Die Backups müssen an einem separaten Speicherort gespeichert werden, da sie lokal beim Start des neuen Root-Volumes verloren gehen.

Sie können die Backups auf einen FTP- oder HTTP-Server hochladen oder die Backups mit kopieren `scp` Befehle.

Prozess	Schritte

Hochladen der Sicherung auf den FTP- oder HTTP-Server	a. Laden Sie das Cluster-Backup hoch:
	
	`system configuration backup upload -node local -backup` *`cluster-backup-name`* `-destination URL`
	
	b. Laden Sie das Knoten-Backup hoch:
	
	`system configuration backup upload -node local -backup` *`node-backup-name`* `-destination URL`

Kopieren Sie die Backups auf einen Remote-Server mit sicherer Kopie	Verwenden Sie auf dem Remoteserver die folgenden Scp-Befehle:
	
	a. Cluster-Backup kopieren:
	
	`scp diagnode-mgmt-FC:/mroot/etc/backups/config/cluster-backup-name.7z .`
	
	b. Kopieren des Node-Backups:
	
	`scp diag@node-mgmt-FC:/mroot/etc/backups/config/node-backup-name.7z .`

9. Stop Node_A_1-FC:

```
halt -node local -ignore-quorum-warnings true
```

10. Boot Node_A_1-FC in Wartungsmodus:

```
boot_ontap maint
```

11. Nehmen Sie im Wartungsmodus erforderliche Änderungen vor, um das Aggregat als Root einzustellen:

    a. Legen Sie die HA-Richtlinie auf cfo fest:

    ```
    aggr options new_aggr ha_policy cfo
    ```

    Beantworten Sie „`ja`“, wenn Sie dazu aufgefordert werden, fortzufahren.

```
Are you sure you want to proceed (y/n)?
```

    a. Legen Sie das neue Aggregat als Root fest:

    ```
    aggr options new_aggr root
    ```

    b. Anhalten der LOADER-Eingabeaufforderung:

    ```
    halt
    ```

12. Booten des Controllers und Sichern der Systemkonfiguration

Der Node startet im Wiederherstellungsmodus, wenn das neue Root-Volume erkannt wird

a. Booten des Controllers:

```
boot_ontap
```

b. Melden Sie sich an und sichern Sie die Konfiguration.

Wenn Sie sich anmelden, wird die folgende Warnung angezeigt:

```
Warning: The correct cluster system configuration backup must be
restored. If a backup
from another cluster or another system state is used then the root
volume will need to be
recreated and NGS engaged for recovery assistance.
```

a. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

b. Sichern Sie die Clusterkonfiguration auf einem Server:

```
system configuration backup download -node local -source URL of
server/cluster-backup-name.7z
```

c. Sichern Sie die Node-Konfiguration auf einem Server:

```
system configuration backup download -node local -source URL of server/node-
backup-name.7z
```

d. Zurück zum Admin-Modus:

```
set -privilege admin
```

13. Überprüfen Sie den Systemzustand des Clusters:

a. Geben Sie den folgenden Befehl ein:

```
cluster show
```

b. Legen Sie den Berechtigungsmodus auf erweitert fest:

```
set -privilege advanced
```

c. Überprüfen Sie die Cluster-Konfigurationsdetails:

```
cluster ring show
```

d. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

14. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.
    a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

       ```
       metrocluster show
       ```

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

       ```
       metrocluster node show
       ```

    c. Geben Sie den folgenden Befehl ein:

       ```
       metrocluster check run
       ```

    d. Ergebnisse der MetroCluster-Prüfung anzeigen:

       ```
       metrocluster check show
       ```

15. Führen Sie einen Switchback vom Controller Node_B_1-FC aus:

    ```
    metrocluster switchback
    ```

16. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
    a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

       ```
       metrocluster show
       ```

    b. Durchführen einer MetroCluster-Prüfung:

       ```
       metrocluster check run
       ```

    c. Ergebnisse der MetroCluster-Prüfung anzeigen:

       ```
       metrocluster check show
       ```

17. Fügen Sie das neue Root-Volume der Volume-Standortdatenbank hinzu.
    a. Legen Sie den Berechtigungsmodus auf erweitert fest:

       ```
       set -privilege advanced
       ```

    b. Fügen Sie das Volume dem Node hinzu:

       ```
       volume add-other-volumes –node node_A_1-FC
       ```

    c. Zurück zur Administratorberechtigungsebene:

       ```
       set -privilege admin
       ```

18. Überprüfen Sie, ob das Volumen nun sichtbar ist und mroot hat.
    a. Anzeigen der Aggregate:

       ```
       storage aggregate show
       ```

b. Überprüfen Sie, ob das Root-Volumen mroot hat:

```
storage aggregate show -fields has-mroot
```

c. Anzeigen der Volumes:

```
volume show
```

19. Erstellen Sie ein neues Sicherheitszertifikat, um den Zugriff auf System Manager erneut zu aktivieren:

```
security certificate create -common-name name -type server -size 2048
```

20. Wiederholen Sie die vorherigen Schritte, um die Aggregate auf Shelfs zu migrieren, die sich im Besitz von Node_A_1-FC befinden.
21. Führen Sie eine Bereinigung durch.

    Um das alte Root-Volume und das Root-Aggregat zu entfernen, müssen Sie sowohl auf Node_A_1-FC als auch auf Node_B_1-FC die folgenden Schritte durchführen.

    a. Löschen Sie das alte Root-Volumen:

```
run local

vol offline old_vol0

vol destroy old_vol0

exit

volume remove-other-volume -vserver node_name -volume old_vol0
```

    b. Löschen Sie das ursprüngliche Root-Aggregat:

```
aggr offline -aggregate old_aggr0_site

aggr delete -aggregate old_aggr0_site
```

22. Migrieren Sie die Daten-Volumes zu Aggregaten auf den neuen Controllern, jeweils ein Volume.

    Siehe "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes"

23. Mustern Sie die alten Shelves aus, indem Sie alle erforderlichen Schritte ausführen "Ausmustern von Shelfs, die von Node_A_1-FC und Node_A_2-FC verschoben wurden".

Umstellung der Konfiguration

Sie müssen das detaillierte Übergangsverfahren befolgen.

Über diese Aufgabe

In den folgenden Schritten werden Sie zu anderen Themen weitergeleitet. Sie müssen die Schritte in jedem Thema in der angegebenen Reihenfolge durchführen.

Schritte

1. Planen Sie die Port-Zuordnung.

   Führen Sie alle Schritte in aus "Zuordnen von Ports von den MetroCluster FC-Nodes zu den MetroCluster IP-Nodes".

2. Bereiten Sie die MetroCluster IP-Controller vor.

   Führen Sie alle Schritte in aus "Vorbereiten der MetroCluster IP-Controller".

3. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   Führen Sie alle Schritte in aus "Überprüfen des Systemzustands der MetroCluster FC-Konfiguration".

4. Bereiten Sie die vorhandenen MetroCluster FC-Nodes vor und entfernen Sie sie.

   Führen Sie alle Schritte in aus "Umstellung der MetroCluster FC Nodes".

5. Fügen Sie die neuen MetroCluster IP-Knoten hinzu.

   Führen Sie alle Schritte in aus "Anschließen der MetroCluster IP-Controller-Module".

6. Abschluss der Transition und Erstkonfiguration der neuen MetroCluster IP Nodes.

   Führen Sie alle Schritte in aus "Konfiguration der neuen Nodes und Abschluss des Übergangs".

Verschieben eines FC SAN-Workloads von MetroCluster FC- zu MetroCluster IP-Nodes

Für den unterbrechungsfreien Wechsel von MetroCluster FC zu IP Nodes müssen Sie FC SAN Host-Objekte unterbrechungsfrei von MetroCluster FC auf IP Nodes verschieben.

Verschieben Sie einen FC SAN-Workload von MetroCluster FC auf MetroCluster IP Nodes

Schritte

1. Neue FC-Schnittstellen (LIFS) an MetroCluster IP-Nodes einrichten:
   a. Ändern Sie bei MetroCluster IP-Nodes gegebenenfalls FC-Ports, die für die Client-Verbindung zu FC-Zielpersönlichkeit verwendet werden sollen.

      Hierfür ist möglicherweise ein Neustart der Nodes erforderlich.

   b. FC-LIFS/Schnittstellen auf IP-Nodes für alle SAN SVMs erstellen Optional können Sie überprüfen, ob die WWPNs von neu erstellten FC LIFs am FC SAN-Switch angemeldet sind
2. Aktualisieren Sie die SAN-Zoning-Konfiguration für neu hinzugefügte FC LIFs auf MetroCluster IP Nodes.

   Um die Verschiebung von Volumes zu vereinfachen, in denen LUNs aktiv Daten für FC SAN-Clients bereitstellen, sollten Sie die vorhandenen FC Switch-Zonen aktualisieren, damit FC SAN-Clients auf LUNs in MetroCluster IP-Nodes zugreifen können.

   a. Fügen Sie am FC SAN-Switch (Cisco oder Brocade) der Zone die WWPNs neu hinzugefügter FC SAN LIFs hinzu.

b. Aktualisieren, speichern und Übergeben der Änderungen am Zoning

c. Überprüfen Sie vom Client auf FC-Initiator-Anmeldungen zu den neuen SAN-LIFs auf den MetroCluster IP-Nodes: `sanlun lun show -p`

   Derzeit sollte der Client sehen und bei den FC-Schnittstellen sowohl auf den MetroCluster-FC- als auch auf den MetroCluster-IP-Nodes angemeldet sein. LUNs und Volumes werden weiterhin physisch auf den MetroCluster FC-Nodes gehostet.

   Da LUNs nur auf MetroCluster FC Node-Schnittstellen gemeldet werden, zeigt der Client nur Pfade über FC Nodes an. Dies kann in der Ausgabe des angezeigt werden `sanlun lun show -p` Und `multipath -ll -d` Befehle.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
-----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
-----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

3. Ändern Sie die Berichtsknoten, um die MetroCluster-IP-Knoten hinzuzufügen

   a. Liste der Reporting-Nodes für LUNs auf der SVM: `lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux`

      Als Nodes für die Berichterstellung werden lokale Nodes angezeigt, da sich LUNs physisch auf FC-Nodes A_1 und A_2 befinden.

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                          igroup         reporting-nodes
-------  --------------------------- ------------
-------------------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol1/lun_linux_3 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol2/lun_linux_4 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol3/lun_linux_7 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_8 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_9 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_12 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_13 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol7/lun_linux_14 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol8/lun_linux_17 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_18 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_19 igroup_linux  A_1,A_2
12 entries were displayed.
```

b. Fügen Sie Reporting-Nodes hinzu, um MetroCluster IP-Nodes einzubeziehen.

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes B_1,B_2 -igroup igroup_linux

12 entries were acted on.
```

c. Listen Sie die Reporting-Knoten auf, und überprüfen Sie die Anwesenheit der neuen Knoten:

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                           igroup          reporting-nodes
------- ---------------------------    ------------
-----------------------------------------------------------------------
----------

vsa_1   /vol/vsa_1_vol1/lun_linux_2   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol1/lun_linux_3   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol2/lun_linux_4   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol3/lun_linux_7   igroup_linux    A_1,A_2,B_1,B_2
...

12 entries were displayed.
```

d. Überprüfen Sie das `sg3-utils` Das Paket wird auf dem Linux-Host installiert. Dies vermeidet ein `rescan-scsi-bus.sh utility not found` Fehler beim erneuten Scannen des Linux-Hosts für die neu zugeordneten LUNs mithilfe des `rescan-scsi-bus` Befehl.

e. Scannen Sie den SCSI-Bus auf dem Host erneut, um die neu hinzugefügten Pfade zu erkennen: `/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

f. Anzeigen der neu hinzugefügten Pfade: `sanlun lun show -p`

   Jede LUN hat vier Pfade.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a0980383046465 13f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

g. Verschieben Sie auf den Controllern die Volumes, die LUNs enthalten, von MetroCluster FC zu den MetroCluster IP-Nodes.

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver    Volume    State    Move Phase   Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------   ----------------
----------------
vsa_1     vsa_1_vol1 healthy  initializing
 - -
```

h. Zeigen Sie auf dem FC SAN-Client die LUN-Informationen an: `sanlun lun show -p`

   Die FC-Schnittstellen auf den MetroCluster IP Nodes, in denen sich die LUN nun befindet, werden als primäre Pfade aktualisiert. Wenn der primäre Pfad nach der Volume-Verschiebung nicht aktualisiert wird, führen Sie /usr/bin/rescan-scsi-bus.sh -a aus oder warten Sie einfach, bis Multipath-Rescanning stattfindet.

   Der primäre Pfad im folgenden Beispiel ist die LIF auf dem MetroCluster IP Node.

```
[root@localhost ~]# sanlun lun show -p

                    ONTAP Path: vsa_1:/vol/vsa_1_vol1/lun_linux_2
                           LUN: 22
                      LUN Size: 2g
                       Product: cDOT
                   Host Device: 3600a098038302d324e5d50305063546e
              Multipath Policy: service-time 0
            Multipath Provider: Native
--------- ---------- ------- ------------
-----------------------------------------------
host      vserver
path      path       /dev/   host         vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------
-----------------------------------------------
up        primary    sddv    host6        fc_5
up        primary    sdjx    host7        fc_6
up        secondary  sdgv    host6        fc_8
up        secondary  sdkr    host7        fc_8
```

a. Wiederholen Sie die oben genannten Schritte für alle Volumes, LUNs und FC-Schnittstellen, die zu einem FC-SAN-Host gehören.

   Nach Abschluss dieser Fertigstellung sollten sich alle LUNs für eine bestimmte SVM und ein FC-SAN-Host auf MetroCluster IP-Nodes befinden.

4. Entfernen Sie die Knoten für die Berichterstellung und scannen Sie Pfade vom Client erneut.

   a. Entfernen Sie die Remote Reporting Nodes (die MetroCluster FC Nodes) für die linux LUNs: `lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igroup_linux -remote-nodes true`

      ```
      cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
      * -igroup igroup_linux -remote-nodes true
      12 entries were acted on.
      ```

   b. Überprüfen Sie die Reporting-Nodes für die LUNs: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
------- --------------------------- ------------
----------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol2/lun_linux_4 igroup_linux B_1,B_2
...

12 entries were displayed.
```

c. SCSI-Bus auf dem Client erneut scannen: `/usr/bin/rescan-scsi-bus.sh -r`

   Die Pfade aus den MetroCluster FC-Knoten werden entfernt:

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
...
```

a. Vergewissern Sie sich, dass vom Host nur Pfade von den MetroCluster IP-Nodes sichtbar sind: `sanlun lun show -p`

b. Entfernen Sie bei Bedarf iSCSI LIFs von den MetroCluster FC-Nodes.

   Dies sollte geschehen, wenn andere LUNs auf den Nodes anderen Clients zugeordnet sind.

Verschieben Sie Linux iSCSI-Hosts von MetroCluster FC zu MetroCluster IP-Knoten

Nach der Umstellung Ihrer MetroCluster Nodes von FC zu IP müssen Sie eventuell Ihre iSCSI-Host-Verbindungen zu den neuen Nodes verschieben.

Über diese Aufgabe

- IPv4-Schnittstellen werden beim Einrichten der neuen iSCSI-Verbindungen erstellt.
- Die Host-Befehle und Beispiele sind spezifisch für Linux-Betriebssysteme.
- Die MetroCluster FC-Nodes werden als alte Nodes bezeichnet und die MetroCluster IP-Nodes als neue Nodes bezeichnet.

Schritt 1: Einrichtung neuer iSCSI-Verbindungen

Um die iSCSI-Verbindungen zu verschieben, richten Sie neue iSCSI-Verbindungen zu den neuen Knoten ein.

Schritte

1. Erstellen Sie iSCSI-Schnittstellen auf den neuen Knoten, und prüfen Sie die Ping-Verbindung zwischen den iSCSI-Hosts und den neuen Schnittstellen auf den neuen Knoten.

   "Netzwerkschnittstellen erstellen"

   Alle iSCSI-Schnittstellen der SVM sollten vom iSCSI-Host erreichbar sein.

2. Identifizieren Sie auf dem iSCSI-Host die vorhandenen iSCSI-Verbindungen vom Host zum alten Knoten:

   ```
   iscsiadm -m session
   ```

   ```
   [root@scspr1789621001 ~]# iscsiadm -m session
   tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   ```

3. Überprüfen Sie auf dem neuen Node die Verbindungen vom neuen Node:

   ```
   iscsi session show -vserver <svm-name>
   ```

```
node_A_1-new::*> iscsi session show -vserver vsa_1
 Tpgroup Initiator Initiator
Vserver Name TSIH Name ISID Alias
--------- ------- ---- ------------------------ ---------
---------------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
scspr1789621001.gdl.englab.netapp.com
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
scspr1789621001.gdl.englab.netapp.com
2 entries were displayed.
```

4. Führen Sie auf dem neuen Node die iSCSI-Schnittstellen in ONTAP für die SVM auf, die die Schnittstellen enthält:

```
iscsi interface show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1
 Logical Status Curr Curr
Vserver Interface  TPGT Admin/Oper IP Address Node Port Enabled
------- ---------- ---- ---------- --------------- ----------- ----
-------
vsa_1 iscsi_lf__n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
true
vsa_1 iscsi_lf__n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
htp-001 e0h true
vsa_1 iscsi_lf__n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
true
vsa_1 iscsi_lf__n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
htp-002 e0h true
vsa_1 iscsi_lf__n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
true
vsa_1 iscsi_lf__n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
true
6 entries were displayed.
```

5. Führen Sie auf dem iSCSI-Host die Ermittlung auf einer der iSCSI-IP-Adressen auf der SVM aus, um die neuen Ziele zu ermitteln:

```
iscsiadm -m discovery -t sendtargets -p iscsi-ip-address
```

Die Erkennung kann mit jeder beliebigen IP-Adresse der SVM ausgeführt werden, einschließlich nicht-iSCSI-Schnittstellen.

```
[root@scspr1789621001 ~]# iscsiadm -m discovery -t sendtargets -p
10.230.68.236:3260
10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.134:3260,1183 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. Melden Sie sich auf dem iSCSI-Host bei allen erkannten Adressen an:

```
iscsiadm -m node -L all -T node-address -p portal-address -l
```

```
[root@scspr1789621001 ~]# iscsiadm -m node -L all -T iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p
10.230.68.236:3260 -l
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] (multiple)
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] (multiple)
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] successful.
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] successful.
```

7. Überprüfen Sie auf dem iSCSI-Host die Anmeldung und Verbindungen:

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. Überprüfen Sie auf dem neuen Node die Anmeldung und die Verbindung mit dem Host:

```
iscsi initiator show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi initiator show -vserver vsa_1
 Tpgroup Initiator
Vserver Name             TSIH Name                  ISID
Igroup Name
------- --------         ---- --------------------- -----------------
-----------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf__n3_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf__n4_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux
4 entries were displayed.
```

Ergebnis

Am Ende dieser Aufgabe kann der Host alle iSCSI-Schnittstellen sehen (auf den alten und neuen Knoten) und ist bei allen diesen Schnittstellen angemeldet.

LUNs und Volumes werden weiterhin physisch auf den alten Knoten gehostet. Da LUNs nur für die alten Node-Schnittstellen gemeldet werden, zeigt der Host nur Pfade über den alten Node an. Um dies zu sehen, führen Sie den aus `sanlun lun show -p` Und `multipath -ll -d` Befehle auf dem Host und überprüfen Sie die Befehlsausgaben.

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ -------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ -------------------
up        primary    sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

Schritt 2: Fügen Sie die neuen Knoten als Reporting-Knoten

Nachdem Sie die Verbindungen zu den neuen Nodes eingerichtet haben, fügen Sie die neuen Nodes als Reporting-Nodes hinzu.

Schritte

1. Führen Sie auf dem neuen Node die Reporting-Nodes für LUNs auf der SVM auf:

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   Die folgenden Nodes für die Berichterstellung sind lokale Nodes, da sich LUNs physisch auf den alten Knoten Node_A_1-old und Node_A_2-old befinden.

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver path                          igroup       reporting-nodes
------- ----------------------------- ------------
---------------------------
vsa_1   /vol/vsa_1_vol1/lun_linux_2  igroup_linux node_A_1-old,node_A_2-
old
.
.
.
vsa_1   /vol/vsa_1_vol9/lun_linux_19 igroup_linux node_A_1-old,node_A_2-
old
12 entries were displayed.
```

2. Fügen Sie auf dem neuen Node Reporting-Nodes hinzu:

```
lun mapping add-reporting-nodes -vserver <svm-name> -path
/vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup <igroup_name>
```

```
node_A_1-new::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-new,node_A_2-new
-igroup igroup_linux
12 entries were acted on.
```

3. Überprüfen Sie auf dem neuen Node, ob die neu hinzugefügten Nodes vorhanden sind:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux vserver path igroup reporting-nodes
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igroup reporting-nodes
------- --------------------------- ------------
---------------------------------------------------------------------------
-------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
.
.
.
12 entries were displayed.
```

4. Der `sg3-utils` Das Paket muss auf dem Linux-Host installiert sein. Dies verhindert ein `rescan-scsi-bus.sh utility not found` Fehler beim erneuten Scannen des Linux-Hosts für die neu zugeordneten LUNs mithilfe des `rescan-scsi-bus` Befehl.

   Überprüfen Sie auf dem Host, ob der `sg3-utils` Paket ist installiert:

   - Für eine Debian-basierte Distribution:

     ```
     dpkg -l | grep sg3-utils
     ```

   - Für eine Red hat basierte Distribution:

     ```
     rpm -qa | grep sg3-utils
     ```

   Installieren Sie bei Bedarf den `sg3-utils` Paket auf dem Linux-Host:

   ```
   sudo apt-get install sg3-utils
   ```

5. Scannen Sie auf dem Host den SCSI-Bus erneut auf dem Host, und ermitteln Sie die neu hinzugefügten Pfade:

   ```
   /usr/bin/rescan-scsi-bus.sh -a
   ```

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

6. Führen Sie auf dem iSCSI-Host die neu hinzugefügten Pfade auf:

```
sanlun lun show -p
```

Für jede LUN werden vier Pfade angezeigt.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
------- ---------- ------- ----------- ---------------------
host vserver
path path /dev/ host vserver
state   type       node    adapter     LIF
------  ---------- ------- ----------- ---------------------
up      primary    sdk      host3      iscsi_lf__n2_p1_
up      secondary  sdh     host2       iscsi_lf__n1_p1_
up      secondary  sdag    host4       iscsi_lf__n4_p1_
up      secondary  sdah    host5       iscsi_lf__n3_p1_
```

7. Verschieben Sie auf dem neuen Node das Volume/die Volumes, die LUNs enthalten, von den alten Nodes auf die neuen Nodes.

```
node_A_1-new::*> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_vol1" command to view the status of this operation.
node_A_1-new::*> vol move show
Vserver  Volume      State       Move       Phase            Percent-
Complete  Time-To-Complete
-------- ----------  --------    ---------- ----------------
----------------  ----------------
vsa_1    vsa_1_vol1  healthy                initializing     -
-
```

8. Überprüfen Sie nach Abschluss der Verschiebung des Volume zu den neuen Nodes, ob das Volume online ist:

```
volume show -state
```

9. Die iSCSI-Schnittstellen auf den neuen Nodes, auf denen sich die LUN jetzt befindet, werden als primäre Pfade aktualisiert. Wenn der primäre Pfad nach der Volume-Verschiebung nicht aktualisiert wird, führen Sie aus `/usr/bin/rescan-scsi-bus.sh -a` Und `multipath -v3` Auf dem Host oder warten Sie einfach, bis der Multipath-Rescanning stattfindet.

   Im folgenden Beispiel ist der primäre Pfad eine LIF auf dem neuen Node.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ -----------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------------
up        primary    sdag    host4        iscsi_lf__n4_p1_
up        secondary  sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
up        secondary  sdah    host5        iscsi_lf__n3_p1_
```

Schritt 3: Entfernen Sie Reporting Nodes und scannen Sie Pfade neu

Sie müssen die Berichtsknoten entfernen und die Pfade erneut scannen.

Schritte

1. Entfernen Sie auf dem neuen Knoten Remote-Reporting-Knoten (die neuen Knoten) für die Linux-LUNs:

   ```
   lun mapping remove-reporting-nodes -vserver <svm-name> -path * -igroup
   <igroup_name> -remote-nodes true
   ```

   In diesem Fall sind die Remote-Knoten alte Knoten.

   ```
   node_A_1-new::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
   * -igroup igroup_linux -remote-nodes true
   12 entries were acted on.
   ```

2. Überprüfen Sie auf dem neuen Node die Reporting-Nodes für die LUNs:

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   ```
   node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
   -ostype linux
   vserver  path                          igroup        reporting-nodes
   -------  ---------------------------  ------------
   -------------------------
   vsa_1    /vol/vsa_1_vol1/lun_linux_2  igroup_linux  node_A_1-
   new,node_A_2-new
   vsa_1    /vol/vsa_1_vol1/lun_linux_3  igroup_linux  node_A_1-
   new,node_A_2-new
   vsa_1    /vol/vsa_1_vol2/lun_linux_4  group_linux   node_A_1-
   new,node_A_2-new
   .
   .
   .
   12 entries were displayed.
   ```

3. Der `sg3-utils` Das Paket muss auf dem Linux-Host installiert sein. Dies verhindert ein `rescan-scsi-bus.sh utility not found` Fehler beim erneuten Scannen des Linux-Hosts für die neu zugeordneten LUNs mithilfe des `rescan-scsi-bus` Befehl.

   Überprüfen Sie auf dem Host, ob der `sg3-utils` Paket ist installiert:

- Für eine Debian-basierte Distribution:

```
dpkg -l | grep sg3-utils
```

- Für eine Red hat basierte Distribution:

```
rpm -qa | grep sg3-utils
```

Installieren Sie bei Bedarf den `sg3-utils` Paket auf dem Linux-Host:

```
sudo apt-get install sg3-utils
```

4. Scannen Sie auf dem iSCSI-Host den SCSI-Bus erneut:

```
/usr/bin/rescan-scsi-bus.sh -r
```

Die Pfade, die entfernt werden, sind die Pfade von den alten Knoten.

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
.
.
.
```

5. Überprüfen Sie auf dem iSCSI-Host, ob nur Pfade von den neuen Nodes sichtbar sind:

```
sanlun lun show -p
```

```
multipath -ll -d
```

Wo Sie weitere Informationen finden

Weitere Informationen zur MetroCluster Konfiguration.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff

"Architektur und Design der MetroCluster IP-Lösung, TR-4689"	• Eine technische Übersicht über die Konfiguration und den Betrieb der MetroCluster IP-Adresse. • Best Practices für eine MetroCluster-IP-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
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln
"Disaster Recovery"	• Disaster Recovery • Erzwungene Umschaltung • Recovery nach einem Multi-Controller- oder Storage-Ausfall

"MetroCluster-Wartung"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes
"MetroCluster Upgrade und Erweiterung"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"MetroCluster Transition"	• Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration
"MetroCluster: Upgrade, Transition und Erweiterung"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Dokumentation zu ONTAP Hardwaresystemen" **Hinweis:** die standardmäßigen Speicherregal-Wartungsverfahren können mit MetroCluster IP-Konfigurationen verwendet werden.	• Hot-Adding eines Festplatten-Shelfs • Hot-entfernen eines Festplatten-Shelfs
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate

Aktualisieren, Aktualisieren oder erweitern der MetroCluster Konfiguration

Beginnen Sie hier - Wählen Sie Ihre Prozedur

Hier starten: Sie haben die Wahl zwischen Controller-Upgrade, Systemaktualisierung oder Erweiterung

Je nach Umfang des Geräte-Upgrades wählen Sie ein Controller-Upgrade-Verfahren, ein Systemaktualisierungsverfahren oder ein Erweiterungsverfahren.

- Das Controller-Upgrade gilt nur für die Controller-Module. Die Controller werden durch ein neues Controller-Modell ersetzt.

  Modelle für Storage Shelfs werden nicht aktualisiert.

  - Bei Switchover- und Switchover-Prozessen wird der MetroCluster Switchover-Betrieb verwendet, um Clients unterbrechungsfreien Service zu bieten, während die Controller-Module im Partner-Cluster aktualisiert werden.
  - Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.
- Aktualisierungsverfahren gelten für die Controller und die Storage Shelfs.

  Im Aktualisierungsverfahren werden der MetroCluster Konfiguration neue Controller und Shelves hinzugefügt, eine zweite DR-Gruppe erstellt und die Daten werden unterbrechungsfrei zu den neuen Nodes migriert.

  Die ursprünglichen Controller werden dann außer Betrieb genommen.
- Erweiterungsverfahren fügen der MetroCluster-Konfiguration zusätzliche Controller und Shelves hinzu, ohne dass jegliche entfernt werden muss.

  Das von Ihnen verwendete Verfahren hängt vom MetroCluster-Typ und der Anzahl der vorhandenen Controller ab.

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

Upgrade-Typ	Gehe zu…
Für Controller-Upgrade	"Wählen Sie ein Controller-Upgrade-Verfahren"
Systemaktualisierung	"Wählen Sie ein Verfahren zur Systemaktualisierung aus"

Erweiterung	• "MetroCluster mit zwei Nodes auf vier Nodes" • "MetroCluster FC mit vier Nodes auf acht Nodes" • "MetroCluster IP mit vier Nodes auf acht Nodes"

Wählen Sie ein Controller-Upgrade-Verfahren

Das von Ihnen verwendete Controller-Upgrade-Verfahren hängt vom Plattformmodell und dem Typ der MetroCluster-Konfiguration ab.

Bei einem Upgrade-Verfahren werden die Controller durch ein neues Controller-Modell ersetzt. Modelle für Storage Shelfs werden nicht aktualisiert.

- Bei Switchover- und Switchover-Prozessen wird der MetroCluster Switchover-Betrieb verwendet, um Clients unterbrechungsfreien Service zu bieten, während die Controller-Module im Partner-Cluster aktualisiert werden.
- Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.

Unterstützte Controller-Upgrades

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

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

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

Alle anderen unterstützten MetroCluster IP-Controller-Upgrades

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

- Wenn Ihre Plattform nicht aufgeführt ist, gibt es keine unterstützte Kombination für Controller-Upgrades.
- Wenn Sie ein Controller-Upgrade durchführen, stimmen der alte und der neue Plattformtyp **muss** überein:
  - Sie können ein FAS System auf ein FAS System oder ein AFF A-Series auf ein AFF A-Series System aufrüsten.
  - Sie können kein FAS System auf eine AFF A-Serie oder eine AFF A-Serie auf eine AFF C-Serie aufrüsten.

    Wenn Sie beispielsweise eine FAS8200 als Plattform aktualisieren möchten, können Sie ein Upgrade auf eine FAS9000 durchführen. Sie können kein Upgrade eines FAS8200 Systems auf ein AFF A700 System durchführen.
- Auf allen Knoten (alt und neu) in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im"Hardware Universe".

Unterstützte AFF- und FAS MetroCluster IP-Controller-Upgrades

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

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

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

Die folgenden Hinweise gelten für beide Gruppen:

- Hinweis 1: Verwenden Sie für dieses Upgrade das Verfahren "Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher)"
- Hinweis 2: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.
- Hinweis 3: Die Zielplattform kann erst nach Abschluss des Controller-Upgrades interne Laufwerke haben. Sie können die internen Laufwerke nach dem Upgrade hinzufügen.
- Hinweis 4: Erfordert den Austausch der Controller-Module.
- Hinweis 5: IOM-Module sind erforderlich, um die alten Controller in ein externes SAS-Shelf zu konvertieren. Informationen zu unterstützten IOM-Modulen finden Sie im"Hardware Universe".

AFF- und FAS-Kombinationen, Gruppe 1

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

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

AFF und FAS Kombinationsgruppe 2

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

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

Unterstützte ASA MetroCluster IP-Controller-Upgrades

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

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

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

Unterstützte MetroCluster FC-Controller-Upgrades

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

- Wenn Ihre Plattform nicht aufgeführt ist, gibt es keine unterstützte Kombination für Controller-Upgrades.
- Wenn Sie ein Controller-Upgrade durchführen, stimmen der alte und der neue Plattformtyp **muss** überein:
  - Sie können ein FAS System auf ein FAS System oder ein AFF A-Series auf ein AFF A-Series System aufrüsten.
  - Sie können kein FAS System auf eine AFF A-Serie oder eine AFF A-Serie auf eine AFF C-Serie aufrüsten.

    Wenn Sie beispielsweise eine FAS8200 als Plattform aktualisieren möchten, können Sie ein Upgrade

auf eine FAS9000 durchführen. Sie können kein Upgrade eines FAS8200 Systems auf ein AFF A700 System durchführen.

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

Unterstützte Upgrades für AFF und FAS MetroCluster FC Controller

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

FAS and AFF		Target MetroCluster FC platform									
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1		Note 1			
	AFF8020		Note 1		Note 1		Note 1		Note 1		
	FAS8040 FAS8060 FAS8080										
	AFF8040 AFF8060 AFF8080										
	FAS8200					Note 2		Note 2		Note 4	
	AFF A300						Note 2		Note 2		Note 4
	FAS8300									Note 4	
	AFF A400										Note 4
	FAS9000									Note 3	
	AFF A700										Note 3
	FAS9500										
	AFF A900										

- Hinweis 1: Für das Upgrade von Controllern, wenn FCVI-Verbindungen auf vorhandenen FAS8020 oder AFF8020 Nodes die Ports 1c und 1d verwenden, lesen Sie Folgendeshttps://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/MetroCluster/Upgrading_controllers_when_FCVI_connections_on_existing_FAS8020_or_AFF8020_nodes_use_ports_1c_and_1d["Knowledge Base-Artikel"^].
- Hinweis 2: Controller-Upgrades von AFF A300- oder FAS8200-Plattformen mit integrierten Ports 0e und 0f als FC-VI-Verbindungen werden nur auf den folgenden Systemen unterstützt:
  - ONTAP 9.9.1 und frühere Versionen
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1 GA
  - ONTAP 9.13.1 und höher

    Weitere Informationen finden Sie im "Öffentlicher Bericht".
- Hinweis 3: Für dieses Upgrade siehe "Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher)"
- Hinweis 4: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.

Unterstützte ASA MetroCluster FC-Controller-Upgrades

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

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

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

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

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

MetroCluster-Typ	Upgrade-Methode	ONTAP-Version	Verfahren
IP	Upgrade mit Befehlen zum Ersetzen des System-Controllers	9.13.1 und höher	"Link zum Verfahren"
FC	Upgrade mit Befehlen zum Ersetzen des System-Controllers	9.10.1 und höher	"Link zum Verfahren"
FC	Manuelles Upgrade mit CLI-Befehlen (nur AFF A700/FAS9000 auf AFF A900/FAS9500)	9.10.1 und höher	"Link zum Verfahren"
IP	Manuelles Upgrade mit CLI-Befehlen (nur AFF A700/FAS9000 auf AFF A900/FAS9500)	9.10.1 und höher	"Link zum Verfahren"
FC	Manuelles Upgrade mit CLI-Befehlen	9.8 und höher	"Link zum Verfahren"

IP	Manuelles Upgrade mit CLI-Befehlen	9.8 und höher	"Link zum Verfahren"

Wählen eines Verfahrens mithilfe der Aggregatverschiebung

Bei einem ARL-basierten Upgrade-Verfahren werden die Aggregatverschiebung verwendet, um Daten unterbrechungsfrei von der alten Konfiguration in die neue, aktualisierte Konfiguration zu verschieben.

MetroCluster-Typ	Aggregatverschiebung	ONTAP-Version	Verfahren
FC	Verwenden Sie Befehle „System Controller ersetzen“, um Controller-Modelle im gleichen Chassis zu aktualisieren	9.10.1 und höher	"Link zum Verfahren"
FC	Wird Verwendet `system controller replace` Befehle	9.8 und höher	"Link zum Verfahren"
FC	Wird Verwendet `system controller replace` Befehle	9.5 bis 9.7	"Link zum Verfahren"
FC	Verwenden von manuellen ARL-Befehlen	9.8	"Link zum Verfahren"
FC	Verwenden von manuellen ARL-Befehlen	9.7 und früher	"Link zum Verfahren"

Auswahl der Methode zur Systemaktualisierung

Das von Ihnen verwendete Verfahren zur Systemaktualisierung hängt vom Plattformmodell und dem Typ der MetroCluster-Konfiguration ab. Aktualisierungsverfahren gelten für die Controller und die Storage Shelfs. Im Aktualisierungsverfahren werden der MetroCluster Konfiguration neue Controller und Shelves hinzugefügt, eine zweite DR-Gruppe erstellt und die Daten werden unterbrechungsfrei zu den neuen Nodes migriert. Die ursprünglichen Controller werden dann außer Betrieb genommen.

Unterstützte Kombinationen aus MetroCluster IP-technischen Aktualisierungen

- Sie müssen das Verfahren zur Technologieaktualisierung abschließen, bevor Sie eine neue Last hinzufügen.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden

Sie im"Hardware Universe".

- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielplattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster neu konfigurieren, damit sie die Grenzen der Zielplattform erreichen oder darunter liegen, bevor Sie die neuen Nodes hinzufügen.
- Siehe "Hardware Universe" Für Plattformgrenzen

Unterstützte Kombinationen aus AFF- und FAS MetroCluster IP-Tech Refresh

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

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

Die folgenden Hinweise gelten für beide Gruppen:

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

AFF- und FAS-Kombinationen, Gruppe 1

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

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

AFF und FAS Kombinationsgruppe 2

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

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

Unterstützte ASA MetroCluster IP-Tech Refresh-Kombinationen

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

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

Unterstützte Kombinationen von MetroCluster FC-Technologie zur Aktualisierung

- Sie müssen das Verfahren zur Technologieaktualisierung abschließen, bevor Sie eine neue Last hinzufügen.
- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im"Hardware Universe".
- Überschreiten Sie keine Objektgrenzen des „unteren“ der Plattformen in der Kombination. Wenden Sie die untere Objektgrenze der beiden Plattformen an.
- Wenn die Grenzen der Zielplattform unter den MetroCluster-Limits liegen, müssen Sie die MetroCluster

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

- Siehe "Hardware Universe" Für Plattformgrenzen

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

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

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

Unterstützte Kombinationen aus FC-Technologieaktualisierung von ASA MetroCluster

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

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

Wählen Sie ein Aktualisierungsverfahren

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

Aktualisierungsmethode	Konfigurationstyp	ONTAP-Version	Verfahren
• Methode: Erweitern Sie die MetroCluster-Konfiguration, und entfernen Sie dann die alten Knoten	FC mit vier Nodes	9.6 und höher	"Link zum Verfahren"
• Methode: Erweitern Sie die MetroCluster-Konfiguration, und entfernen Sie dann die alten Knoten	IP mit vier Nodes	9.8 und höher	"Link zum Verfahren"

Wählen Sie ein Erweiterungsverfahren aus

Das von Ihnen verwendete Erweiterungsverfahren hängt vom Typ der MetroCluster-Konfiguration und der ONTAP-Version ab.

Beim Erweiterungsverfahren muss der MetroCluster Konfiguration neue Controller und neuer Storage hinzugefügt werden. Die Erweiterung muss an jedem Standort eine geraden Anzahl an Controllern beibehalten. Das Verfahren, das Sie verwenden, hängt von der Anzahl der Nodes in der ursprünglichen MetroCluster Konfiguration ab.

Erweiterungsmethode	Konfigurationstyp	ONTAP-Version	Verfahren
Methode: Erweitern Sie eine MetroCluster FC mit zwei Nodes auf vier	FC mit zwei Nodes	ONTAP 9 und höher (Plattformen müssen in ONTAP 9.2 und höher unterstützt werden)	"Link zum Verfahren"
Methode: Erweitern Sie eine MetroCluster FC mit vier Nodes auf acht	FC mit vier Nodes	ONTAP 9 oder höher	"Link zum Verfahren"
Methode: Erweitern Sie eine MetroCluster-IP mit vier Knoten auf acht	IP mit vier Nodes	ONTAP 9.9.1 und höher	"Link zum Verfahren"

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

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

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

Informationen zu diesem Workflow

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

1. **"Upgrade wird vorbereitet"**

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

2 **"Upgrade Ihrer Controller"**

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

3 **"Schließen Sie das Upgrade ab"**

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

Upgrade wird vorbereitet

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

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

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

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

- Wenn Ihre Plattform nicht aufgeführt ist, gibt es keine unterstützte Kombination für Controller-Upgrades.
- Wenn Sie ein Controller-Upgrade durchführen, stimmen der alte und der neue Plattformtyp **muss** überein:
  - Sie können ein FAS System auf ein FAS System oder ein AFF A-Series auf ein AFF A-Series System aufrüsten.
  - Sie können kein FAS System auf eine AFF A-Serie oder eine AFF A-Serie auf eine AFF C-Serie aufrüsten.

    Wenn Sie beispielsweise eine FAS8200 als Plattform aktualisieren möchten, können Sie ein Upgrade auf eine FAS9000 durchführen. Sie können kein Upgrade eines FAS8200 Systems auf ein AFF A700 System durchführen.
- Auf allen Knoten (alt und neu) in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im"Hardware Universe".

Unterstützte AFF- und FAS MetroCluster IP-Controller-Upgrades

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

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

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

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

Die folgenden Hinweise gelten für beide Gruppen:

- Hinweis 1: Controller-Upgrades werden auf Systemen mit ONTAP 9.13.1 oder höher unterstützt.
- Hinweis 2: Die Zielplattform kann erst nach Abschluss des Controller-Upgrades interne Laufwerke haben. Sie können die internen Laufwerke nach dem Upgrade hinzufügen.
- Hinweis 3: Erfordert den Austausch der Controller-Module.
- Hinweis 4: IOM-Module sind erforderlich, um die alten Controller in ein externes SAS-Shelf zu konvertieren. Informationen zu unterstützten IOM-Modulen finden Sie im"Hardware Universe".

AFF- und FAS-Kombinationen, Gruppe 1

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

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

AFF und FAS Kombinationsgruppe 2

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

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

Unterstützte ASA MetroCluster IP-Controller-Upgrades

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

Weitere Verfahren finden Sie unter"Wählen Sie eine Upgrade- oder Aktualisierungsmethode aus".

Was kommt als Nächstes?

Lesen Sie die "Voraussetzungen für die Verwendung dieses Upgrade-Verfahrens".

Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens

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

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

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

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

  Informationen zu unterstützten Switches und Firmware-Versionen finden Sie im "Hardware Universe" oder im "IMT" .

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

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

- Folgende Vorgehensweise eignet sich zum Upgrade von Controllern in einer MetroCluster IP-Konfiguration mit vier Nodes mithilfe von NSO-basiertem automatischem Switchover und Switchback.

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

- Wenn es auf Ihrem System aktiviert ist, "End-to-End-Verschlüsselung deaktivieren" bevor Sie das Upgrade durchführen.
- Sie müssen das automatische NSO-Controller-Upgrade durchführen, um die Controller an beiden Standorten nacheinander aktualisieren zu können.
- Durch dieses automatische NSO-basierte Controller-Upgrade-Verfahren können Sie den Controller-Ersatz an einen MetroCluster Disaster Recovery (DR)-Standort initiieren. Sie können jeweils nur einen Controller-Austausch an einem Standort initiieren.
- Um an Standort A einen Controller-Austausch zu initiieren, müssen Sie den Startbefehl für den Controller-Austausch von Standort B ausführen Der Vorgang leitet Sie weiter, Controller beider Nodes nur an Standort A zu ersetzen. Um die Controller an Standort B zu ersetzen, müssen Sie den Startbefehl für den Controller-Ersatz von Standort A ausführen Es wird eine Meldung angezeigt, in der der Standort identifiziert wird, an dem die Controller ersetzt werden.

Folgende Beispielnamen werden in diesem Verfahren verwendet:

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

Was kommt als Nächstes?

"Aktivieren Sie die Konsolenprotokollierung".

Aktivieren Sie die Konsolenprotokollierung vor dem MetroCluster IP-Upgrade

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

Upgrade durchführen.

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Was kommt als Nächstes?

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

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

Für Upgrades von Systemen, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie vor dem Upgrade ein Boot-arg auf den alten Controllern einrichten.

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

Schritt 1: Bestimmen Sie den Bootarg, den Sie auf den alten Controllern einstellen müssen

Für alle unterstützten Upgrades auf den folgenden Systemen müssen Sie vor der Durchführung des Controller-Upgrades ein Boot-arg auf den alten Controllern einrichten:

- AFF A70, AFF A90, AFF A1K
- FAS70, FAS90
- AFF C80
- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60
- FAS50

> Wenn Sie ein Upgrade auf eines der aufgeführten Systeme durchführen, müssen Sie * einen erforderlichen Bootarg auf dem vorhandenen System festlegen, bevor Sie das Upgrade durchführen. Für alle anderen Upgrades können Sie diese Aufgabe überspringen und direkt zu gehen "Bereiten Sie das System für das Upgrade vor".

Bei den meisten Upgrades von Systemen, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie den Bootarg auf den alten Controllern einstellen `hw.cxgbe.toe_keepalive_disable`. Bestimmte Upgrade-Pfade erfordern jedoch, dass Sie stattdessen den Bootarg einstellen

`bootarg.siw.interop_enabled`.

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

Für dieses Upgrade…	Bootarg festlegen…
Von AFF A250 nach AFF A30	`bootarg.siw.interop_enabled`
Von AFF C250 nach AFF C30	`bootarg.siw.interop_enabled`
Von AFF A150 nach AFF A20	`bootarg.siw.interop_enabled`
Von AFF A220 nach AFF A20	`bootarg.siw.interop_enabled`
Alle anderen unterstützten Upgrades auf AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, AFF C60 oder FAS50 Systeme	`hw.cxgbe.toe_keepalive_disable`

Schritt 2: Stellen Sie den erforderlichen Bootarg auf den alten Controllern ein

Diese Aufgabe ist **nur** erforderlich, wenn Sie ein Upgrade auf ein AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, AFF C60 oder FAS50 System durchführen.

Schritte

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

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

2. Stellen Sie den erforderlichen Bootarg für Ihre Upgrade-Kombination ein. Sie haben bereits den Bootarg festgelegt, den Sie mithilfe der Tabelle in festlegen müssenBestimmen Sie, welchen Bootarg Sie einstellen müssen.

   hw.cxgbe.toe_keepalive_disable

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

   ```
   setenv hw.cxgbe.toe_keepalive_disable 1

   saveenv

   printenv hw.cxgbe.toe_keepalive_disable
   ```

   bootarg.siw.interop_enabled

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

   ```
   setenv bootarg.siw.interop_enabled 1

   saveenv

   printenv bootarg.siw.interop_enabled
   ```

3. Booten des Node:

```
boot_ontap
```

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

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

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

Wie es weiter geht

"Bereiten Sie das System für das Upgrade vor".

Bereiten Sie das MetroCluster IP-System für das Upgrade vor

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

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

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

Über diese Aufgabe

Führen Sie diese Aufgabe unter folgenden Umständen aus:

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

Bevor Sie beginnen

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

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

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

- Wenn beide Ihrer alten und neuen Plattformmodelle in der folgenden Liste aufgeführt sind, müssen Sie die VLAN-ID vor dem Upgrade der Controller * nicht * aktualisieren:

- FAS8200 oder AFF A300
- AFF A320
- FAS9000 oder AFF A700
- AFF A800, AFF C800, ASA A800 oder ASA C800

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

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

Schritte

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

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

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

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"
2. Laden Sie die RCFs herunter, und installieren Sie sie.

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

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

Starten Sie den Controller-Austauschvorgang

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

Über diese Aufgabe

Bevor die MetroCluster-Prüfungen beginnen, wird ONTAP Mediator, falls installiert, automatisch erkannt und entfernt. Um das Entfernen zu bestätigen, werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben. Wenn Sie das Upgrade abgeschlossen haben, die Vorprüfungen fehlschlagen oder Sie das Upgrade nicht fortsetzen möchten, müssen Sie manuell "Konfigurieren Sie den ONTAP Mediator-Dienst neu" .

Während des Upgrades können Sie die ausführen `system controller replace show` Oder `system controller replace show-details` Befehl von Standort A, um den Status zu überprüfen. Wenn die Befehle eine leere Ausgabe zurückgeben, warten Sie einige Minuten, und führen Sie den Befehl erneut aus.

Schritte

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

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

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

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

   Die Prüfungen werden im automatisierten Betrieb durchgeführt. Wenn keine Probleme gefunden werden, wird der Vorgang angehalten, sodass Sie die konfigurationsbezogenen Informationen manuell erfassen können.

   Das aktuelle Quellsystem und alle kompatiblen Zielsysteme werden angezeigt. Wenn Sie den Quellcontroller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang nach dem Booten der neuen Knoten angehalten und meldet einen Fehler. Führen Sie die manuelle Wiederherstellung durch, um den Cluster wieder in einen fehlerfreien Zustand zu versetzen.

   Der `system controller replace start` Der Befehl meldet möglicherweise den folgenden Vorprüffehler:

   ```
   Cluster-A::*>system controller replace show
   Node        Status         Error-Action
   ----------- -------------- ------------------------------------
   Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
   showed errors in component aggregates
   ```

   Überprüfen Sie, ob dieser Fehler aufgetreten ist, weil Sie nicht gespiegelte Aggregate oder ein anderes Problem an Aggregaten haben. Vergewissern Sie sich, dass sich alle gespiegelten Aggregate in einem ordnungsgemäßen Zustand befinden und dass sie nicht beeinträchtigt bzw. gespiegelt werden. Wenn dieser Fehler nur auf nicht gespiegelte Aggregate zurückzuführen ist, können Sie diesen Fehler durch Auswahl des überschreiben `-skip-metrocluster-check true` Option auf der `system controller replace start` Befehl. Wenn auf Remote-Storage zugegriffen werden kann, sind die nicht gespiegelten Aggregate nach einer Umschaltung online. Falls die Remote-Storage-Verbindung ausfällt, können die nicht gespiegelten Aggregate nicht online geschaltet werden.

2. Erfassen Sie manuell die Konfigurationsinformationen, indem Sie sich bei Standort B anmelden und den

Befehlen folgen, die in der Konsolenmeldung unter der aufgeführt sind `system controller replace show` Oder `system controller replace show-details` Befehl.

Sammeln Sie vor dem Upgrade Informationen

Vor dem Upgrade, wenn das Root-Volume verschlüsselt ist, müssen Sie den Sicherungsschlüssel und andere Informationen sammeln, um die neuen Controller mit den alten verschlüsselten Root-Volumes zu booten.

Über diese Aufgabe

Diese Aufgabe wird für die bestehende MetroCluster IP-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel für die vorhandenen Controller, damit Sie bei der Einrichtung der neuen Controller problemlos die Kabel identifizieren können.
2. Zeigen Sie die Befehle an, um den Backup-Schlüssel und weitere Informationen zu erfassen:

   ```
   system controller replace show
   ```

   Führen Sie die unter aufgeführten Befehle aus `show` Befehl aus dem Partner-Cluster.

   Der `show` In der Befehlsausgabe werden drei Tabellen angezeigt, die die MetroCluster-Schnittstellen-IPs, System-IDs und System-UUIDs enthalten. Diese Informationen sind später im Verfahren zum Festlegen der Bootargs erforderlich, wenn Sie den neuen Node booten.

3. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

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

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster-IP-Konfiguration mit vier Knoten werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260
   - Node_B_1-alt: 4068741254
   - Node_B_2-alt: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

In diesem Beispiel für eine MetroCluster-IP-Konfiguration mit zwei Knoten werden die folgenden alten System-IDs abgerufen:

- Node_A_1: 4068741258
- Knoten_B_1: 4068741254

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

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node <node-name> -type physical`
   - `network port vlan show -node <node-name>`
   - `network port ifgrp show -node <node-name> -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`

- `storage aggregate show`
- `system node run -node <node-name> sysconfig -a`
- `aggr show -r`
- `disk show`
- `system node run <node-name> disk show`
- `vol show -fields type`
- `vol show -fields type , space-guarantee`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

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

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

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

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

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

   a. Wenn Onboard Key Manager konfiguriert ist:

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

      Sie benötigen die Passphrase später im Upgrade-Verfahren.

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

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

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

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

   ```
   system controller replace resume
   ```

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

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

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration über den Tiebreaker oder eine andere Software entfernen, bevor der alte Controller ersetzt wird.

Schritte

1. "Entfernen der vorhandenen MetroCluster-Konfiguration" Über die Tiebreaker Software.
2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Was kommt als Nächstes?

"Vorbereiten der Netzwerkkonfiguration der alten Controller".

Upgrade Ihrer Controller

Bereiten Sie die Netzwerkkonfiguration der alten MetroCluster IP-Controller vor

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

Bevor Sie beginnen

Vor dem Starten der Umschaltung hält der Automatisierungsvorgang pausiert, sodass Sie manuell überprüfen können, ob alle LIFs „`up`“ an Standort B. sind Ggf. Beliebige LIFs mit „`deigenen`“ bis „`up`“ bereitstellen und den Automatisierungsvorgang mit dem fortsetzen `system controller replace resume` Befehl.

Der Automatisierungsvorgang initiiert die Umschaltvorgänge. Nach Abschluss dieser Vorgänge wird der Vorgang bei **pausiert für Benutzereingriff** angehalten, sodass Sie die Controller racken und installieren können, die Partner-Controller starten und die Root-Aggregat-Festplatten dem neuen Controller-Modul aus Flash-Backup mit dem zuvor gesammelten zuweisen können `sysids`.

Über diese Aufgabe

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

Schritte

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

   ```
   boot_ontap
   ```

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

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

Shared-Cluster-/HA-Ports

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

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

Shared-MetroCluster/HA-Ports

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

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

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

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

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

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

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

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

   > Dieser Schritt ist für ein erfolgreiches Upgrade erforderlich.

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

   Informationen zur Portverteilung und -Zuweisung auf den neuen Knoten finden Sie im "Hardware Universe".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Anzeigen der LIFs:

```
network interface show
```

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

b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

„`e0d`“ ist zum Beispiel ein physischer Port an alten Controllern und ist auch auf neuen Controllern vorhanden. „`e0d`“ wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

Informationen zur Portnutzung der einzelnen Plattformmodelle finden Sie im"Hardware Universe".

c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

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

Im folgenden Beispiel lautet „`e0d`“.

Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

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

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

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

6. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und Schnittstellengruppen, die Cluster-Ports als Mitgliedsports verwenden.

a. VLAN-Ports löschen:

```
network port vlan delete -node <node-name> -vlan-name <portid-vlandid>
```

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

```
network port ifgrp remove-port -node <node-name> -ifgrp <interface-group-name> -port <portid>
```

Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

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

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

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

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

7. Anhalten der Knoten:

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

Dieser Schritt muss auf beiden Knoten durchgeführt werden.

8. Überprüfen Sie, ob die Nodes an der `LOADER` Eingabeaufforderung angezeigt werden, und sammeln und erhalten Sie die aktuellen Umgebungsvariablen.
9. Ermitteln Sie die Bootarg-Werte:

```
printenv
```

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

Was kommt als Nächstes?

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

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

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

Richten Sie die neuen Controller ein

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

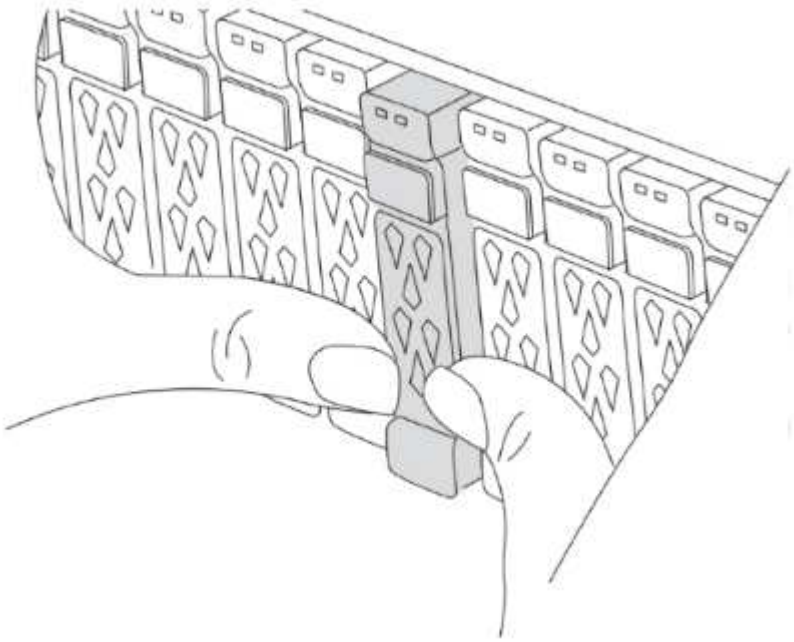
Schritte

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

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

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

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



4. Installieren Sie die Controller-Module.

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

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

Konvertierung von Controller zu externem Shelf

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

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

Schritte

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

   "Hardware Universe"

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

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

c. Setzen Sie andere Festplatten-Shelf-IDs bei Bedarf zurück.

d. Schalten Sie die Shelfs aus.

e. Verkabeln Sie das umgewandelte Festplatten-Shelf mit einem SAS-Port auf dem neuen System und bei Verwendung von Out-of-Band-ACP-Verkabelung zum ACP-Port auf dem neuen Node.

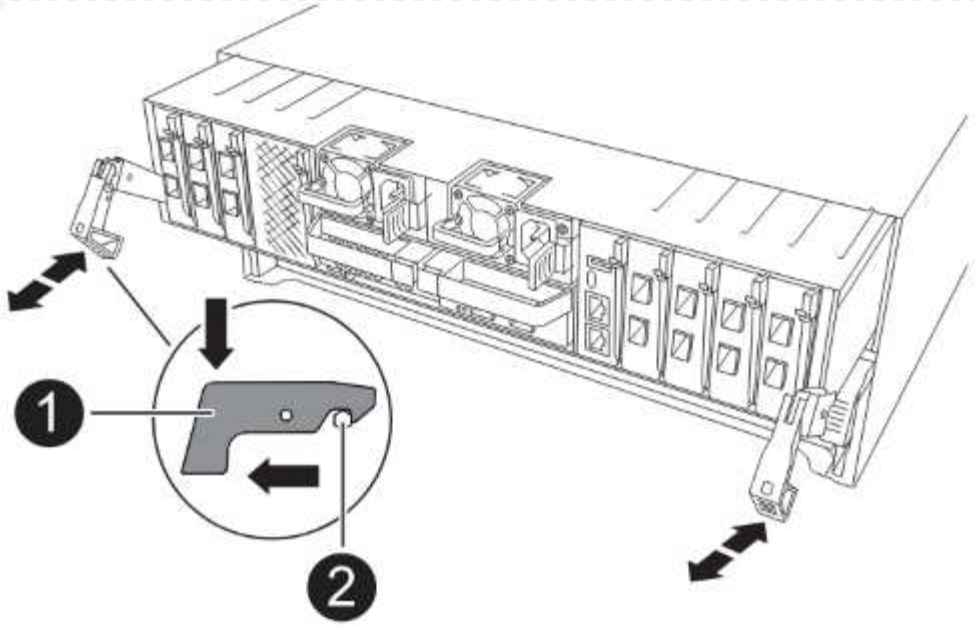
f. Schalten Sie das umgewandelte Laufwerk-Shelf und alle anderen an die neuen Nodes angeschlossenen Laufwerk-Shelfs ein.

g. Schalten Sie die neuen Nodes ein und unterbrechen Sie dann den Boot-Prozess auf jedem Node, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Austausch des Controller-Moduls

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

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



Alle anderen Upgrades

Installieren Sie die Controller-Module im Rack oder Schrank.

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

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

   "Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Aufforderung Strg-C, um die Eingabeaufforderung anzuzeigen `LOADER` .

Booten Sie die neuen Controller ein

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

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

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

`version_image.tgz`

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

4. Konfigurieren Sie an der `LOADER` Eingabeaufforderung die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

     ```
     ifconfig e0M -auto
     ```

   - Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Führen Sie den Netzboot aus.

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

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

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein
   `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie
   die URL der Bilddatei ein: `\http://web_server_ip/path_to_web-
   accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

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

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

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

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

   ```
   halt
   ```

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

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

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

   ```
   boot_ontap menu
   ```

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

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

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

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

   Antworten `yes` An die Bestätigungsaufforderung.

Was kommt als Nächstes?

"Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status fest".

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

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

Wiederherstellung der HBA-Konfiguration

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

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`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>`

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

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

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

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die Änderungen:

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

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

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

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte sein `mccip`.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

```
ha-config modify controller mccip

ha-config modify chassis mccip
```

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

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

      ```
      storage port show
      ```

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

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

      Beispiel:

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

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

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

   Informationen zu den Speicherports für das System, auf das Sie aktualisieren, finden Sie im "Hardware Universe" .

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

      ```
      storage port show
      ```

4. Stoppen Sie den Knoten: `halt`

   Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

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

Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers

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

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

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

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

Was kommt als Nächstes?

"Aktualisieren Sie die Switch-RCF-Dateien und legen Sie die MetroCluster IP-Bootarg-Werte fest".

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

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

Aktualisieren Sie die Switch-RCFs, um die neuen Plattformen aufzunehmen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

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

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"
2. Laden Sie die RCFs herunter, und installieren Sie sie.

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

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

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

Für die neuen Controller-Module müssen bestimmte MetroCluster IP-Bootarg-Werte konfiguriert werden. Die Werte müssen mit den auf den alten Controller-Modulen konfigurierten übereinstimmen.

Über diese Aufgabe

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

    Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.
- Die von Ihnen festgelegten MetroCluster Bootarg-Werte hängen davon ab, ob Ihr neues System gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet.

Shared-Cluster-/HA-Ports

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

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

Shared-MetroCluster/HA-Ports

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

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

Schritte

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

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

Systeme, die Shared Cluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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

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

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

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

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

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

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

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

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

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

Systeme, die gemeinsam genutzte MetroCluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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

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

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. Legen Sie an DER LOADER-Eingabeaufforderung der neuen Nodes die UUUIDs fest:

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

   a. Legen Sie die UUIDs auf Node_B_1-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1-New angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. Legen Sie die UUIDs auf Node_B_2-New fest:

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2-New angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

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

```
disk show
```

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

```
::> disk show
                    Usable               Disk    Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner

Info: This cluster has partitioned disks. To get a complete list of
spare disk
      capacity use "storage aggregate show-spare-disks".
----------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

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

   ```
   setenv bootarg.mcc.adp_enabled true
   ```

5. Legen Sie die folgenden Variablen fest:

   ```
   setenv bootarg.mcc.local_config_id <original-sys-id>

   setenv bootarg.mcc.dr_partner <dr-partner-sys-id>
   ```

   > Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls, Node_B_1-old, gesetzt werden.

   a. Legen Sie die Variablen auf Node_B_1-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1-New angezeigt:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Legen Sie die Variablen auf Node_B_2-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2-New angezeigt:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Was kommt als Nächstes?

"Weisen Sie die Root-Aggregat-Festplatten neu zu".

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

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

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln Sie vor dem Upgrade Informationen".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Verkabeln Sie alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.).
2. Halten Sie das System an und starten Sie von der in den Wartungsmodus `LOADER` Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). Dieses Beispiel zeigt keine Laufwerke an, die anderen Nodes in der MetroCluster-Konfiguration gehören.

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

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

```
disk reassign -s <old-sysid> -d <new-sysid>
```

Wenn Ihr MetroCluster IP-System mit erweiterter Festplattenpartitionierung konfiguriert ist, müssen Sie die ID des DR-Partnersystems angeben, indem Sie den Befehl ausführen `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid`.

Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

   `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status            Options
   aggr0_node_b_1-root         online      raid_dp, aggr     root, nosnap=on,
                               mirrored
   mirror_resync_priority=high(fixed)
                               fast zeroed
                               64-bit
   ```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Was kommt als Nächstes?

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

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

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

Starten Sie die neuen Controller

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

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr <ip-address>

   setenv bootarg.kmip.init.netmask <netmask>

   setenv bootarg.kmip.init.gateway <gateway-address>

   setenv bootarg.kmip.init.interface <interface-id>
   ```

3. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

4. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

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

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

Reagieren Sie mit „`y`“ auf die Eingabeaufforderungen zur Änderung der System-ID. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

Während eines Neustarts nach der Option „`6`“ wird die Bestätigungsaufforderung angezeigt `Override system ID? {y|n}` Angezeigt. Eingabe `y`.

6. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „`6`“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

7. Starten der Knoten:

   ```
   boot_ontap
   ```

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

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

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

   a. Broadcast-Domänen anzeigen:

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

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

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

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

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

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

   d. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast-Domäne hostet.

   e. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

   f. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

      Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

      "Erstellen einer Cluster-Peer-Beziehung"

   g. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

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

"Erstellen Sie eine VLAN"

"Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen"

a. Überprüfen Sie, ob das Partner-Cluster erreichbar ist und ob die Konfiguration auf dem Partner-Cluster erfolgreich resynchronisiert ist:

```
metrocluster switchback -simulate true
```

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

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

11. Vergewissern Sie sich, dass die MetroCluster ordnungsgemäß konfiguriert ist. Prüfen Sie den Knoten-Status:

```
metrocluster node show
```

Überprüfen Sie, ob sich die neuen Knoten (site_B) in **warten auf den Status wechseln** von site_A befinden

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs auf den entsprechenden Nodes gehostet werden, bevor Sie mit dem automatischen Switchback fortfahren.

Über diese Aufgabe

- Diese Aufgabe wird auf Site_B. ausgeführt

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

Schritte

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

   a. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

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

```
network interface show
```

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

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

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

```
vserver config override -command "network interface modify -vserver <svm-
name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
<new_node_name>"
```

Wenn Sie den Befehl zur Änderung der Netzwerkschnittstelle in eingeben `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können das Netzwerk erstellen `interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

a. Vergewissern Sie sich, dass alle Daten-LIFs nun am richtigen Home Port sind:

```
network interface show
```

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

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

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

3. Vorgang fortsetzen:

```
system controller replace resume
```

Was kommt als Nächstes?

"Schließen Sie das Controller-Upgrade ab".

Schließen Sie das MetroCluster IP-Controller-Upgrade ab

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

Überprüfung der Erreichbarkeit des Netzwerks

Der Automatisierungsvorgang führt Überprüfungen des Verifikationssystems durch und hält anschließend Pausen ein, um die Erreichbarkeit des Netzwerks zu überprüfen. Nach der Überprüfung wird die

Rückgewinnungsphase für die Ressourcen eingeleitet und der Automatisierungsvorgang führt den Wechsel zurück an Standort A durch und hält die Prüfungen nach dem Upgrade an. Nachdem Sie den Automatisierungsvorgang fortgesetzt haben, führt er die Prüfungen nach dem Upgrade durch und markiert, wenn keine Fehler erkannt werden, das Upgrade als abgeschlossen.

Schritte

1. Überprüfen Sie die Netzwerkzuwachbarkeit, indem Sie die Konsolenmeldung ausführen.
2. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

   ```
   system controller replace resume
   ```

3. Der Automatisierungsvorgang wird durchgeführt `heal-aggregate`, `heal-root-aggregate`, Und die Umschaltung Operationen an Standort A, und die nach dem Upgrade prüft. Wenn der Vorgang angehalten wird, überprüfen Sie den SAN-LIF-Status manuell und überprüfen Sie die Netzwerkkonfiguration anhand der Konsolenmeldung.
4. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

   ```
   system controller replace resume
   ```

5. Prüfen Sie den Status der Prüfungen nach der Aktualisierung:

   ```
   system controller replace show
   ```

   Wenn bei der Überprüfung nach dem Upgrade keine Fehler gemeldet wurden, ist das Upgrade abgeschlossen.

6. Melden Sie sich nach Abschluss des Controller-Upgrades bei Standort B an und überprüfen Sie, ob die ersetzten Controller ordnungsgemäß konfiguriert sind.

Aktualisieren Sie die Nodes auf Cluster_A

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

Schritte

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

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

Fügen Sie interne Laufwerke erneut zum neuen Controller hinzu

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

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

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

Konfigurieren Sie ONTAP Mediator neu

Konfigurieren Sie ONTAP Mediator manuell, der vor dem Start des Upgrades automatisch entfernt wurde.

1. Verwenden Sie die Schritte in "Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration".

Wiederherstellung des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Fügen Sie MetroCluster-Konfigurationen hinzu".

Konfigurieren Sie die End-to-End-Verschlüsselung

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

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

Workflow für MetroCluster IP-Controller-Upgrades mithilfe von Switchover und Switchback (ONTAP 9.8 und höher)

Mit ONTAP 9.8 ermöglicht die MetroCluster Umschaltung unterbrechungsfreien Service für Clients, während Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Informationen zu diesem Workflow

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

1 **"Upgrade wird vorbereitet"**

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

2 **"Upgrade Ihrer Controller"**

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

3 **"Schließen Sie das Upgrade ab"**

Führen Sie das Controller-Upgrade durch, indem Sie die Upgrade-Aufgaben am zweiten Standort wiederholen

und die Überwachungskonfiguration wiederherstellen.

Upgrade wird vorbereitet

Anforderungen für die Verwendung dieses MetroCluster IP-Upgrade-Verfahrens

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

Plattformen, die durch dieses Verfahren unterstützt werden

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

    Siehe "Wahl einer Upgrade- oder Aktualisierungsmethode" Für zusätzliche Verfahren.

Anforderungen

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

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

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

  Informationen zu unterstützten Switches und Firmware-Versionen finden Sie im "Hardware Universe" oder im "IMT" .

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

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

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

Folgende Beispielnamen werden in diesem Verfahren verwendet:

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

Was kommt als Nächstes?

"Aktivieren Sie die Konsolenprotokollierung".

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

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

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

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

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

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

Was kommt als Nächstes?

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

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

Controller-Upgrades für Systeme, die in ONTAP 9.15.1 oder höher eingeführt wurden, erfordern es, dass Sie ein Boot-arg auf den alten Controllern einrichten, bevor Sie mit dem Upgrade beginnen können.

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

Schritt 1: Bestimmen Sie den Bootarg, den Sie auf den alten Controllern einstellen müssen

Für alle unterstützten Upgrades auf den folgenden Systemen müssen Sie vor der Durchführung des Controller-Upgrades ein Boot-arg auf den alten Controllern einrichten:

- AFF A70, AFF A90, AFF A1K
- FAS70, FAS90
- AFF C80
- AFF A50, AFF A20, AFF A30
- AFF C30, AFF C60
- FAS50

> Wenn Sie ein Upgrade auf eines der aufgeführten Systeme durchführen, müssen Sie * einen erforderlichen Bootarg auf dem vorhandenen System festlegen, bevor Sie das Upgrade durchführen. Für alle anderen Upgrades können Sie diese Aufgabe überspringen und direkt zu gehen "Bereiten Sie das System für das Upgrade vor".

Bei den meisten Upgrades von Systemen, die in ONTAP 9.15.1 oder höher eingeführt wurden, müssen Sie den Bootarg auf den alten Controllern einstellen `hw.cxgbe.toe_keepalive_disable`. Bestimmte Upgrade-Pfade erfordern jedoch, dass Sie stattdessen den Bootarg einstellen `bootarg.siw.interop_enabled`.

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

Für dieses Upgrade…	Bootarg festlegen…
Von AFF A250 nach AFF A30	`bootarg.siw.interop_enabled`
Von AFF C250 nach AFF C30	`bootarg.siw.interop_enabled`
Von AFF A150 nach AFF A20	`bootarg.siw.interop_enabled`
Von AFF A220 nach AFF A20	`bootarg.siw.interop_enabled`
Alle anderen unterstützten Upgrades auf AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, AFF C60 oder FAS50 Systeme	`hw.cxgbe.toe_keepalive_disable`

Schritt 2: Stellen Sie den erforderlichen Bootarg auf den alten Controllern ein

Diese Aufgabe ist **nur** erforderlich, wenn Sie ein Upgrade auf ein AFF A70, AFF A90, AFF A1K, FAS70, FAS90, AFF C80, AFF A50, AFF A20, AFF A30, AFF C30, AFF C60 oder FAS50 System durchführen.

Schritte

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

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

2. Stellen Sie den erforderlichen Bootarg für Ihre Upgrade-Kombination ein. Sie haben bereits den Bootarg festgelegt, den Sie mithilfe der Tabelle in festlegen müssenBestimmen Sie, welchen Bootarg Sie einstellen müssen.

   hw.cxgbe.toe_keepalive_disable

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

   ```
   setenv hw.cxgbe.toe_keepalive_disable 1

   saveenv

   printenv hw.cxgbe.toe_keepalive_disable
   ```

   bootarg.siw.interop_enabled

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

   ```
   setenv bootarg.siw.interop_enabled 1

   saveenv

   printenv bootarg.siw.interop_enabled
   ```

3. Booten des Node:

   ```
   boot_ontap
   ```

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

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

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

Was kommt als Nächstes?

"Bereiten Sie das System für das Upgrade vor".

Bereiten Sie das MetroCluster IP-System für das Upgrade vor

Bevor Sie Änderungen an der vorhandenen MetroCluster Konfiguration vornehmen,

überprüfen Sie den Zustand der Konfiguration, bereiten die neuen Plattformen vor und führen verschiedene andere Aufgaben aus.

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

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

Über diese Aufgabe

Führen Sie diese Aufgabe unter folgenden Umständen aus:

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

Bevor Sie beginnen

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

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

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

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

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

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

Schritte

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

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

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

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"
2. Laden Sie die RCFs herunter, und installieren Sie sie.

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

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

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

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

Über diese Aufgabe

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

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

Physische Ports für Cluster-Interconnect		
Alter Controller	Neuer Controller	Erforderliche Maßnahme

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

Schritte

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

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

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

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

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

Daten 4						
San						
Intercluster-Port						

Booten Sie die neuen Controller ein

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

Schritte

1. Netzboot der neuen Controller:

   a. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.

   b. Laden Sie die entsprechende ONTAP Software im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.

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

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

      ```
      _ontap-version_image.tgz
      ```

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

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

Wenn IP-Adresse…	Dann…
DHCP	Konfigurieren der automatischen Verbindung: `ifconfig e0M -auto`
Festgelegt	Konfigurieren Sie die manuelle Verbindung: `ifconfig e0M -addr=`*`ip_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`*

   e. Führen Sie den Netzboot aus.

      ```
      netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-
      ```

`version_image.tgz`

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

   Ignorieren Sie die folgende Meldung:

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

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

   `http://`*`web_server_ip/path_to_web-accessible_directory/ontap-version`*`_image.tgz`

b. Geben Sie ggf. den Benutzernamen und das Kennwort ein, oder drücken Sie die Eingabetaste, um fortzufahren.

c. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

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

d. Starten Sie den Neustart durch Eingabe **`y`** Wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

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

Löschen Sie die Konfiguration auf einem Controller-Modul

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

Schritte

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

   `halt`

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

   `set-defaults`

3. Umgebung speichern:

   `saveenv`

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

```
boot_ontap menu
```

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

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

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

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

   Antworten `yes` An die Bestätigungsaufforderung.

Überprüfen Sie vor Standort-Upgrade den MetroCluster-Zustand

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

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

Schritte

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

   a. Prüfen Sie, ob die Knoten multipathed sind:
      `node run -node <node_name> sysconfig -a`

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

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

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

   c. Überprüfen Sie auf Statusmeldungen:

      ```
      system health alert show
      ```

      Geben Sie diesen Befehl für jedes Cluster ein.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

      ```
      system license show
      ```

      Geben Sie diesen Befehl für jedes Cluster ein.

   e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Geben Sie diesen Befehl für jedes Cluster ein.

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

```
cluster date show
```

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

2. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.
   a. Bestätigen Sie die MetroCluster-Konfiguration und den Betriebsmodus `normal`: `metrocluster show`
   b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden: `metrocluster node show`
   c. Geben Sie den folgenden Befehl ein:

```
metrocluster check run
```

   d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

3. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.
   a. Laden Sie Config Advisor herunter und führen Sie sie aus.

   "NetApp Downloads: Config Advisor"

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

Sammeln Sie vor dem Upgrade Informationen

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

Schritte

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

   Sammeln Sie die Ausgabe der folgenden Befehle für jeden Node:

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`

- `network port show -node <node_name> -type physical`
- `network port vlan show -node <node_name>`
- `network port ifgrp show -node <node_name> -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node <node_name> sysconfig -a`
- `aggr show -r`
- `disk show`
- `system node run <node-name> disk show`
- `vol show -fields type`
- `vol show -fields type , space-guarantee`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

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

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

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

   Im folgenden Beispiel wird die Befehlsausgabe mit den UUIDs angezeigt:

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

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

Cluster oder Node	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Knoten_B_1	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Knoten_B_2	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

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

   Sammeln Sie die Ausgabe der folgenden Befehle:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

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

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

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

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

   a. Wenn Onboard Key Manager konfiguriert ist:
      ```
      security key-manager onboard show-backup
      ```

      Sie benötigen die Passphrase später im Upgrade-Verfahren.

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

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

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

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

   Die folgende Ausgabe zeigt die neu zugewiesen Laufwerke.

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

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

Entfernen Sie die Mediator- oder Tiebreaker-Überwachung

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

Schritte

1. Sammeln Sie die Ausgabe für den folgenden Befehl:

   ```
   storage iscsi-initiator show
   ```

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

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

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

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

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

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

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

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

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

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

Was kommt als Nächstes?

"Wechseln Sie über die MetroCluster-Konfiguration".

Upgrade Ihrer Controller

Wechseln Sie über die MetroCluster IP-Konfiguration

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

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe:

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

Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl für Cluster_A ein:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   d. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

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

Was kommt als Nächstes?

"Entfernen Sie die Schnittstellenkonfigurationen, und deinstallieren Sie die alten Controller".

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

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

Über diese Aufgabe

- Diese Schritte führen Sie auf den alten Controllern aus (Node_B_1-old, Node_B_2-old).

- Sie benötigen die Informationen, die Sie für diesen Vorgang gesammelt "Weisen Sie den neuen Nodes Ports von den alten Nodes zu"haben.

Schritte

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

   ```
   boot_ontap
   ```

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

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

Shared-Cluster-/HA-Ports

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

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

Shared-MetroCluster/HA-Ports

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

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

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

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

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

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

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

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

   > Dieser Schritt ist für ein erfolgreiches Upgrade erforderlich.

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

   Informationen zur Portverteilung und -Zuweisung auf den neuen Knoten finden Sie im "Hardware Universe".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Anzeigen der LIFs:

```
network interface show
```

Alle Daten-LIFs wie SAN und NAS sind Administrator betriebsbereit und betriebsbereit, da sie sich am Switchover-Standort (Cluster_A) befinden.

b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

e0d ist zum Beispiel ein physischer Port auf den alten Controllern und ist auch auf neuen Controllern vorhanden. e0d wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

Informationen zur Portnutzung für Plattformmodelle finden Sie im "Hardware Universe"

c. Ändern Sie alle DATEN-LIFS, um den gemeinsamen Port als Home Port zu verwenden:
```
network interface modify -vserver <svm-name> -lif <data-lif> -home-port
<port-id>
```

Im folgenden Beispiel ist dies "e0d".

Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

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

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

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

6. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und Schnittstellengruppen, die Cluster-Ports als Mitgliedsports verwenden.

a. VLAN-Ports löschen:
```
network port vlan delete -node <node_name> -vlan-name <portid-vlandid>
```

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

```
network port ifgrp remove-port -node <node_name> -ifgrp <interface-group-
name> -port <portid>
```

Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

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

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

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

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

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

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

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

   ```
   printenv
   ```

10. Trennen Sie die Speicher- und Netzwerkverbindungen auf Node_B_1-old und Node_B_2-old. Beschriften Sie die Kabel, sodass Sie sie mit den neuen Nodes verbinden können.
11. Trennen Sie die Stromkabel von Node_B_1-old und Node_B_2-old.
12. Entfernen Sie die Controller Node_B_1-old und Node_B_2-old aus dem Rack.

Was kommt als Nächstes?

"Richten Sie die neuen Controller ein".

Richten Sie die neuen MetroCluster IP-Controller ein

Rack und Verkabelung der neuen MetroCluster IP-Controller

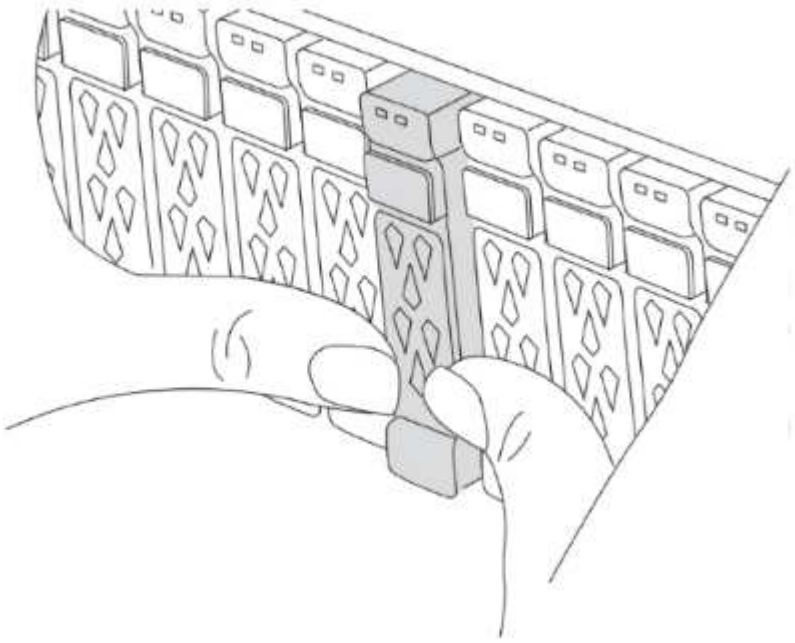
Schritte

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

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

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

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



4. Installieren Sie die Controller-Module.

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

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

Konvertierung von Controller zu externem Shelf

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

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

Schritte

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

   "Hardware Universe"

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

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

c. Setzen Sie andere Festplatten-Shelf-IDs bei Bedarf zurück.

d. Schalten Sie die Shelfs aus.

e. Verkabeln Sie das umgewandelte Festplatten-Shelf mit einem SAS-Port auf dem neuen System und bei Verwendung von Out-of-Band-ACP-Verkabelung zum ACP-Port auf dem neuen Node.

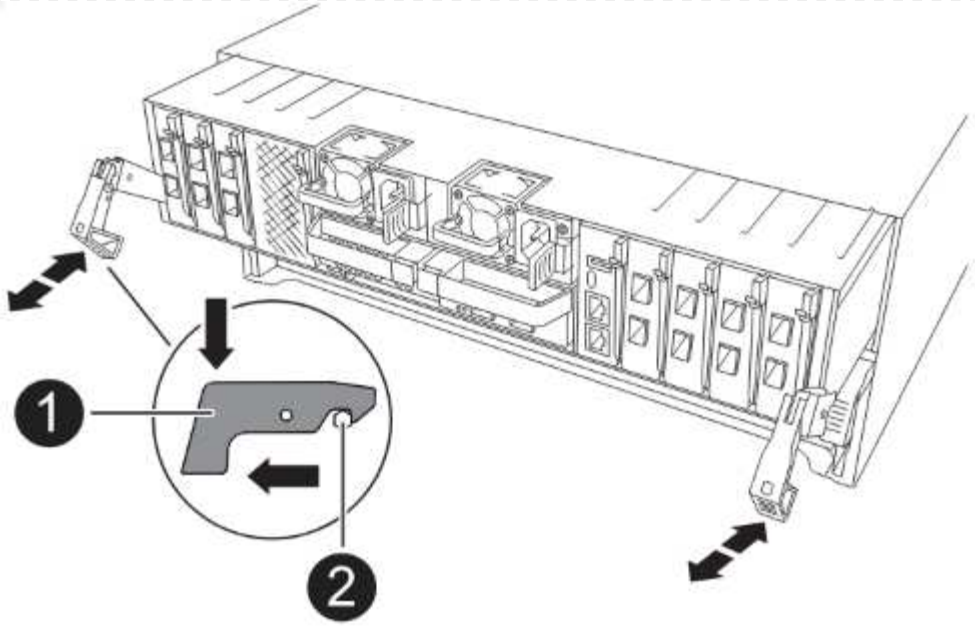
f. Schalten Sie das umgewandelte Laufwerk-Shelf und alle anderen an die neuen Nodes angeschlossenen Laufwerk-Shelfs ein.

g. Schalten Sie die neuen Nodes ein und unterbrechen Sie dann den Boot-Prozess auf jedem Node, indem Sie Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.

Austausch des Controller-Moduls

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

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



Alle anderen Upgrades

Installieren Sie die Controller-Module im Rack oder Schrank.

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

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

   "Dokumentation zu ONTAP Hardwaresystemen"

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

Was kommt als Nächstes?

"Stellen Sie die HBA-Konfiguration wieder her, und legen Sie den HA-Status fest".

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

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

Wiederherstellung der HBA-Konfiguration

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

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die 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>`

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

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

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

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die Änderungen:

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

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

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

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte sein `mccip`.

2. Wenn der angezeigte Systemstatus des Controllers oder Chassis nicht korrekt ist, legen Sie den HA-Status fest:

```
ha-config modify controller mccip

ha-config modify chassis mccip
```

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

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

      ```
      storage port show
      ```

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

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

      Beispiel:

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

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

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

   Informationen zu den Speicherports für das System, auf das Sie aktualisieren, finden Sie im "Hardware Universe" .

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

      ```
      storage port show
      ```

4. Stoppen Sie den Knoten: `halt`

   Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

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

Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers

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

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

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

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

Was kommt als Nächstes?

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

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

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

Aktualisieren Sie die Switch-RCFs, um die neuen Plattformen aufzunehmen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

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

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

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"
2. Laden Sie die RCFs herunter, und installieren Sie sie.

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

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

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

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

Über diese Aufgabe

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

    Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.
- Die von Ihnen festgelegten MetroCluster Bootarg-Werte hängen davon ab, ob Ihr neues System gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet.

Shared-Cluster-/HA-Ports

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

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

Shared-MetroCluster/HA-Ports

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

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

Schritte

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

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

Systeme, die Shared Cluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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

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

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

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

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

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

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

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

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

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

Systeme, die gemeinsam genutzte MetroCluster/HA-Ports verwenden

a. Legen Sie die folgenden Bootargs fest:

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

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

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

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

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

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. Legen Sie an DER LOADER-Eingabeaufforderung der neuen Nodes die UUUIDs fest:

```
setenv bootarg.mgwd.partner_cluster_uuid <partner-cluster-UUID>

setenv bootarg.mgwd.cluster_uuid <local-cluster-UUID>

setenv bootarg.mcc.pri_partner_uuid <DR-partner-node-UUID>

setenv bootarg.mcc.aux_partner_uuid <DR-aux-partner-node-UUID>

setenv bootarg.mcc_iscsi.node_uuid <local-node-UUID>
```

   a. Legen Sie die UUIDs auf Node_B_1-New fest:

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1-New angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

   b. Legen Sie die UUIDs auf Node_B_2-New fest:

      Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2-New angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

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

```
disk show
```

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

```
::> disk show
                    Usable               Disk    Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner

Info: This cluster has partitioned disks. To get a complete list of
spare disk
      capacity use "storage aggregate show-spare-disks".
----------------    ---------- ----- --- ------- ----------- ---------
--------
1.11.0              894.0GB    11    0   SSD      shared     testaggr
node_A_1
1.11.1              894.0GB    11    1   SSD      shared     testaggr
node_A_1
1.11.2              894.0GB    11    2   SSD      shared     testaggr
node_A_1
```

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

   ```
   setenv bootarg.mcc.adp_enabled true
   ```

5. Legen Sie die folgenden Variablen fest:

   ```
   setenv bootarg.mcc.local_config_id <original-sys-id>

   setenv bootarg.mcc.dr_partner <dr-partner-sys-id>
   ```

   > Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls, Node_B_1-old, gesetzt werden.

   a. Legen Sie die Variablen auf Node_B_1-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1-New angezeigt:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Legen Sie die Variablen auf Node_B_2-New fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2-New angezeigt:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Was kommt als Nächstes?

"Weisen Sie die Root-Aggregat-Festplatten neu zu".

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

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

Über diese Aufgabe

Die alten System-IDs wurden in identifiziert "Sammeln Sie vor dem Upgrade Informationen".

Sie führen die Schritte im Wartungsmodus aus.

> Root-Aggregat-Festplatten sind die einzigen Festplatten, die während des Controller-Upgrades neu zugewiesen werden müssen. Die Eigentumsrechte an Datenaggregaten werden im Rahmen des Switchover/Switchback-Vorgangs übernommen.

Schritte

1. Starten des Systems in den Wartungsmodus:

   ```
   boot_ontap maint
   ```

2. Zeigen Sie die Festplatten auf Node_B_1-New in der Eingabeaufforderung Wartungsmodus an:

   ```
   disk show -a
   ```

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

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

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.
```

3. Weisen Sie die Root-Aggregat-Disks in den Laufwerk-Shelfs den neuen Controllern wieder zu.

Wenn Sie ADP verwenden…	Verwenden Sie dann diesen Befehl…
Ja.	`disk reassign -s <old-sysid> -d <new-sysid> -r <dr-partner-sysid>`
Nein	`disk reassign -s <old-sysid> -d <new-sysid>`

4. Weisen Sie die Root-Aggregat-Festplatten in den Laufwerk-Shelfs den neuen Controllern neu zu:

   `disk reassign -s <old-sysid> -d <new-sysid>`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken in einer nicht-ADP-Konfiguration:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob die Festplatten des Root-Aggregats ordnungsgemäß neu zugewiesen wurden:

   ```
   disk show
   ```

   ```
   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                     OWNER                     POOL   SERIAL NUMBER
HOME                      DR HOME
------------              -------------             -----  -------------
-------------             -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Was kommt als Nächstes?

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

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

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

Starten Sie die neuen Controller

Sie müssen die neuen Controller booten, um sicherzustellen, dass die Bootarg-Variablen korrekt sind und, falls erforderlich, die Verschlüsselungswiederherstellungsschritte durchführen.

Schritte

1. Anhalten der neuen Knoten:

```
halt
```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

```
setenv bootarg.kmip.init.ipaddr <ip-address>

setenv bootarg.kmip.init.netmask <netmask>

setenv bootarg.kmip.init.gateway <gateway-addres>

setenv bootarg.kmip.init.interface <interface-id>
```

3. Überprüfen Sie, ob die Partner-sysid aktuell ist:

```
printenv partner-sysid
```

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

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

4. ONTAP-Startmenü anzeigen:

```
boot_ontap menu
```

5. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option `10` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option `11` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

6. Wählen Sie im Startmenü „`(6) Flash-Update aus Backup config`“ aus.

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

Reagieren Sie mit „`y`“ auf die Eingabeaufforderungen zur Änderung der System-ID. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

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

   Verwenden Sie die Schritte in "Legen Sie die MetroCluster-IP-Bootarg-Variablen fest".

8. Überprüfen Sie, ob die Partner-sysid die richtige ist:

   ```
   printenv partner-sysid
   ```

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

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

9. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option `10` Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

   Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ und anschließend die Option auswählen `6` Bei der ersten Eingabeaufforderung für das Startmenü. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

10. Warten Sie, bis die ausgetauschten Nodes gebootet werden.

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

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

Sie verwenden…	Befehl

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

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

    a. Broadcast-Domänen anzeigen:

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

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

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

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

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

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

    d. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

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

    "Erstellen Sie eine VLAN"

    "Kombinieren Sie physische Ports, um Schnittstellengruppen zu erstellen"

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs zu Beginn des Upgrade-Vorgangs auf entsprechenden Nodes und Ports gehostet werden, die zugeordnet sind.

Über diese Aufgabe

- Diese Aufgabe wird auf Site_B. ausgeführt
- Sehen Sie sich den Port Mapping Plan an"Weisen Sie den neuen Nodes Ports von den alten Nodes zu", den Sie in erstellt haben.

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

Schritte

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

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

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

   ```
   network interface show
   ```

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

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

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

   ```
   vserver config override -command "network interface modify -vserver <svm-
   name> -home-port <active_port_after_upgrade> -lif <lif_name> -home-node
   <new_node_name>"
   ```

   Wenn Sie den Befehl zur Änderung der Netzwerkschnittstelle in eingeben `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können das Netzwerk erstellen `interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Vergewissern Sie sich, dass alle Daten-LIFs nun am richtigen Home Port sind:

   ```
   network interface show
   ```

   b. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

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

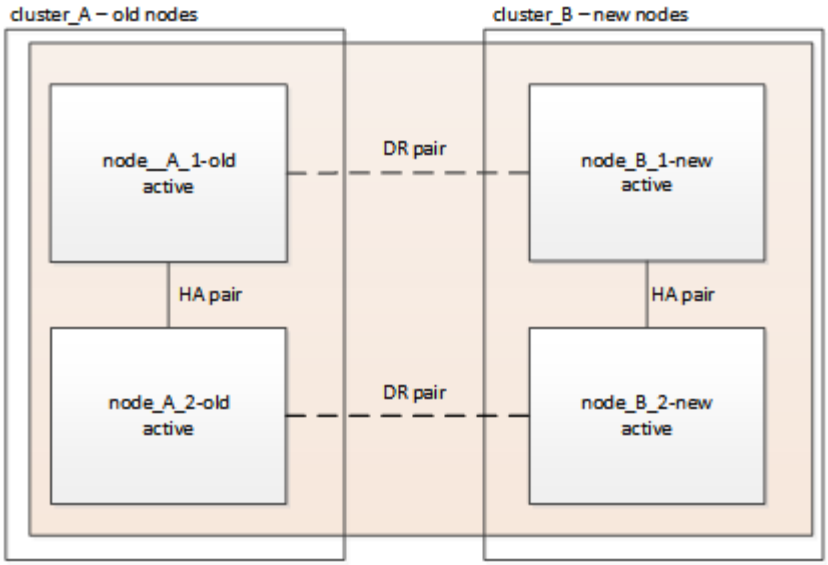
   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Was kommt als Nächstes?

"Umschalten der MetroCluster-Konfiguration".

Schalten Sie die MetroCluster IP-Konfiguration zurück

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



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Führen Sie die Reparatur und den Wechsel durch, indem Sie die erforderlichen Befehle von einem beliebigen Node im aktiven Cluster ausführen (das Cluster, das kein Upgrade durchlaufen hat).
   a. Heilen Sie die Datenaggregate:
      `metrocluster heal aggregates`
   b. Heilen Sie die Root-Aggregate:

      ```
      metrocluster heal root
      ```

   c. Zurückwechseln des Clusters:

      ```
      metrocluster switchback
      ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang normal angezeigt wird:

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

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Was kommt als Nächstes?

"Schließen Sie das Upgrade ab".

Schließen Sie das MetroCluster IP-Controller-Upgrade ab

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

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

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

Über diese Aufgabe

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

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

b. Führen Sie eine MetroCluster-Prüfung durch:
```
metrocluster check run
```

c. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

2. Überprüfen Sie die MetroCluster-Konnektivität und den Status.

a. Prüfen Sie die MetroCluster-IP-Verbindungen:

```
storage iscsi-initiator show
```

b. Prüfen Sie, ob die Knoten arbeiten:

```
metrocluster node show
```

c. Überprüfen Sie, ob die MetroCluster IP Schnittstellen aktiv sind:

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

d. Überprüfen Sie, ob lokaler Failover aktiviert ist:

```
storage failover show
```

Aktualisieren Sie die Nodes auf Cluster_A

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

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit "Bereiten Sie sich auf das Upgrade vor".

   Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

Fügen Sie die internen Laufwerke erneut zum neuen Controller hinzu

Wenn Sie ein System mit ausschließlich externen Laufwerken auf ein System mit externen und internen Laufwerken (Festplatten und Controller im selben Gehäuse) aktualisiert haben, können Sie die aus den internen Steckplätzen des neuen Systems entfernten oder entfernten Festplatten hinzufügen oder neu einsetzen. Dies ist jederzeit möglich, nachdem das Upgrade an beiden Standorten abgeschlossen ist und der Cluster fehlerfrei ist.

Nachdem Sie die Laufwerke erneut hinzugefügt oder neu eingesetzt haben, können sie nach Bedarf in ONTAP verwendet werden.

> Diese Aufgabe gilt nur für bestimmte Upgrade-Kombinationen. Weitere Informationen finden Sie unter "Entfernen Sie interne Laufwerke aus dem Gehäuse des neuen Controllers" .

Stellen Sie die Tiebreaker- oder Mediator-Überwachung wieder her

Nach Abschluss des Upgrades der MetroCluster-Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

Schritte

1. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Fügen Sie MetroCluster-Konfigurationen hinzu".
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration".
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritte

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:
   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Konfigurieren Sie die End-to-End-Verschlüsselung

Falls es von Ihrem System unterstützt wird, können Sie zwischen den MetroCluster IP-Standorten den Back-End-Verkehr, wie NVLOG- und Storage-Replizierungsdaten, verschlüsseln. Siehe "Konfigurieren Sie die End-to-End-Verschlüsselung" Finden Sie weitere Informationen.

Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster IP-Konfiguration mit Switchover und Switchback (ONTAP 9.10.1 oder höher)

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Über diese Aufgabe

- Für ein Upgrade der Controller-Module der AFF A700 auf AFF A900 müssen die Controller ONTAP 9.10.1 oder höher ausgeführt werden.

- Zum Upgrade der FAS9000 Controller-Module auf FAS9500 müssen die Controller ONTAP 9.10.1P3 oder höher ausführen.
- Upgrades für alle Controller der Konfiguration sollten während des gleichen Wartungszeitraums durchgeführt werden.

  Der Betrieb der MetroCluster Konfiguration mit einer AFF A700 und einem AFF A900 oder einem FAS9000 und FAS9500 Controller wird außerhalb dieser Wartungsaktivitäten nicht unterstützt.

- Auf den IP-Switches muss eine unterstützte Firmware-Version ausgeführt werden.
- Auf den neuen Plattformen werden die IP-Adressen, Netmasken und Gateways der ursprünglichen Plattformen wiederverwendet.
- Die folgenden Beispielnamen werden in diesem Verfahren sowohl in Beispielen als auch in Grafiken verwendet:
  - Standort_A
    - Vor dem Upgrade:
      - Node_A_1-A700
      - Node_A_2-A700
    - Nach dem Upgrade:
      - Node_A_1-A900
      - Node_A_2-A900
  - Standort_B
    - Vor dem Upgrade:
      - Node_B_1-A700
      - Node_B_2-A700
    - Nach dem Upgrade:
      - Node_B_1-A900
      - Node_B_2-A900

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

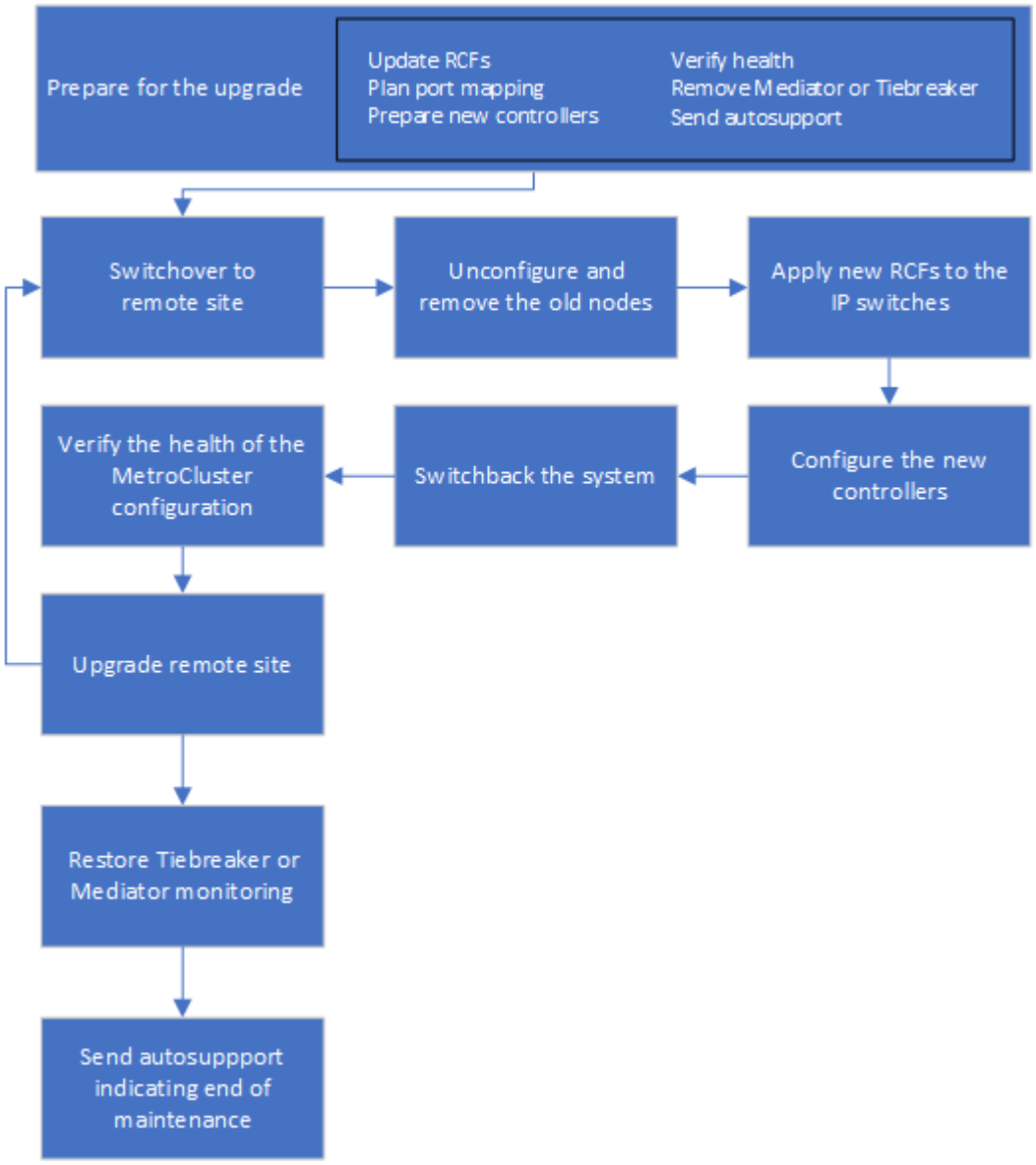
- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Workflow für das Upgrade von Controllern in einer MetroCluster IP-Konfiguration

Mithilfe des Workflow-Diagramms können Sie Upgrade-Aufgaben planen.



Bereiten Sie sich auf das Upgrade vor

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die neuen Plattformen vorbereiten und andere verschiedene Aufgaben ausführen.

Steckplatz 7 beim AFF A700 oder FAS9000 Controller löschen

Die MetroCluster-Konfiguration auf einem AFF A900 oder FAS9500 verwendet einen der Ports auf den DR-Karten in den Steckplätzen 5 und 7. Wenn beim AFF A700 oder der FAS9000 Karten in Steckplatz 7 vorhanden sind, müssen Sie die Karten in andere Steckplätze für alle Nodes des Clusters verschieben.

Aktualisieren Sie die RCF-Dateien des MetroCluster-Switch, bevor Sie die Controller aktualisieren

Sie müssen die RCF-Dateien auf MetroCluster-Switches aktualisieren, wenn Sie dieses Upgrade durchführen.

In der folgenden Tabelle sind die für AFF A900/FAS9500 MetroCluster IP-Konfigurationen unterstützten VLAN-Bereiche aufgeführt.

Modell der Plattform	Unterstützte VLAN-IDs
• AFF A900 ODER FAS9500	• 10 • 20 • Beliebiger Wert im Bereich 101 bis 4096 inklusive.

- Wenn der Switch nicht mit der minimal unterstützten RCF-Dateiversion konfiguriert ist, müssen Sie die RCF-Datei aktualisieren. Informationen zur korrekten RCF-Dateiversion für Ihr Switch-Modell finden Sie im "RcfFileGenerator-Tool". Die folgenden Schritte sind für die RCF-Datei-Anwendung.

Schritte

1. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP-Switch auf die Werkseinstellungen zurück"
2. Laden Sie die RCF-Dateien herunter und installieren Sie sie.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   - "Laden Sie die Broadcom RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die Cisco IP RCF-Dateien herunter, und installieren Sie sie"
   - "Laden Sie die NVIDIA IP RCF-Dateien herunter, und installieren Sie sie"

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

Beim Upgrade von einer AFF A700 auf ein AFF A900 oder FAS9000 auf FAS9500 werden die Datennetzwerkports, FCP SAN-Adapterports sowie SAS- und NVMe-Storage-Ports nicht geändert. Die Daten-LIFs bleiben dort, wo sie sich während und nach dem Upgrade befinden. Daher sind Sie nicht erforderlich, die Netzwerk-Ports von den alten Nodes den neuen Nodes zuzuordnen.

Überprüfen Sie vor Standort-Upgrade den MetroCluster-Zustand

Sie überprüfen den Zustand und die Konnektivität der MetroCluster-Konfiguration, bevor Sie das Upgrade durchführen.

> Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:

   a. Prüfen Sie, ob die Knoten multipathed sind:
   `node run -node node-name sysconfig -a`

      Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   b. Stellen Sie sicher, dass in der Konfiguration: + keine defekten Festplatten vorhanden sind
   `storage disk show -broken`

      Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   c. Überprüfen Sie auf Statusmeldungen:

      ```
      system health alert show
      ```

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

      ```
      system license show
      ```

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

   e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

      ```
      network device-discovery show
      ```

      Sie sollten diesen Befehl für jedes Cluster ausgeben.

   f. Vergewissern Sie sich, dass Zeitzone und Uhrzeit auf beiden Standorten richtig eingestellt sind:

      ```
      cluster date show
      ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehl zum Konfigurieren der Zeit- und Zeitzone.

2. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.

   a. Bestätigen Sie die MetroCluster-Konfiguration und den Betriebsmodus `normal`:
   `metrocluster show`

   b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:
   `metrocluster node show`

   c. Geben Sie den folgenden Befehl ein:

      ```
      metrocluster check run
      ```

   d. Ergebnisse der MetroCluster-Prüfung anzeigen:

      ```
      metrocluster check show
      ```

3. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.

a. Laden Sie Config Advisor herunter und führen Sie sie aus.

   "NetApp Downloads: Config Advisor"

b. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

Sammeln Sie vor dem Upgrade Informationen

Vor dem Upgrade müssen Informationen für alle Nodes gesammelt und bei Bedarf die Netzwerk-Broadcast-Domänen angepasst, beliebige VLANs und Schnittstellengruppen entfernt und Verschlüsselungsinformationen gesammelt werden.

Schritte

1. Notieren Sie die physische Verkabelung für jeden Node und kennzeichnen Sie die Kabel nach Bedarf, damit die neue Nodes ordnungsgemäß verkabelt werden.
2. Sammeln Sie die Ausgabe der folgenden Befehle für jeden Node:
   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node` *`node-name`* `sysconfig -a`
   - `vserver fcp initiator show`
   - `storage disk show`
   - `metrocluster configuration-settings interface show`
3. Erfassen Sie die UUIDs für Site_B (die Site, an der die Plattformen gerade aktualisiert werden):
   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Diese Werte müssen auf den neuen Controller-Modulen „Site_B“ genau konfiguriert werden, um eine erfolgreiche Aktualisierung zu gewährleisten. Kopieren Sie die Werte in eine Datei, damit Sie sie später im Upgrade-Prozess in die richtigen Befehle kopieren können. + im folgenden Beispiel wird die Befehlsausgabe mit den UUIDs angezeigt:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
   (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

Es wird empfohlen, die UUIDs in eine Tabelle wie die folgende aufzunehmen.

Cluster oder Node	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1-A700	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2-A700	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1-A700	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2-A700	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Wenn sich die MetroCluster-Nodes in einer SAN-Konfiguration befinden, sammeln Sie die relevanten Informationen.

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:
   `security key-manager backup show`

6. Wenn die MetroCluster Nodes Verschlüsselung für Volumes oder Aggregate nutzen, kopieren Sie Informationen zu Schlüsseln und Passphrases. Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen".
   a. Wenn Onboard Key Manager konfiguriert ist: `security key-manager onboard show-backup`+ Sie benötigen die Passphrase später im Upgrade-Verfahren.
   b. Wenn das Enterprise-Verschlüsselungsmanagement (KMIP) konfiguriert ist, geben Sie die folgenden Befehle ein:

```
security key-manager external show -instance
security key-manager key query
```

7. Ermitteln Sie die System-IDs der vorhandenen Nodes: `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   Die folgende Ausgabe zeigt die neu zugewiesen Laufwerke.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322           537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323           537403324
1           cluster_B node_B_2-A700   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Entfernen Sie die Mediator- oder Tiebreaker-Überwachung

Vor dem Aktualisieren der Plattformen müssen Sie die Überwachung entfernen, wenn die MetroCluster-Konfiguration mit dem Tiebreaker oder Mediator Utility überwacht wird.

Schritte

1. Sammeln Sie die Ausgabe für den folgenden Befehl:

   `storage iscsi-initiator show`

2. Entfernen Sie die vorhandene MetroCluster-Konfiguration von Tiebreaker, Mediator oder einer anderen Software, die die Umschaltung initiieren kann.

Sie verwenden…	Gehen Sie folgendermaßen vor:
Tiebreaker	"Entfernen von MetroCluster-Konfigurationen" Beim *MetroCluster Tiebreaker Installations- und Konfigurationsinhalt*
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei dem Cluster an.
2. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   Der `maintenance-window-in-hours` Parameter gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Wiederholen Sie diese Schritte auf der Partner-Site.

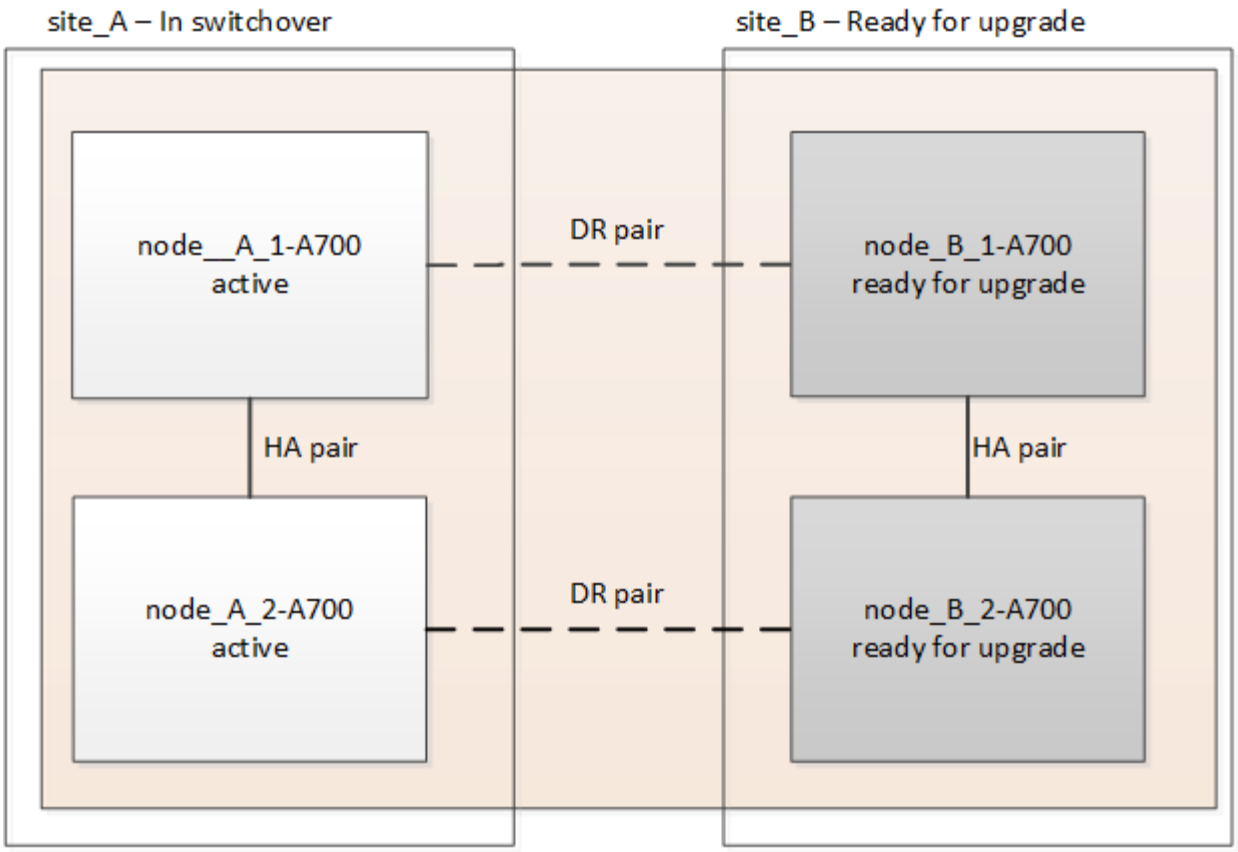
Wechseln Sie über die MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Site_A aktiv und stellt Daten für beide Standorte bereit. Site_B ist inaktiv und bereit, den Upgrade-Prozess zu starten.



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl auf Site_A aus:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   d. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

   Das automatische Heilen von Aggregaten nach der ausgehandelten Umschaltung wird während eines Controller-Upgrades deaktiviert. Nodes an Site_B werden angehalten und am angehalten `LOADER` Eingabeaufforderung:

Entfernen Sie das Controller-Modul der AFF A700 oder FAS9000 Plattform und NVS

Über diese Aufgabe

Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Schritte

1. Ermitteln Sie die Bootarg-Werte von beiden Knoten an Site_B: `printenv`
2. Schalten Sie das Chassis an Site_B. aus

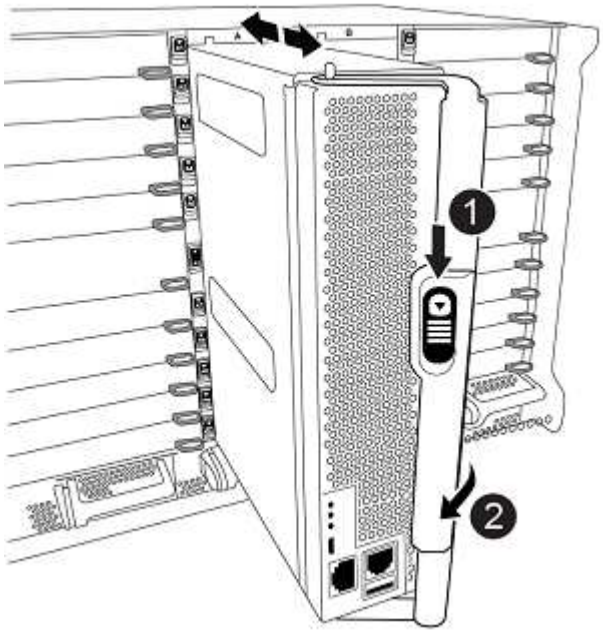
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

Gehen Sie wie folgt vor, um das AFF A700 oder das FAS9000 Controller-Modul zu entfernen

Schritte

1. Trennen Sie gegebenenfalls das Konsolenkabel und das Managementkabel vom Controller-Modul, bevor Sie das Controller-Modul entfernen.
2. Entriegeln und entfernen Sie das Controller-Modul aus dem Gehäuse.

   a. Schieben Sie die orangefarbene Taste am Nockengriff nach unten, bis sie entsperrt ist.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

   a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse. Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul wie folgt:

Hinweis: Das NVS-Modul befindet sich in Steckplatz 6 und ist doppelt so hoch wie andere Module im System.

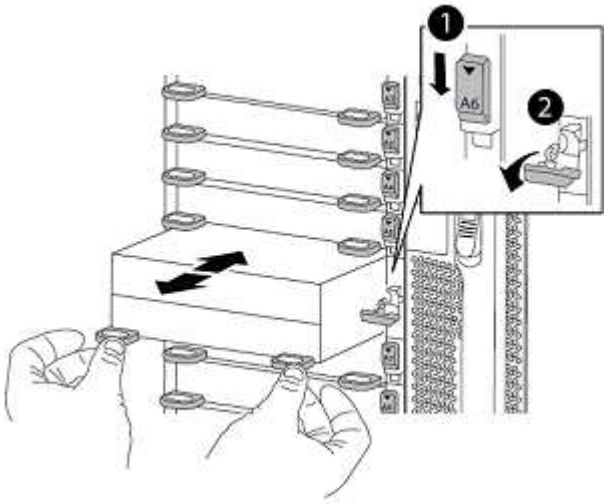
Schritte

1. Entriegeln und entfernen Sie den NVS aus Steckplatz 6.

   a. Drücken Sie die Taste mit den Buchstaben und der nummerierten Nocken. Die Nockentaste bewegt sich vom Gehäuse weg.

   b. Drehen Sie die Nockenverriegelung nach unten, bis sie sich in horizontaler Position befindet. Der NVS löst sich aus dem Gehäuse und bewegt sich ein paar Zentimeter.

   c. Entfernen Sie den NVS aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

2. Wenn Sie zusätzliche Module verwenden, die als Coredump-Geräte bei der AFF A700 oder FAS9000 NVS verwendet werden, übertragen Sie diese nicht auf den AFF A900 oder FAS9500 NVS. Übertragen Sie keine Teile vom AFF A700 oder FAS9000 Controller-Modul und NVS auf das AFF A900 oder FAS9500 Modul.

Installieren Sie die AFF A900- oder FAS9500 NVS- und Controller-Module

Sie müssen das AFF A900 oder FAS9500 NVS und das Controller-Modul installieren, das Sie im Upgrade-Kit auf beiden Knoten bei Site_B. erhalten haben Verschieben Sie das coredump-Gerät nicht vom AFF A700 oder FAS9000 NVS-Modul in das AFF A900 oder FAS9500 NVS Modul.

Über diese Aufgabe

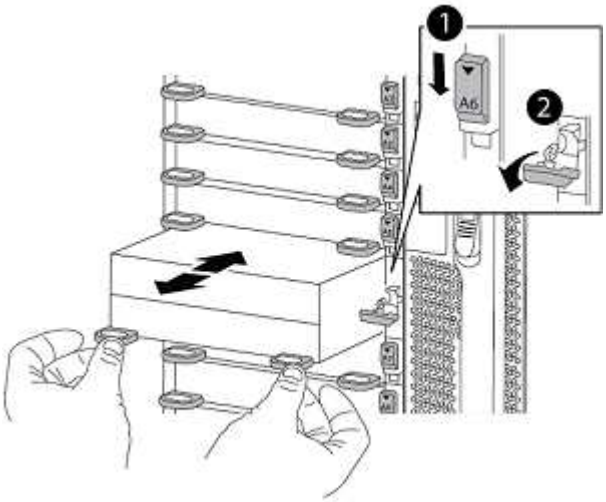
Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Installieren Sie den AFF A900 oder FAS9500 NVS

Gehen Sie wie folgt vor, um den AFF A900 oder FAS9500 NVS in Steckplatz 6 beider Knoten in Site_B. zu installieren

Schritte

1. Richten Sie den NVS an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie den NVS vorsichtig in den Schlitz, bis der vorletzte und nummerierte E/A-Nockenriegel mit dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVS.



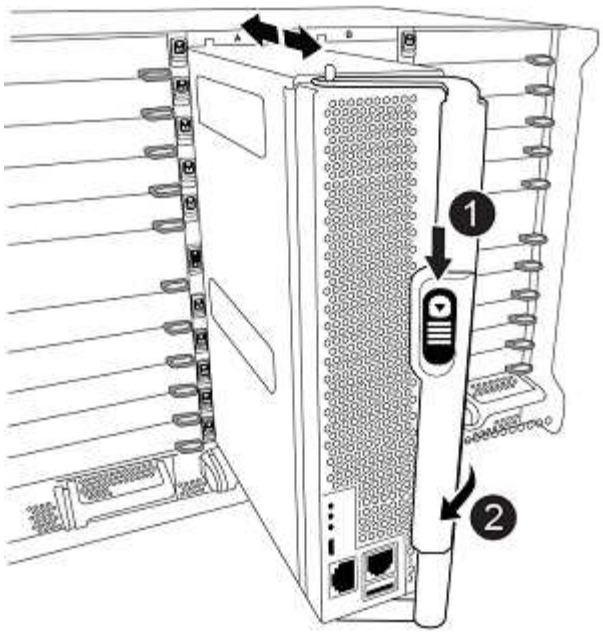
	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

Installieren Sie das AFF A900 oder FAS9500 Controller-Modul.

Gehen Sie wie folgt vor, um das AFF A900 oder FAS9500 Controller-Modul zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
2. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist. Achtung: Um Schäden an den Anschlüssen zu vermeiden, verwenden Sie keine übermäßige Kraft, wenn Sie das Controller-Modul in das Gehäuse schieben.
3. Verkabeln Sie die Management- und Konsolen-Ports mit dem Controller-Modul.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

4. Installieren Sie die zweite X91146A-Karte in Steckplatz 7 jedes Knotens.
   a. Stellen Sie die e5b-Verbindung auf e7b.
   b. schieben Sie die e5a-Verbindung auf e5b.

> Steckplatz 7 auf allen Knoten des Clusters sollte leer sein, wie im Abschnitt beschrieben. Weisen Sie den neuen Nodes Ports von den alten Nodes zu

5. Schalten Sie das Chassis EIN und verbinden Sie die serielle Konsole.
6. Wenn der Knoten nach der BIOS-Initialisierung Autoboot startet, unterbrechen Sie DEN AUTOBOOT, indem Sie Control-C drücken
7. Nach dem Autoboot wird die Eingabeaufforderung DES LOADERS unterbrochen. Wenn Sie das Autoboot nicht während des Bootens unterbrechen und node1 mit dem Booten startet, warten Sie, bis die Eingabeaufforderung Strg-C drücken, um zum Boot-Menü zu wechseln. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option 8, um den Node neu zu booten und das Autoboot während des Neustarts zu unterbrechen.
8. Legen Sie an der LOADER-Eingabeaufforderung die Standardvariablen für die Umgebung fest: Set-default
9. Speichern Sie die Standardeinstellungen für Umgebungsvariablen:
   ```
   saveenv
   ```

Netzboot-Nodes an Site_B

Nach Austausch des AFF A900 oder FAS9500 Controller-Moduls und der NVS müssen Sie die AFF A900 oder FAS9500 Nodes als Netzboot einsetzen. Die ONTAP-Version und die Patch-Ebene, die auf dem Cluster ausgeführt werden, müssen dann installiert werden. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie

eine Kopie des ONTAP 9 Boot Images auf einen Webserver hinzufügen, auf den das System zugreifen kann. Es ist nicht möglich, die auf den Boot-Medien eines AFF A900 oder FAS9500 Controller-Moduls installierte ONTAP Version zu prüfen, es sei denn, sie ist in einem Chassis installiert und eingeschaltet. Die ONTAP Version auf dem AFF A900 oder FAS9500 Boot-Medium muss mit der ONTAP Version übereinstimmen, die auf dem AFF A700 oder FAS9000 System ausgeführt wird und bei dem Upgrade der Primär- und der Backup Boot Images übereinstimmen. Sie können die Images konfigurieren, indem Sie einen Netzboot gefolgt vom ausführen `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Sie müssen die erforderlichen Systemdateien für Ihr System sowie die korrekte Version von ONTAP von der NetApp Support-Website herunterladen.

Über diese Aufgabe

Wenn die installierte ONTAP Version nicht mit der auf den ursprünglichen Controllern installierten Version identisch ist, müssen Sie die neuen Controller als Netzboot ausführen. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software im Software Download Bereich der NetApp Support Site herunter und speichern Sie die `ontap-version_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.
4. Ihre Verzeichnisliste sollte <ontap_version>_image.tgz enthalten.
5. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.

> Sie sollten den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn das Dynamic Host Configuration Protocol (DCHP)…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`

Nicht Ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> -dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` Ist die IP-Adresse des Storage-Systems. `<netmask>` Ist die Netzwerkmaske des Storage-Systems. `<gateway>` Ist das Gateway für das Storage-System. `<dns_addr>` Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. Dieser Parameter ist optional. `<dns_domain>` Der Domain Name (DNS) ist der Domain-Name. Dieser Parameter ist optional. HINWEIS: Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

6. Ausführen eines Netzboots auf Node_B_1:
   `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>\_image.tgz` In Schritt 2.

   > Unterbrechen Sie den Startvorgang nicht.

7. Warten Sie, bis der Node_B_1 nun auf dem AFF A900 oder FAS9500 Controller-Modul ausgeführt wird, und zeigen Sie die Startmenüoptionen wie unten dargestellt an:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. Wählen Sie im Startmenü Option `(7) Install new software first`.Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert. HINWEIS: Ignorieren Sie die folgende Meldung: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`. Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades.

   Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen.

9. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:
   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>\_image.tgz`
10. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
    a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:
       `Do you want to restore the backup configuration now? {y|n}`
    b. Eingabe `y to reboot when you see the following prompt:`
       `` `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n} ``Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.
11. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium:
    a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`:
       `This will delete critical system configuration, including cluster membership.`
       `Warning: do not run this option on a HA node that has been taken over.`
       `Are you sure you want to continue?:`
    b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.
12. Wählen Sie die Option `5` Wechseln Sie vom Boot-Menü zum Wartungsmodus. Antwort `yes` In die -Eingabeaufforderungen, bis der Node im Wartungsmodus beendet wird, und die Eingabeaufforderung *>.
13. Wiederholen Sie diese Schritte zum Netzboot Node_B_2.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:
   a. Überprüfen Sie die aktuellen Einstellungen der Ports:

      ```
      ucadmin show
      ```

   b. Aktualisieren Sie die 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`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte sein `mccip`.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mccip
   ```

```
ha-config modify chassis mccip
```

3. Stoppen Sie den Knoten: `halt`

   Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:

4. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `show date`
5. Stellen Sie bei Bedarf das Datum in UTC oder GMT ein: `set date <mm/dd/yyyy>`
6. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`
7. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`
8. Einstellungen speichern: `saveenv`
9. Umgebungsvariablen erfassen: `printenv`

Aktualisieren Sie die RCF-Dateien des Switches, um die neuen Plattformen aufzunehmen

Sie müssen die Switches auf eine Konfiguration aktualisieren, die die neuen Plattformmodelle unterstützt.

Über diese Aufgabe

Diese Aufgabe führen Sie an dem Standort mit den derzeit aktualisierten Controllern durch. In den Beispielen, die in diesem Verfahren gezeigt werden, aktualisieren wir zunächst Site_B.

Bei einem Upgrade der Controller On Site_A werden die Switches von Site_A aktualisiert.

Schritte

1. Bereiten Sie die IP-Switches auf die Anwendung der neuen RCFs vor.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   - "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
   - "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"

2. Laden Sie die RCFs herunter, und installieren Sie sie.

   Befolgen Sie die Schritte im Abschnitt für Ihren Switch-Anbieter:

   - "Laden Sie die Broadcom RCFs herunter, und installieren Sie sie"
   - "Laden Sie die Cisco IP-RCFs herunter, und installieren Sie sie"
   - "Laden Sie die NVIDIA IP-RCFs herunter, und installieren Sie sie"

Konfigurieren Sie die neuen Controller

Neue Controller sollten jetzt bereit und verkabelt sein.

Legen Sie die MetroCluster-IP-Bootarg-Variablen fest

Für die neuen Controller-Module müssen bestimmte MetroCluster IP-Bootarg-Werte konfiguriert werden. Die Werte müssen mit den auf den alten Controller-Modulen konfigurierten übereinstimmen.

Über diese Aufgabe

In dieser Aufgabe verwenden Sie die UUIDs und System-IDs, die zuvor im Upgrade-Verfahren in identifiziert wurden Sammeln Sie vor dem Upgrade Informationen.

Schritte

1. Am `LOADER>` Eingabeaufforderung: Legen Sie folgende Bootargs auf den neuen Knoten an Standort_B fest:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   Im folgenden Beispiel werden die Werte für Node_B_1-A900 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   Im folgenden Beispiel werden die Werte für Node_B_2-A900 mit VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. Bei den neuen Nodes `LOADER` Eingabeaufforderung, UUUIDs festlegen:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Legen Sie die UUIDs auf Node_B_1-A900 fest.

Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_1-A900 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Legen Sie die UUIDs auf Node_B_2-A900 fest:

Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_B_2-A900 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Wenn die Originalsysteme für ADP konfiguriert wurden, aktivieren Sie an der LOADER-Eingabeaufforderung der Ersatz-Nodes ADP:

```
setenv bootarg.mcc.adp_enabled true
```

4. Legen Sie die folgenden Variablen fest:

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> Der `setenv bootarg.mcc.local_config_id` Variable muss auf die sys-id des **original** Controller-Moduls, Node_B_1-A700 gesetzt werden.

a. Legen Sie die Variablen auf Node_B_1-A900 fest.

Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_1-A900 angezeigt:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Legen Sie die Variablen auf Node_B_2-A900 fest.

Im folgenden Beispiel werden die Befehle zum Einstellen der Werte auf Node_B_2-A900 angezeigt:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Wenn Sie die Verschlüsselung mit dem externen Schlüsselmanager verwenden, legen Sie die erforderlichen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu.

Über diese Aufgabe

Diese Schritte werden im Wartungsmodus ausgeführt.

Schritte

1. Starten des Systems in den Wartungsmodus:

   ```
   boot_ontap maint
   ```

2. Zeigen Sie die Laufwerke auf Node_B_1-A900 in der Eingabeaufforderung Wartungsmodus an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (537403322). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. Weisen Sie die Root-Aggregat-Disks in den Laufwerk-Shelfs den neuen Controllern wieder zu.

Wenn Sie ADP verwenden…	Verwenden Sie dann diesen Befehl…
Ja.	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
Nein	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Weisen Sie die Root-Aggregat-Festplatten in den Laufwerk-Shelfs den neuen Controllern neu zu:

   ```
   disk reassign -s old-sysid -d new-sysid
   ```

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken in einer nicht-ADP-Konfiguration:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob die Festplatten des Root-Aggregats korrekt neu zugewiesen sind.

   ```
   disk show
   ```

   ```
   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                     DR HOME
------------             -------------            -----  -------------
-------------            -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Booten der neuen Controller

Sie müssen die neuen Controller booten, um sicherzustellen, dass die Bootarg-Variablen korrekt sind und, falls erforderlich, die Verschlüsselungswiederherstellungsschritte durchführen.

Schritte

1. Anhalten der neuen Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Überprüfen Sie, ob die Partner-sysid aktuell ist:

```
printenv partner-sysid
```

Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

4. ONTAP-Startmenü anzeigen:

```
boot_ontap menu
```

5. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

6. Wählen Sie im Startmenü die Option `(6) Update flash from backup config`.

> Mit Option 6 wird der Node vor Abschluss zweimal neu gestartet.

Antworten `y` Zu den Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Unterbrechen Sie den AUTOMATISCHEN START, um die Controller am LOADER zu stoppen.

> Überprüfen Sie auf jedem Knoten die in eingestellten Bootargs "Festlegen der MetroCluster-IP-Bootarg-Variablen" Und korrigieren Sie alle falschen Werte. Gehen Sie nur zum nächsten Schritt, nachdem Sie die Bootarg-Werte überprüft haben.

8. Überprüfen Sie doppelt, ob die Partner-Sysid die richtige ist:

```
printenv partner-sysid
```

Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

9. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

Sie müssen den Wiederherstellungsvorgang durchführen, indem Sie die Option 10 oder Option 11 wählen, abhängig von der Einstellung des Schlüsselmanagers und Option 6 an der Eingabeaufforderung des Startmenüs. Um die Knoten vollständig zu booten, müssen Sie eventuell den Wiederherstellungsvorgang mit Option 1 (normaler Start) durchführen.

10. Warten Sie, bis die neuen Knoten Node_B_1-A900 und Node_B_2-A900 gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

    ```
    network port broadcast-domain show
    ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

    "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

c. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

   VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

   "Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

Überprüfung und Wiederherstellung der LIF-Konfiguration

Vergewissern Sie sich, dass LIFs zu Beginn des Upgrade-Vorgangs auf entsprechenden Nodes und Ports gehostet werden, die zugeordnet sind.

Über diese Aufgabe

- Diese Aufgabe wird auf Site_B. ausgeführt
- Sehen Sie sich den in erstellten Port-Mapping-Plan an Weisen Sie den neuen Nodes Ports von den alten Nodes zu

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Wenn Sie den Befehl zur Änderung der Netzwerkschnittstelle in eingeben `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können das Netzwerk erstellen `interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

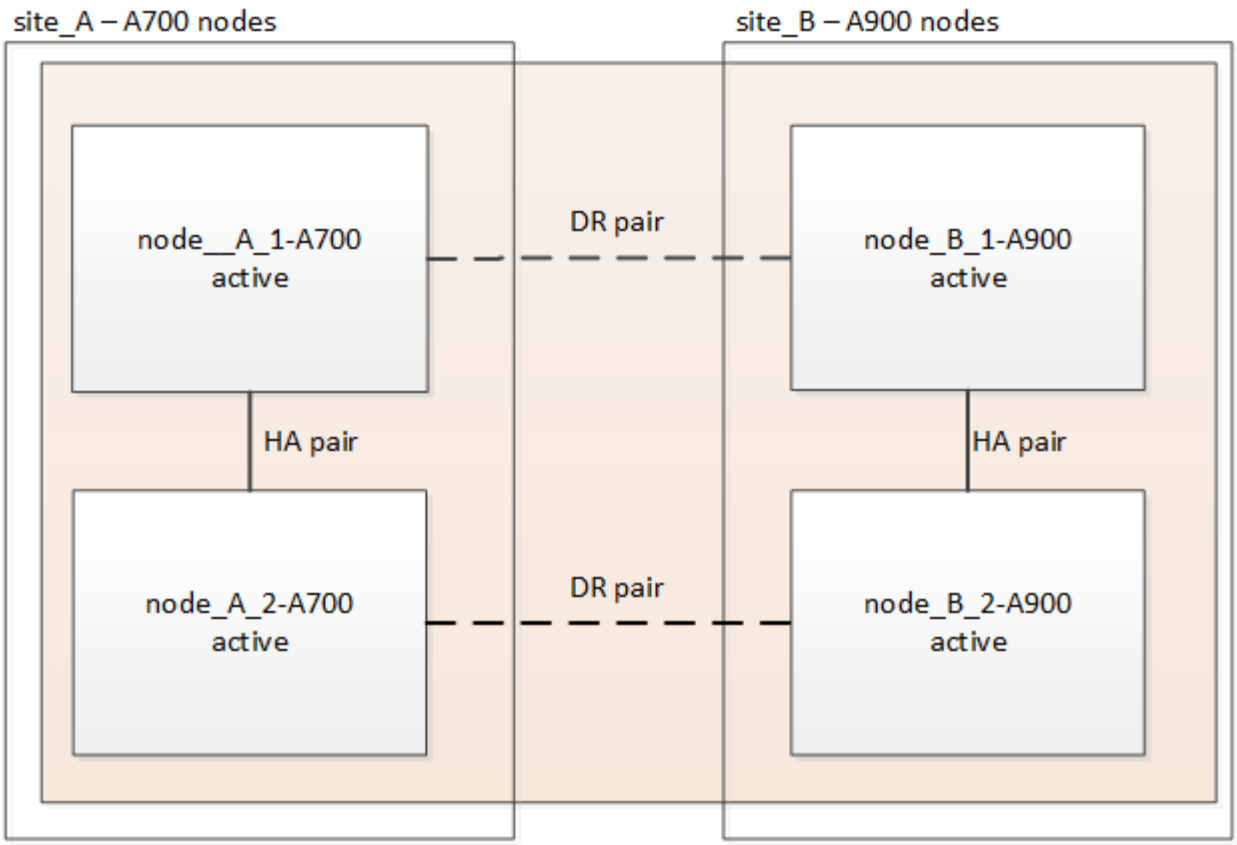
2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   ```
   network interface revert * -vserver vserver-name
   ```

   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Schalten Sie die MetroCluster-Konfiguration zurück

In dieser Aufgabe führen Sie den Vorgang zum zurückwechseln durch, und die MetroCluster-Konfiguration kehrt in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das aus `metrocluster node show` Führen Sie den Befehl von Site_B aus, und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Führen Sie die Reparatur und den Wechsel durch, indem Sie die erforderlichen Befehle von einem beliebigen Node im aktiven Cluster ausführen (das Cluster, das kein Upgrade durchlaufen hat).
   a. Heilen Sie die Datenaggregate:
      `metrocluster heal aggregates`
   b. Heilen Sie die Root-Aggregate:

      ```
      metrocluster heal root
      ```

   c. Zurückwechseln des Clusters:

      ```
      metrocluster switchback
      ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang normal angezeigt wird:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:
   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:
      `metrocluster show`
   b. Führen Sie eine MetroCluster-Prüfung durch:
      `metrocluster check run`
   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

      `metrocluster check show`

2. Überprüfen Sie die MetroCluster-Konnektivität und den Status.

a. Prüfen Sie die MetroCluster-IP-Verbindungen:

```
storage iscsi-initiator show
```

b. Prüfen Sie, ob die Knoten arbeiten:

```
metrocluster node show
```

c. Überprüfen Sie, ob die MetroCluster IP Schnittstellen aktiv sind:

```
metrocluster configuration-settings interface show
```

d. Überprüfen Sie, ob lokaler Failover aktiviert ist:

```
storage failover show
```

Aktualisieren Sie die Knoten auf site_A

Sie müssen die Upgrade-Aufgaben auf Site_A wiederholen

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Site_A zu aktualisieren, beginnend mit Bereiten Sie sich auf das Upgrade vor.

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Standorten und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von site_A verwendet wird, werden Sie von Site_B. umschalten

Stellen Sie die Tiebreaker- oder Mediator-Überwachung wieder her

Nach Abschluss des Upgrades der MetroCluster-Konfiguration können Sie die Überwachung mit dem Tiebreaker oder Mediator Utility fortsetzen.

Schritte

1. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor
Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen" Im Abschnitt *MetroCluster Tiebreaker Installation and Configuration*.
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" im Abschnitt *MetroCluster IP-Installation und -Konfiguration*.
Applikationen von Drittanbietern	Siehe Produktdokumentation.

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritte

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:
   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```
   b. Wiederholen Sie den Befehl im Partner-Cluster.

Aktualisieren Sie Controller in einer MetroCluster FC Konfiguration mithilfe von Switchover und Switchback

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Unterstützte Plattformkombinationen

Bei bestimmten Plattformen können Sie in einer MetroCluster FC-Konfiguration über den Switchover- und Switchback-Betrieb aufrüsten.

Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster FC-Upgrade-Tabelle in "Wählen Sie ein Controller-Upgrade-Verfahren".

Siehe "Wahl einer Upgrade- oder Aktualisierungsmethode" Für zusätzliche Verfahren.

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Andere Komponenten in der Konfiguration, wie z. B. Storage Shelfs oder Switches, können nicht gleichzeitig aktualisiert werden.

- Sie können dieses Verfahren mit bestimmten ONTAP-Versionen verwenden:
  - ONTAP 9.3 und höher unterstützen Konfigurationen mit zwei Nodes.
  - In ONTAP 9.8 und höher werden Konfigurationen mit vier oder acht Nodes unterstützt.

    Verwenden Sie diese Vorgehensweise nicht bei Konfigurationen mit vier oder acht Nodes und ONTAP Versionen vor 9.8.

- Ihre ursprünglichen und neuen Plattformen müssen kompatibel sein und unterstützt werden.

  "NetApp Hardware Universe"

> Wenn die ursprünglichen oder neuen Plattformen FAS8020 oder AFF8020 Systeme mit den Ports 1c und 1d im FC-VI-Modus sind, lesen Sie den Knowledge Base-Artikel "Controller-Upgrade bei FCVI-Verbindungen auf vorhandenen FAS8020 oder AFF8020 Nodes verwenden die Ports 1c und 1d."

- Die Lizenzen an beiden Standorten müssen übereinstimmen. Sie können neue Lizenzen von beziehen "NetApp Support".
- Dieses Verfahren gilt für Controller-Module in einer MetroCluster FC-Konfiguration (eine Fabric-Attached MetroCluster Konfiguration mit zwei Nodes oder eine Fabric-Attached MetroCluster Konfiguration mit zwei, vier oder acht Nodes).
- Alle Controller in derselben DR-Gruppe sollten während des gleichen Wartungszeitraums aktualisiert werden.

  Das Bebetreiben der MetroCluster-Konfiguration mit unterschiedlichen Controller-Typen in derselben DR-Gruppe wird außerhalb dieser Wartungsaktivitäten nicht unterstützt. Bei MetroCluster Konfigurationen mit acht Nodes müssen die Controller in einer DR-Gruppe identisch sein. Jedoch können beide DR-Gruppen unterschiedliche Controller-Typen verwenden.

- Für eine vorab-Zuordnung von Storage-, FC- und Ethernet-Verbindungen zwischen Original-Nodes und neuen Nodes wird empfohlen.
- Wenn die neue Plattform weniger Steckplätze als das ursprüngliche System besitzt oder weniger oder unterschiedliche Ports vorhanden sind, müssen Sie dem neuen System möglicherweise einen Adapter hinzufügen.

  Weitere Informationen finden Sie im "NetApp Hardware Universe"

Folgende Beispielnamen werden in diesem Verfahren verwendet:

- Standort_A
  - Vor dem Upgrade:
    - Node_A_1-alt
    - Node_A_2-alt
  - Nach dem Upgrade:
    - Node_A_1-neu
    - Node_A_2-neu
- Standort_B
  - Vor dem Upgrade:
    - Node_B_1-alt
    - Node_B_2-alt
  - Nach dem Upgrade:
    - Node_B_1-neu
    - Node_B_2-neu

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren

und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Bereiten Sie sich auf das Upgrade vor

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die neuen Plattformen vorbereiten und andere verschiedene Aufgaben ausführen.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Sie überprüfen den Zustand und die Konnektivität der MetroCluster-Konfiguration, bevor Sie das Upgrade durchführen.

> Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:

   a. Prüfen Sie, ob die Knoten multipathed sind:
   `node run -node node-name sysconfig -a`

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

   ```
   storage disk show -broken
   ```

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   c. Überprüfen Sie auf Statusmeldungen:

   ```
   system health alert show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

```
system license show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

f. Vergewissern Sie sich, dass Zeitzone und Uhrzeit auf beiden Standorten korrekt eingestellt sind:

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

2. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

3. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.

a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:

```
metrocluster node show
```

c. Geben Sie den folgenden Befehl ein:

```
metrocluster check run
```

d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

4. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.

a. Laden Sie Config Advisor herunter und führen Sie sie aus.

"NetApp Downloads: Config Advisor"

b. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

Weisen Sie den neuen Nodes Ports von den alten Nodes zu

Sie müssen die Zuordnung der LIFs zu physischen Ports auf den alten Nodes zu den physischen Ports auf den neuen Nodes planen.

Über diese Aufgabe

Wenn der neue Node zum ersten Mal während des Upgrades gebootet wird, stellt er die aktuellste Konfiguration des alten Node wieder dar, der ersetzt wird. Wenn Sie Node_A_1-New booten, versucht ONTAP, LIFs auf denselben Ports zu hosten, die in Node_A_1-old verwendet wurden. Deshalb müssen Sie im Rahmen des Upgrades die Port- und LIF-Konfiguration anpassen, sodass diese mit der der des alten Node kompatibel ist. Während des Upgrades führen Sie sowohl für die alten als auch für die neuen Nodes Schritte durch, um eine korrekte Cluster-, Management- und Daten-LIF-Konfiguration sicherzustellen.

Die folgende Tabelle zeigt Beispiele für Konfigurationsänderungen in Bezug auf die Portanforderungen der neuen Nodes.

Physische Ports für Cluster-Interconnect		
Alter Controller	Neuer Controller	Erforderliche Maßnahme
e0a, e0b	e3a, e3b	Kein passender Port. Erstellen Sie nach dem Upgrade die Clusterports neu. "Bereiten Sie Cluster-Ports auf einem vorhandenen Controller-Modul vor"
e0c, e0d	e0a, e0b, e0c, e0d	e0c und e0d sind passende Anschlüsse. Sie müssen die Konfiguration nicht ändern, aber nach einem Upgrade können Sie die Cluster-LIFs über die verfügbaren Cluster-Ports verteilen.

Schritte

1. Legen Sie fest, welche physischen Ports auf den neuen Controllern verfügbar sind und welche LIFs auf den Ports gehostet werden können.

   Die Port-Nutzung des Controllers hängt vom Plattformmodul ab und welche Switches Sie in der MetroCluster IP-Konfiguration verwenden werden. Sie können die Port-Nutzung der neuen Plattformen von erfassen "NetApp Hardware Universe".

   Identifizieren Sie außerdem die Auslastung des FC-VI-Kartensteckplatzes.

2. Planen Sie Ihre Portnutzung und füllen Sie auf Wunsch die folgenden Tabellen als Referenz für jeden der neuen Nodes aus.

   Sie verweisen auf die Tabelle, während Sie das Upgrade-Verfahren durchführen.

	Node_A_1-alt			Node_A_1-neu		
LIF	Ports	IPspaces	Broadcast-Domänen	Ports	IPspaces	Broadcast-Domänen
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						

Node-Management						
Cluster-Management						
Daten 1						
Daten 2						
Daten 3						
Daten 4						
San						
Intercluster-Port						

Sammeln Sie vor dem Upgrade Informationen

Vor der Aktualisierung müssen Sie Informationen für jeden der alten Knoten erfassen und bei Bedarf die Netzwerk-Broadcast-Domänen anpassen, VLANs und Schnittstellengruppen entfernen und Verschlüsselungsinformationen sammeln.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel der vorhandenen Controller, damit Sie beim Einrichten der neuen Controller Kabel problemlos identifizieren können.
2. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260
   - Node_B_1-alt: 4068741254
   - Node_B_2-alt: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                       node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------- ------------------
-------------                  -------------------
-------------------              ---------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                       4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                       4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                        4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                       4068741260
4068741258
4 entries were displayed.
```

In diesem Beispiel für eine MetroCluster FC-Konfiguration mit zwei Nodes werden die folgenden alten System-IDs abgerufen:

- Node_A_1: 4068741258
- Knoten_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*

- `network port ifgrp show -node node_name -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

4. Wenn sich die MetroCluster-Nodes in einer SAN-Konfiguration befinden, sammeln Sie die relevanten Informationen.

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

   ```
   security key-manager backup show
   ```

6. Wenn die MetroCluster Nodes Verschlüsselung für Volumes oder Aggregate nutzen, kopieren Sie Informationen zu Schlüsseln und Passphrases.

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen".

   a. Wenn Onboard Key Manager konfiguriert ist:

      ```
      security key-manager onboard show-backup
      ```

      Sie benötigen die Passphrase später im Upgrade-Verfahren.

   b. Wenn das Enterprise-Verschlüsselungsmanagement (KMIP) konfiguriert ist, geben Sie die folgenden Befehle ein:

      ```
      security key-manager external show -instance
      ```

   ```
   security key-manager key query
   ```

Entfernen Sie die vorhandene Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "MetroCluster-Konfigurationen entfernen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit die Wartung läuft.

   a. Geben Sie den folgenden Befehl ein:

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` Gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Wiederholen Sie den Befehl im Partner-Cluster.

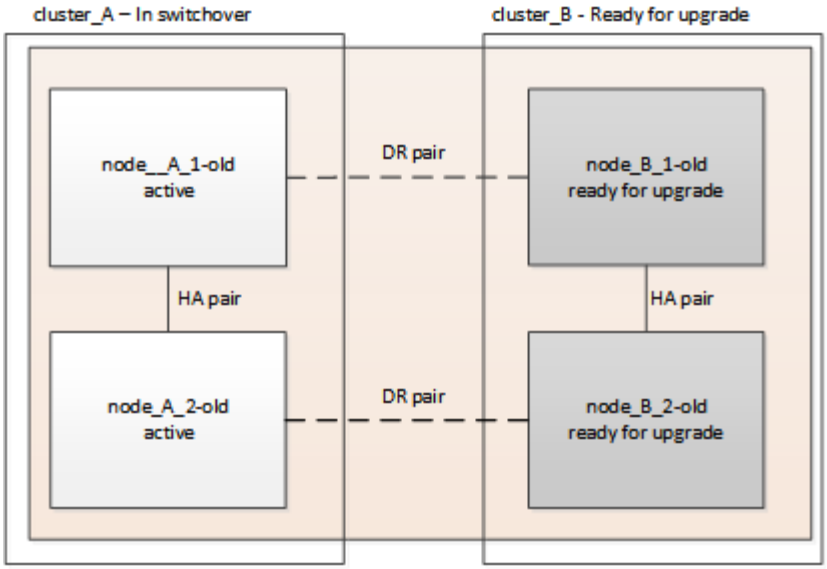
Wechseln Sie über die MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Cluster_A aktiv und stellt Daten für beide Standorte bereit. Cluster_B ist inaktiv und bereit, den Upgrade-Prozess zu starten, wie in der folgenden Abbildung dargestellt.



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Wählen Sie die Option aus, die Ihrer Konfiguration entspricht, und geben Sie den korrekten Befehl auf Cluster_A aus:

   > **Option 1: FC-Konfiguration mit vier oder acht Nodes und ONTAP 9.8 oder höher**
   >
   > Führen Sie den Befehl aus: `metrocluster switchover -controller-replacement true`
   >
   > **Option 2: FC-Konfiguration mit zwei Nodes und ONTAP 9.3 und höher**
   >
   > Führen Sie den Befehl aus: `metrocluster switchover`

   Der Vorgang kann einige Minuten dauern.

   b. Überwachen Sie den Switchover-Betrieb:

   ```
   metrocluster operation show
   ```

   c. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

   ```
   metrocluster show
   ```

   d. Den Status der MetroCluster-Knoten überprüfen:

   ```
   metrocluster node show
   ```

2. Heilen Sie die Datenaggregate.

   a. Heilen der Datenaggregate:

   ```
   metrocluster heal data-aggregates
   ```

   b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster`

`operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Heilen Sie die Root-Aggregate.
   a. Heilen der Datenaggregate:

      ```
      metrocluster heal root-aggregates
      ```

   b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

      ```
      cluster_A::> metrocluster operation show
        Operation: heal-root-aggregates
            State: successful
       Start Time: 7/29/2020 20:58:41
         End Time: 7/29/2020 20:59:42
           Errors: -
      ```

Vorbereiten der Netzwerkkonfiguration der alten Controller

Um sicherzustellen, dass das Netzwerk auf den neuen Controllern ordnungsgemäß fortgesetzt wird, müssen Sie LIFs auf einen gemeinsamen Port verschieben und dann die Netzwerkkonfiguration der alten Controller entfernen.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie verwenden die in erfassten Informationen "Zuordnen von Ports von den alten Nodes zu den neuen Nodes".

Schritte

1. Booten Sie die alten Nodes, und melden Sie sich dann bei den Nodes an:

   ```
   boot_ontap
   ```

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      ```
      network interface show
      ```

Alle Daten-LIFS einschließlich SAN und NAS befinden sich in Betrieb, da sie sich am Switchover-Standort (Cluster_A) befinden.

b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

   e0d ist zum Beispiel ein physischer Port auf den alten Controllern und ist auch auf neuen Controllern vorhanden. e0d wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

   Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

   Im folgenden Beispiel ist dies "e0d".

   Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Ändern Sie Broadcast-Domänen, um vlan und physische Ports zu entfernen, die gelöscht werden müssen:

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Wiederholen Sie diesen Schritt für alle VLAN- und physischen Ports.

4. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und ifgrps, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

   b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

      `network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

      Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

   a. Entfernen Sie VLAN und Interface Group Ports aus Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Anhalten der Knoten:

```
halt -inhibit-takeover true -node node-name
```

Dieser Schritt muss auf beiden Knoten durchgeführt werden.

Entfernen Sie die alten Plattformen

Die alten Controller müssen aus der Konfiguration entfernt werden.

Über diese Aufgabe

Diese Aufgabe wird auf Site_B. ausgeführt

Schritte

1. Stellen Sie eine Verbindung mit der seriellen Konsole der alten Controller (Node_B_1-old und Node_B_2-old) an Site_B her, und überprüfen Sie, dass die LOADER-Eingabeaufforderung angezeigt wird.
2. Trennen Sie die Speicher- und Netzwerkverbindungen auf Node_B_1-old und Node_B_2-old, und kennzeichnen Sie die Kabel, damit sie wieder mit den neuen Nodes verbunden werden können.
3. Trennen Sie die Stromkabel von Node_B_1-old und Node_B_2-old.
4. Entfernen Sie die Controller Node_B_1-old und Node_B_2-old aus dem Rack.

Konfigurieren Sie die neuen Controller

Sie müssen die Controller im Rack unterbringen und installieren, die erforderliche Einrichtung im Wartungsmodus durchführen und dann die Controller booten und die LIF-Konfiguration auf den Controllern überprüfen.

Richten Sie die neuen Controller ein

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Wenn die neuen Controller-Module nicht eigene FC-VI-Karten enthalten und FC-VI-Karten von alten

Controllern mit neuen Controllern kompatibel sind, tauschen Sie FC-VI-Karten aus und installieren Sie diese in den richtigen Steckplätzen.

Siehe "NetApp Hardware Universe" Für Slot-Informationen für FC-VI-Karten.

5. Verkabeln Sie die Strom-, seriellen Konsolen- und Managementverbindungen der Controller, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

   Schließen Sie derzeit keine anderen Kabel an, die von den alten Controllern getrennt wurden.

   "Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Eingabeaufforderung Strg-C, um die LOADER-Eingabeaufforderung anzuzeigen.

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	Extrahieren Sie den Inhalt der ontap-Version_image.tgzfile in das Zielverzeichnis: Tar -zxvf ontap-Version_image.tgz HINWEIS: Wenn Sie den Inhalt auf Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot Image zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: ontap-Version_image.tgz Sie müssen nicht die ontap-Version_image.tgz-Datei extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

```
ifconfig e0M -auto
```

- Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

```
ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Wählen Sie im Startmenü die Option **(7) Neue Software zuerst installieren** aus, um das neue Software-Image auf das Boot-Gerät herunterzuladen und zu installieren.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein
   `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie
   die URL der Bilddatei ein: `\http://web_server_ip/path_to_web-
   accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Starten Sie den Neustart durch Eingabe `y` Wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

Löschen Sie die Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

   ```
   boot_ontap menu
   ```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`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`

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   der HA-Status für alle Komponenten sollte mcc sein.

Wenn die MetroCluster-Konfiguration…	Der HA-Status sollte…
Zwei Nodes	mcc-2n
Vier oder acht Nodes	mcc

2. Wenn der angezeigte Systemzustand des Controllers nicht richtig ist, setzen Sie den HA-Status für das Controller-Modul und das Chassis:

Wenn die MetroCluster-Konfiguration…	Geben Sie diese Befehle ein…

Zwei Knoten	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Vier oder acht Knoten	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln Sie vor dem Upgrade Informationen".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Beenden Sie das System und das Booten in den Wartungsmodus von der LOADER-Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

   Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   `disk reassign -s old-sysid -d new-sysid`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status           Options
   aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                            mirrored
   mirror_resync_priority=high(fixed)
                            fast zeroed
                            64-bit
   ```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

4. Wenn Sie die Stammverschlüsselung verwenden, wählen Sie je nach der verwendeten ONTAP-Version die Startmenü-Option oder geben Sie den Startmenü-Befehl für Ihre Konfiguration für die Schlüsselverwaltung aus.

ONTAP 9.8 und höher

Ab ONTAP 9.8 wählen Sie die Startmenü-Option.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

ONTAP 9.7 und frühere Versionen

Geben Sie bei ONTAP 9.7 und früheren Versionen den Befehl des Startmenüs ein.

Sie verwenden…	Geben Sie diesen Befehl an der Eingabeaufforderung des Startmenüs aus…
Integriertes Verschlüsselungsmanagement	`recover_onboard_keymanager`
Externes Verschlüsselungskeymanagement	`recover_external_keymanager`

5. Wenn Autoboot aktiviert ist, unterbrechen Sie den Autoboot, indem Sie STRG-C. drücken
6. Führen Sie im Startmenü die Option „`6`“ aus.

   Mit der Option „`6`“ wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist:

   `printenv partner-sysid`

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

```
setenv partner-sysid partner-sysID
```

8. Wenn Sie die Stammverschlüsselung verwenden, wählen Sie je nach der verwendeten ONTAP-Version die Startmenü-Option oder geben Sie den Startmenü-Befehl für Ihre Konfiguration für das Verschlüsselungsmanagement erneut aus.

   ONTAP 9.8 und höher

   Ab ONTAP 9.8 wählen Sie die Startmenü-Option.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

   Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „`6`“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

   ONTAP 9.7 und frühere Versionen

   Geben Sie bei ONTAP 9.7 und früheren Versionen den Befehl des Startmenüs ein.

Sie verwenden…	Geben Sie diesen Befehl an der Eingabeaufforderung des Startmenüs aus…
Integriertes Verschlüsselungsmanagement	`recover_onboard_keymanager`
Externes Verschlüsselungskeymanagement	`recover_external_keymanager`

   Möglicherweise müssen Sie die ausgeben `recover_xxxxxxxx_keymanager` Befehl wird mehrmals am Boot-Menü angezeigt, bis die Nodes vollständig gebootet werden.

9. Starten der Knoten:

   ```
   boot_ontap
   ```

10. Warten Sie, bis die ersetzten Nodes gestartet werden.

Führen Sie ein Giveback durch, wenn sich einer der beiden Knoten im Übernahmemodus befindet:

```
storage failover giveback
```

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

    ```
    network port broadcast-domain show
    ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

    "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast Domain hostet.

    d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

    e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

    Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

    "Erstellen einer Cluster-Peer-Beziehung"

    f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

    VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

    "Erstellen Sie eine VLAN"

    "Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen"

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

LIF-Konfiguration überprüfen

Stellen Sie vor dem Wechsel sicher, dass LIFs auf den entsprechenden Nodes/Ports gehostet werden. Folgende Schritte sind auszuführen

Über diese Aufgabe

Diese Aufgabe wird in Site_B ausgeführt, wo die Nodes mit Root-Aggregaten gestartet wurden.

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Wenn Sie den eingeben `network interface modify` Befehl im `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können die erstellen `network interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

   a. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   ```
   network interface revert * -vserver vserver-name
   ```

   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Installieren Sie die neuen Lizenzen

Vor dem Wechsel-Back-Vorgang müssen Sie Lizenzen für die neuen Controller installieren.

Schritte

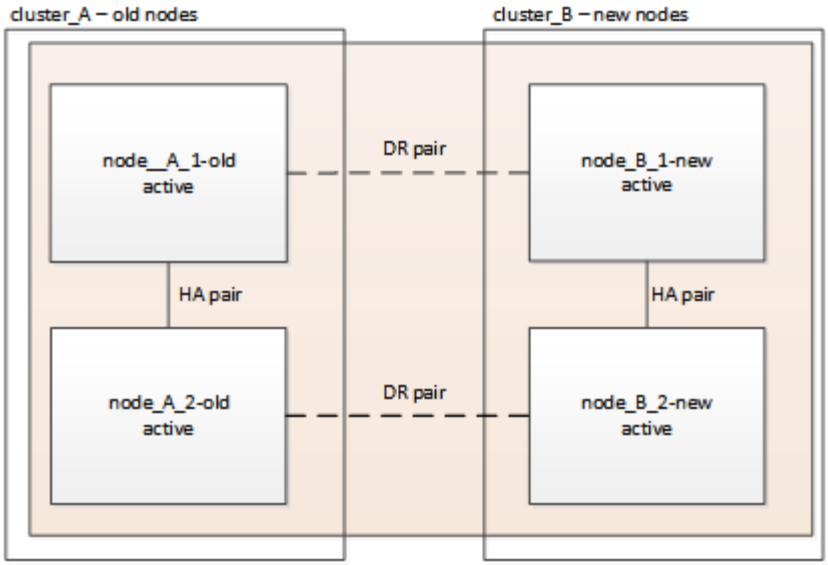
1. "Installieren von Lizenzen für das neue Controller-Modul"

Schalten Sie die MetroCluster-Konfiguration zurück

Nachdem die neuen Controller konfiguriert wurden, schalten Sie die MetroCluster Konfiguration zurück und kehren den normalen Betrieb zurück.

Über diese Aufgabe

In dieser Aufgabe führen Sie den Vorgang zum Zurückkehren aus und kehren die MetroCluster-Konfiguration in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade.



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.
   a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
   b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.
2. Zurückwechseln des Clusters:

   ```
   metrocluster switchback
   ```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

   ```
   cluster_B::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_B         Configuration state configured
                             Mode                switchover
                             AUSO Failure Domain -
   Remote: cluster_A         Configuration state configured
                             Mode                waiting-for-switchback
                             AUSO Failure Domain -
   ```

   Der Umkehrvorgang ist abgeschlossen, wenn die Ausgabe angezeigt wird `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:

   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

   ```
   metrocluster show
   ```

   b. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   > Nach dem Ausführen von `metrocluster check run` Und `metrocluster check show`, Sie sehen eine Fehlermeldung ähnlich der folgenden:

Beispiel

```
Failed to validate the node and cluster components before the switchover
operation.
                  Cluster_A:: node_A_1 (non-overridable veto): DR
partner NVLog mirroring is not online. Make sure that the links between
the two sites are healthy and properly configured.
```

+
Dieses Verhalten wird aufgrund einer Controller-Diskrepanz während des Upgrade-Prozesses erwartet und die Fehlermeldung kann sicher ignoriert werden.

Aktualisieren Sie die Nodes auf Cluster_A

Sie müssen die Upgrade-Aufgaben auf „Cluster_A“ wiederholen

Schritt

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit "Bereiten Sie sich auf das Upgrade vor".

   Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Cluster_A verwendet wird, erfolgt die Umschaltung von Cluster_B.

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritt

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
   a. Geben Sie den folgenden Befehl ein:

      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```

   b. Wiederholen Sie den Befehl im Partner-Cluster.

Wiederherstellung des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Fügen Sie MetroCluster-Konfigurationen hinzu" in *Installation und Konfiguration des MetroCluster-Tiebreakers*.

Controller-Upgrade von AFF A700/FAS9000 auf AFF A900/FAS9500 in einer MetroCluster FC-Konfiguration mittels Umschaltung und Switchback (ONTAP 9.10.1 oder höher)

Mit dem MetroCluster Switchover profitieren Kunden von unterbrechungsfreiem Service, während die Controller-Module im Partner-Cluster aktualisiert werden. Im Rahmen dieses Verfahrens können Sie keine weiteren Komponenten (z. B. Storage Shelves oder Switches) aktualisieren.

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Sie können keine anderen Komponenten in der Konfiguration, wie Storage Shelfs oder Switches, gleichzeitig aktualisieren.

- Sie können dieses Verfahren zum Upgrade einer AFF A700 auf AFF A900 mit ONTAP 9.10.1 oder höher verwenden.
- Sie können dieses Verfahren zum Upgrade einer FAS9000 auf FAS9500 mit ONTAP 9.10.1P3 und höher verwenden.
  - In ONTAP 9.10.1 und höher werden Konfigurationen mit vier und acht Nodes unterstützt.

    Das AFF A900 System wird nur ab ONTAP 9.10.1 unterstützt.

  "NetApp Hardware Universe"

- Upgrades für alle Controller der Konfiguration sollten während des gleichen Wartungszeitraums durchgeführt werden.

  In der folgenden Tabelle ist die unterstützte Modellmatrix für das Controller-Upgrade aufgeführt.

Altes Plattform-Modell	Neues Plattformmodell
• AFF A700	• AFF A900
• FAS9000	• FAS9500

- Während des Upgrade-Verfahrens müssen Sie die MetroCluster Fabric ändern, einschließlich RCF und physischen Kabeländerungen. Sie können die RCF- und Verkabelungsänderungen durchführen, bevor Sie die Controller-Aktualisierung durchführen.
- Für dieses Upgrade sind keine Änderungen der Storage-, FC- und Ethernet-Verbindungen zwischen den ursprünglichen Nodes und den neuen Nodes erforderlich.
- Während des Upgrades sollten Sie keine anderen Karten zum AFF A700 oder FAS9000 System hinzufügen oder entfernen. Weitere Informationen finden Sie im "NetApp Hardware Universe"

Folgende Beispielnamen werden in Beispielen und Grafiken in diesem Verfahren verwendet:

- Standort_A
  - Vor dem Upgrade:
    - Node_A_1-A700
    - Node_A_2-A700
  - Nach dem Upgrade:
    - Node_A_1-A900
    - Node_A_2-A900
- Standort_B
  - Vor dem Upgrade:
    - Node_B_1-A700

        - Node_B_2-A700
    - Nach dem Upgrade:
        - Node_B_1-A900
        - Node_B_2-A900

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Bereiten Sie sich auf das Upgrade vor

Bevor Sie Änderungen an der bestehenden MetroCluster Konfiguration vornehmen, müssen Sie den Zustand der Konfiguration überprüfen, die RCF-Dateien und die Verkabelung mit der neuen für die AFF A900 oder FAS9000 Fabric MetroCluster-Konfiguration erforderlichen Port-Konnektivitätstopologie abstimmen und weitere verschiedene Aufgaben ausführen.

Steckplatz 7 am AFF A700 Controller löschen

Die MetroCluster Konfiguration auf einem AFF A900 oder FAS9500 erfordert 8 FC-VI-Ports über FC-VI-Karten in den Steckplätzen 5 und 7. Wenn beim AFF A700 oder der FAS9000 Karten in Steckplatz 7 vorhanden sind, müssen Sie die Karten in andere Steckplätze für alle Nodes des Clusters verschieben.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Bevor Sie die RCF-Dateien und die Verkabelung für die Fabric MetroCluster-Konfiguration von AFF A900 oder FAS9500 aktualisieren, müssen Sie den Zustand und die Konnektivität der Konfiguration überprüfen.

> Nachdem Sie die Controller am ersten Standort aktualisiert haben und bevor Sie den zweiten aktualisieren, wird ausgeführt `metrocluster check run` gefolgt von `metrocluster check show` gibt einen Fehler zurück in der `config-replication` Feld. Dieser Fehler weist auf eine Nichtübereinstimmung der NVRAM-Größe zwischen den Knoten an jedem Standort hin und ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind. Sie können den Fehler ignorieren, bis das Controller-Upgrade für alle Knoten in der DR-Gruppe abgeschlossen ist.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:

    a. Prüfen Sie, ob die Knoten multipathed sind:

```
node run -node node-name sysconfig -a
```

Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

```
storage disk show -broken
```

Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

c. Überprüfen Sie auf Statusmeldungen:

```
system health alert show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

d. Überprüfen Sie die Lizenzen auf den Clustern:

```
system license show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

```
network device-discovery show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

f. Vergewissern Sie sich, dass Zeitzone und Uhrzeit auf beiden Standorten korrekt eingestellt sind:

```
cluster date show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

2. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

```
storage switch show
```

Sie sollten diesen Befehl für jedes Cluster ausgeben.

3. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.

a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

```
metrocluster show
```

b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:

```
metrocluster node show
```

c. Geben Sie den folgenden Befehl ein:

```
metrocluster check run
```

d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

4. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.
   a. Laden Sie Config Advisor herunter und führen Sie sie aus.

      "NetApp Downloads: Config Advisor"

   b. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

Aktualisieren Sie die RCF-Dateien des Fabric Switch

Für die AFF A900 oder FAS9500 Fabric MetroCluster sind zwei FC-VI-Adapter mit vier Ports pro Node erforderlich, im Vergleich zu einem FC-VI-Adapter mit vier Ports, den eine AFF A700 benötigt. Bevor Sie das Controller-Upgrade auf den AFF A900 oder FAS9500 Controller starten, müssen Sie die Fabric Switch RCF-Dateien ändern, um die AFF A900 oder FAS9500 Verbindungstopologie zu unterstützen.

1. Von "Download-Seite für MetroCluster RCF-Dateien", Laden Sie die korrekte RCF-Datei für ein AFF A900 oder FAS9500 Fabric MetroCluster sowie das Switch-Modell herunter, das in der AFF A700 oder FAS9000 Konfiguration verwendet wird.
2. Aktualisieren Sie die RCF-Datei auf den Fabric-A-Schaltern, wechseln Sie A1 und wechseln Sie B1, indem Sie die Schritte unter befolgen "Konfigurieren der FC-Switches".

   > Das RCF-Dateiupdate zur Unterstützung der AFF A900 oder FAS9500 Fabric MetroCluster-Konfiguration hat keine Auswirkungen auf die Ports und Verbindungen, die für die Konfiguration der AFF A700 oder FAS9000 Fabric MetroCluster verwendet werden.

3. Nach Aktualisierung der RCF-Dateien auf den Fabric A Switches sollten alle Storage- und FC-VI-Verbindungen online geschaltet werden. Prüfen Sie die FC-VI-Verbindungen:

   ```
   metrocluster interconnect mirror show
   ```

   a. Vergewissern Sie sich, dass die lokalen und Remote-Standortlaufwerke in aufgeführt sind `sysconfig` Ausgabe:
4. nach der RCF-Dateiaktualisierung für Fabric A-Switches müssen Sie überprüfen, ob sich MetroCluster in einem ordnungsgemäßen Zustand befindet.
   a. Verbindungen des Metro-Clusters prüfen:
      `metrocluster interconnect mirror show`
   b. MetroCluster-Prüfung ausführen:
      `metrocluster check run`
   c. Nach Abschluss des Laufes sind die Ergebnisse der MetroCluster-Ausführung zu sehen:
      `metrocluster check show`
5. Aktualisieren Sie die Fabric-B-Schalter (Schalter 2 und 4), indem Sie sich wiederholen Schritt 2 Bis Schritt 5.

Überprüfen Sie nach dem Update der RCF-Datei den Zustand der MetroCluster-Konfiguration

Sie müssen den Zustand und die Konnektivität der MetroCluster Konfiguration überprüfen, bevor Sie das

Upgrade durchführen.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:

   a. Prüfen Sie, ob die Knoten multipathed sind:
   `node run -node node-name sysconfig -a`

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   b. Vergewissern Sie sich, dass in der Konfiguration keine defekten Festplatten vorhanden sind:

   ```
   storage disk show -broken
   ```

   Sie sollten diesen Befehl für jeden Node in der MetroCluster-Konfiguration ausgeben.

   c. Überprüfen Sie auf Statusmeldungen:

   ```
   system health alert show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

   d. Überprüfen Sie die Lizenzen auf den Clustern:

   ```
   system license show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

   e. Überprüfen Sie die mit den Knoten verbundenen Geräte:

   ```
   network device-discovery show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

   f. Vergewissern Sie sich, dass Zeitzone und Uhrzeit auf beiden Standorten korrekt eingestellt sind:

   ```
   cluster date show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben. Sie können das verwenden `cluster date` Befehle zum Konfigurieren der Zeit- und Zeitzone.

2. Prüfen Sie, ob auf den Switches Zustandswarnmeldungen vorliegen (falls vorhanden):

   ```
   storage switch show
   ```

   Sie sollten diesen Befehl für jedes Cluster ausgeben.

3. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.

   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

   ```
   metrocluster show
   ```

   b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:

```
metrocluster node show
```

c. Geben Sie den folgenden Befehl ein:

```
metrocluster check run
```

d. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

4. Prüfen Sie die MetroCluster-Verkabelung mit dem Tool Config Advisor.
   a. Laden Sie Config Advisor herunter und führen Sie sie aus.

      "NetApp Downloads: Config Advisor"

   b. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

Zuordnung der Ports des AFF A700 oder FAS9000 Nodes zu den AFF A900 oder FAS9500 Nodes

Während des Controller-Upgrades dürfen nur die in diesem Verfahren erwähnten Verbindungen geändert werden.

Wenn die AFF A700 oder FAS9000 Controller über eine Karte in Steckplatz 7 verfügen, sollten Sie sie in einen anderen Steckplatz verschieben, bevor Sie das Controller-Upgrade durchführen. Sie müssen Steckplatz 7 für die Hinzufügung des zweiten FC-VI-Adapters besitzen, der für die Funktionsweise von Fabric MetroCluster auf den AFF A900 oder FAS9500 Controllern erforderlich ist.

Sammeln Sie vor dem Upgrade Informationen

Vor der Aktualisierung müssen Sie Informationen für jeden der alten Knoten erfassen und bei Bedarf die Netzwerk-Broadcast-Domänen anpassen, VLANs und Schnittstellengruppen entfernen und Verschlüsselungsinformationen sammeln.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Erfassen der System-IDs für die MetroCluster-Konfiguration-Nodes:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-A700: 537037649
   - Node_A_2-A700: 537407030
   - Node_B_1-A700: 0537407114
   - Node_B_2-A700: 537035354

```
Cluster_A::*> metrocluster node show -fields node-systemid,ha-partner-
systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id cluster    node           node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ------------------------- ------------- -------------------
------------------- ---------------------
1           Cluster_A  nodeA_1-A700   537407114     537035354
537411005           537410611
1           Cluster_A  nodeA_2-A700   537035354     537407114
537410611           537411005
1           Cluster_B  nodeB_1-A700   537410611     537411005
537035354           537407114
1           Cluster_B  nodeB_2-A700   537411005

4 entries were displayed.
```

2. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node` *`node-name`* `sysconfig -a`

3. Wenn sich die MetroCluster-Nodes in einer SAN-Konfiguration befinden, sammeln Sie die relevanten Informationen.

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

4. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

```
security key-manager backup show
```

5. Wenn die MetroCluster Nodes Verschlüsselung für Volumes oder Aggregate nutzen, kopieren Sie Informationen zu Schlüsseln und Passphrases.

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen".

   a. Wenn Onboard Key Manager konfiguriert ist:

      ```
      security key-manager onboard show-backup
      ```

      Sie benötigen die Passphrase später im Upgrade-Verfahren.

   b. Wenn das Enterprise-Verschlüsselungsmanagement (KMIP) konfiguriert ist, geben Sie die folgenden Befehle ein:

      ```
      security key-manager external show -instance
      ```

```
security key-manager key query
```

Entfernen Sie die vorhandene Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen anderer Anbieter (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration vor dem Umstieg aus dem Tiebreaker oder einer anderen Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration über die Tiebreaker Software.

   "Entfernen von MetroCluster-Konfigurationen"

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Senden Sie vor der Wartung eine individuelle AutoSupport Nachricht

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit die Wartung läuft.

   a. Geben Sie den folgenden Befehl ein:

      ```
      system node autosupport invoke -node * -type all -message MAINT=maintenance-
      ```

window-in-hours

`maintenance-window-in-hours` Gibt die Länge des Wartungsfensters an, mit maximal 72 Stunden. Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Wiederholen Sie den Befehl im Partner-Cluster.

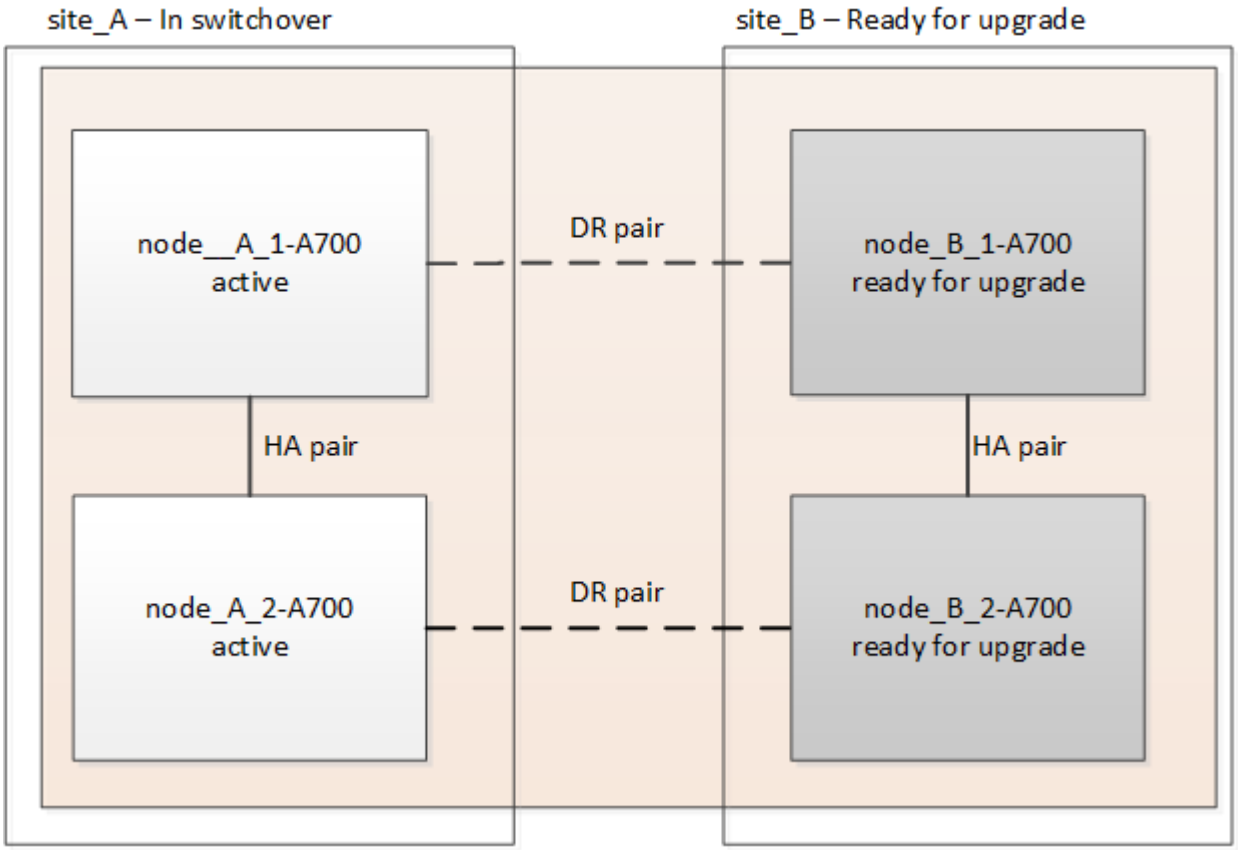
Wechseln Sie über die MetroCluster-Konfiguration

Sie müssen die Konfiguration auf Site_A umschalten, damit die Plattformen auf Site_B aktualisiert werden können.

Über diese Aufgabe

Diese Aufgabe muss auf Site_A ausgeführt werden

Nach Abschluss dieser Aufgabe ist Site_A aktiv und stellt Daten für beide Standorte bereit. Site_B ist inaktiv und bereit, den Upgrade-Prozess zu starten, wie in der folgenden Abbildung dargestellt. (Diese Abbildung gilt auch für das Upgrade einer FAS9000 auf einen FAS9500 Controller.)



Schritte

1. Wechseln Sie über die MetroCluster-Konfiguration zu Site_A, damit Site_B-Knoten aktualisiert werden können:

   a. Geben Sie den folgenden Befehl auf Site_A aus:

```
metrocluster switchover -controller-replacement true
```

Der Vorgang kann einige Minuten dauern.

a. Überwachen Sie den Switchover-Betrieb:

```
metrocluster operation show
```

b. Nach Abschluss des Vorgangs bestätigen Sie, dass die Nodes sich im Switchstatus befinden:

```
metrocluster show
```

c. Den Status der MetroCluster-Knoten überprüfen:

```
metrocluster node show
```

2. Heilen Sie die Datenaggregate.

a. Heilen der Datenaggregate:

```
metrocluster heal data-aggregates
```

b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Heilen Sie die Root-Aggregate.

a. Heilen der Datenaggregate:

```
metrocluster heal root-aggregates
```

b. Bestätigen Sie, dass der Heilvorgang abgeschlossen ist, indem Sie den ausführen `metrocluster operation show` Befehl auf dem gesunden Cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul und den NVS an Site_B

Sie müssen die alten Controller aus der Konfiguration entfernen.

Sie führen diese Aufgabe auf Site_B. aus

Bevor Sie beginnen

Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Schritte

1. Stellen Sie eine Verbindung zur seriellen Konsole der alten Controller (Node_B_1-700 und Node_B_2-700) an Site_B her, und überprüfen Sie, ob der angezeigt wird `LOADER` Eingabeaufforderung:
2. Ermitteln Sie die Bootarg-Werte von beiden Knoten an Site_B: `printenv`
3. Schalten Sie das Chassis an Site_B. aus

Entfernen Sie das Controller-Modul und den NVS von beiden Nodes an Site_B

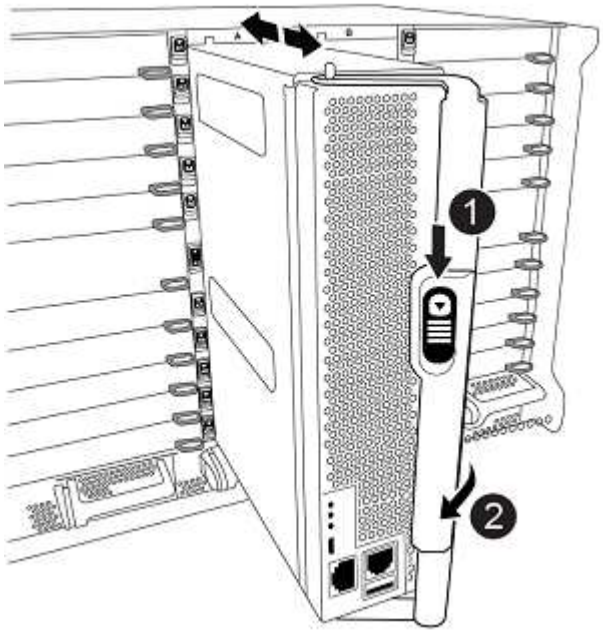
Entfernen Sie das AFF A700 oder das FAS9000 Controller-Modul

Gehen Sie wie folgt vor, um das AFF A700 oder das FAS9000 Controller-Modul zu entfernen.

Schritte

1. Trennen Sie gegebenenfalls das Konsolenkabel und das Managementkabel vom Controller-Modul, bevor Sie das Controller-Modul entfernen.
2. Entriegeln und entfernen Sie das Controller-Modul aus dem Gehäuse.

   a. Schieben Sie die orangefarbene Taste am Nockengriff nach unten, bis sie entsperrt ist.



1	Freigabetaste für den CAM-Griff

	CAM-Griff

a. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse. Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul

Entfernen Sie das AFF A700 oder das FAS9000 NVS-Modul wie folgt:

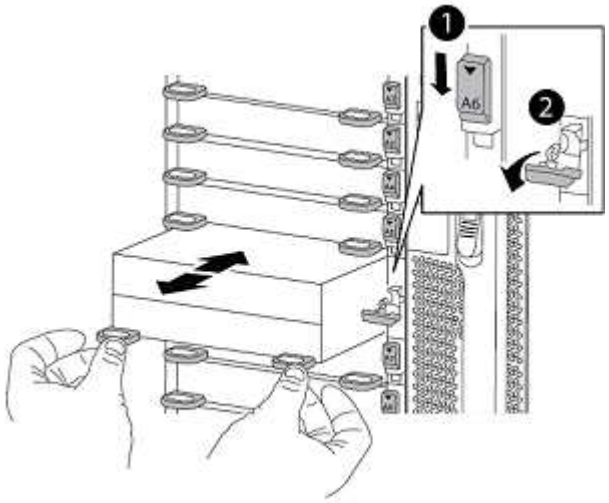
> Das AFF A700 oder FAS9000 NVS-Modul befindet sich in Steckplatz 6 und ist im Vergleich zu den anderen Modulen im System doppelt so hoch.

1. Entriegeln und entfernen Sie den NVS aus Steckplatz 6.

   a. Drücken Sie die Taste mit der Nummerierung und dem Buchstaben. Die Nockentaste bewegt sich vom Gehäuse weg.

   b. Drehen Sie die Nockenverriegelung nach unten, bis sie sich in horizontaler Position befindet. Der NVS löst sich aus dem Gehäuse und bewegt sich ein paar Zentimeter.

   c. Entfernen Sie den NVS aus dem Gehäuse, indem Sie an den Zuglaschen an den Seiten der Modulfläche ziehen.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

- Übertragen Sie keine Add-On-Module, die als Coredump-Geräte auf dem nichtflüchtigen Speichermodul AFF A700 in Steckplatz 6 verwendet werden, auf das AFF A900 NVS-Modul. Übertragen Sie keine Teile vom AFF A700-Controller und NVS-Modulen auf das AFF A900-Controller-Modul.
- Bei Upgrades von FAS9000 zu FAS9500 sollten Sie Flash Cache Module des FAS9000 NVS-Moduls nur in das FAS9500 NVS-Modul übertragen. Übertragen Sie keine anderen Teile vom FAS9000 Controller und NVS-Modulen auf das FAS9500 Controller-Modul.

Installieren Sie das AFF A900 oder FAS9500 NVS und das Controller-Modul

Sie müssen das AFF A900 oder FAS9500 NVS und das Controller-Modul aus dem Upgrade-Kit auf beiden Knoten in Site_B. installieren Verschieben Sie das coredump-Gerät nicht vom AFF A700 oder FAS9000 NVS-Modul in das AFF A900 oder FAS9500 NVS Modul.

Bevor Sie beginnen

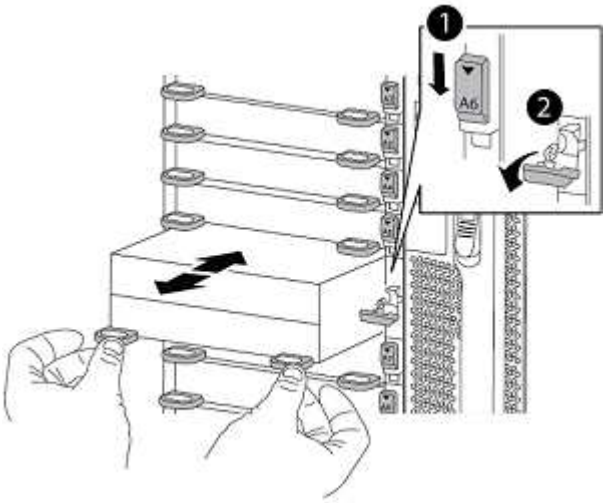
Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

Installieren Sie den AFF A900 oder FAS9500 NVS

Gehen Sie wie folgt vor, um den AFF A900 oder FAS9500 NVS in Steckplatz 6 beider Nodes an Site_B zu installieren

Schritte

1. Richten Sie den NVS an den Kanten der Gehäuseöffnung in Steckplatz 6 aus.
2. Schieben Sie den NVS vorsichtig in den Schlitz, bis der vorletzte und nummerierte E/A-Nockenriegel mit dem E/A-Nockenstift einrastet. Drücken Sie dann den E/A-Nockenverschluss bis zum Verriegeln des NVS.



	Gerettete und nummerierte E/A-Nockenverriegelung
	E/A-Riegel vollständig entriegelt

Installieren Sie das AFF A900 oder FAS9500 Controller-Modul

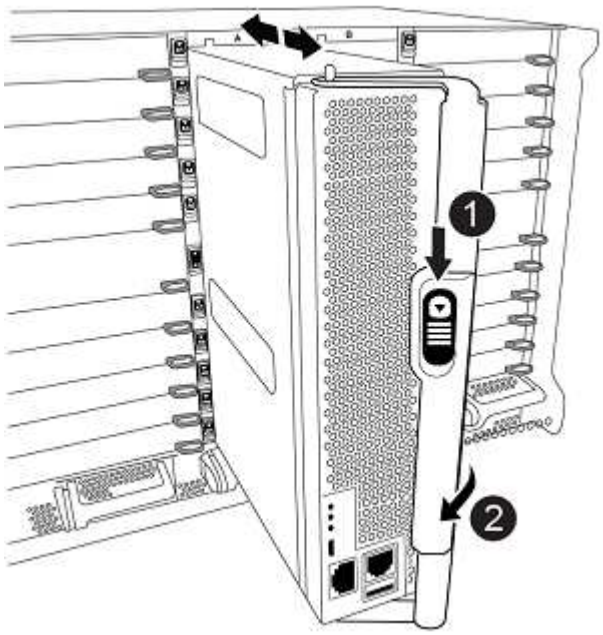
Gehen Sie wie folgt vor, um das AFF A900 oder FAS9500 Controller-Modul zu installieren.

Schritte

1. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
2. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt. Die Verriegelung steigt, wenn das Controller-Modul voll eingesetzt ist.

   > Beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden, um Schäden an den Anschlüssen zu vermeiden.

3. Verkabeln Sie die Management- und Konsolen-Ports mit dem Controller-Modul.



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

4. Installieren Sie die zweite X91129A-Karte in Steckplatz 7 jedes Knotens.
   a. Verbinden Sie die FC-VI-Ports aus Steckplatz 7 mit den Switches. Siehe "Installation und Konfiguration über Fabric-Attached Storage" Dokumentation und gehen Sie zu den AFF A900 oder FAS9500 Fabric MetroCluster Verbindungsanforderungen für den Switch-Typ in Ihrer Umgebung.
5. Schalten Sie das Chassis EIN, und verbinden Sie die serielle Konsole.
6. Wenn der Knoten nach der BIOS-Initialisierung den Autoboot startet, unterbrechen Sie DEN AUTOBOOT, indem Sie Control-C drücken
7. Nachdem Sie den Autoboot unterbrochen haben, werden die Nodes an der LOADER-Eingabeaufforderung angehalten. Wenn Sie die automatische Bootzeit nicht unterbrechen und node1 den Startvorgang startet, warten Sie, bis die Eingabeaufforderung Control-C drücken kann, um in das Startmenü zu gelangen. Nachdem der Node im Boot-Menü angehalten wurde, verwenden Sie Option 8, um den Node neu zu

booten und den Autoboot während des Neubootens zu unterbrechen.

8. Am `LOADER` Geben Sie die Standardvariablen für die Umgebung an: `set-defaults`
9. Speichern Sie die Standardeinstellungen für Umgebungsvariablen: `saveenv`

Netzboot der Nodes über Site_B

Nach Austausch des AFF A900 oder FAS9500 Controller-Moduls und der NVS müssen Sie die AFF A900 oder FAS9500 Nodes als Netzboot einsetzen. Die ONTAP-Version und die Patch-Ebene, die auf dem Cluster ausgeführt werden, müssen dann installiert werden. Laufzeit `netboot` Bedeutet, dass Sie von einem auf einem Remote-Server gespeicherten ONTAP Image booten. Bei der Vorbereitung auf `netboot`, Sie müssen eine Kopie des ONTAP 9-Startabbilds auf einem Webserver hinzufügen, auf den das System zugreifen kann.

Es ist nicht möglich, die auf den Boot-Medien eines AFF A900 oder FAS9500 Controller-Moduls installierte ONTAP Version zu überprüfen, es sei denn, sie ist in einem Chassis installiert und eingeschaltet. Die ONTAP Version auf dem AFF A900 oder FAS9500 Startmedium muss mit der ONTAP Version übereinstimmen, die auf dem AFF A700 oder FAS9000 System ausgeführt wird und bei dem Upgrade sowohl die Primär- als auch die Backup-Boot-Images übereinstimmen. Sie können die Bilder konfigurieren, indem Sie eine ausführen `netboot` Gefolgt von `wipeconfig` Befehl aus dem Startmenü. Wenn das Controller-Modul zuvor in einem anderen Cluster verwendet wurde, führt das aus `wipeconfig` Mit dem Befehl wird die Restkonfiguration auf dem Boot-Medium gelöscht.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie mit dem System auf einen HTTP-Server zugreifen können.
- Sie müssen die erforderlichen Systemdateien für Ihr System und die korrekte Version von ONTAP von der herunterladen "NetApp Support" Standort. Über diese Aufgabe müssen Sie wissen `netboot` Die neuen Controller, wenn die installierte ONTAP Version nicht mit der auf den ursprünglichen Controllern installierten Version identisch ist. Nachdem Sie jeden neuen Controller installiert haben, starten Sie das System über das auf dem Webserver gespeicherte ONTAP 9-Image. Anschließend können Sie die richtigen Dateien auf das Boot-Medium herunterladen, um später das System zu booten.

Schritte

1. Datenzugriff "NetApp Support" Zum Herunterladen der Dateien müssen Sie einen Netzboot zum Ausführen des Netzboots des Systems ausführen.
2. Laden Sie die entsprechende ONTAP Software im Software Download Bereich der NetApp Support Site herunter und speichern Sie die `<ontap_version>_image.tgz` Datei in einem webbasierten Verzeichnis.
3. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind. Ihre Verzeichnisliste sollte enthalten `<ontap_version>_image.tgz`.
4. Konfigurieren Sie die `netboot` Verbindung durch Auswahl einer der folgenden Aktionen. Hinweis: Sie sollten den Management-Port und die IP als verwenden `netboot` Verbindung. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn DHCP (Dynamic Host Configuration Protocol) lautet…	Dann…
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -auto`

Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> -dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` Ist die IP-Adresse des Storage-Systems. `<netmask>` Ist die Netzwerkmaske des Storage-Systems. `<gateway>` Ist das Gateway für das Storage-System. `<dns_addr>` Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. Dieser Parameter ist optional. `<dns_domain>` Der Domain Name (DNS) ist der Domain-Name. Dieser Parameter ist optional. HINWEIS: Andere Parameter können für Ihre Schnittstelle erforderlich sein. Geben Sie an der Firmware-Eingabeaufforderung die Hilfe ifconfig ein, um Details zu erhalten.

5. Performance `netboot` Bei Knoten 1:
`netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`Der `<path_to_the_web-accessible_directory>` Sollten Sie dazu führen, wo Sie das heruntergeladen haben `<ontap_version>_image.tgz` In Schritt 2.

   Unterbrechen Sie den Startvorgang nicht.

6. Warten Sie, bis Knoten 1 auf dem AFF A900 oder FAS9500 Controller-Modul ausgeführt wird, um die Startmenü-Optionen anzuzeigen, wie unten gezeigt:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

7. Wählen Sie im Startmenü Option `(7) Install new software first`. Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

> Ignorieren Sie die folgende Meldung: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`. Dieser Hinweis gilt für unterbrechungsfreie ONTAP Software-Upgrades und nicht für Controller-Upgrades. Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen.

8. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:

   ```
   http://<web_server_ip/path_to_web-
   accessible_directory>/<ontap_version>_image.tgz
   ```

9. Führen Sie die folgenden Teilschritte durch, um das Controller-Modul neu zu booten:
   a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:
      `Do you want to restore the backup configuration now? {y|n}`
   b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:
      `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`

      Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.

10. Führen Sie an der Eingabeaufforderung den aus `wipeconfig` Befehl zum Löschen einer früheren Konfiguration auf dem Startmedium:
    a. Wenn die folgende Meldung angezeigt wird, beantworten Sie die Antwort `yes`:
       ```
       This will delete critical system configuration, including cluster
       membership.
       Warning: do not run this option on a HA node that has been taken over.
       Are you sure you want to continue?:
       ```
    b. Der Node wird neu gebootet, um den abzuschließen `wipeconfig` Und hält dann am Startmenü an.

11. Wählen Sie die Option `5` Wechseln Sie vom Boot-Menü zum Wartungsmodus. Antwort `yes` Zu den Aufforderungen, bis der Node im Wartungsmodus und mit der Eingabeaufforderung angehalten wird `*>`.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:
   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`
   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`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`*

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   der HA-Status für alle Komponenten sollte mcc sein.

2. Wenn der angezeigte Systemzustand des Controllers oder Chassis nicht korrekt ist, setzen Sie den HA-Status ein:

   ```
   ha-config modify controller mcc
   ```

   ```
   ha-config modify chassis mcc
   ```

3. Stoppen Sie den Knoten: `halt`Der Node sollte am anhalten `LOADER>` Eingabeaufforderung:
4. Überprüfen Sie auf jedem Node das Systemdatum, die Uhrzeit und die Zeitzone: `Show date`
5. Stellen Sie bei Bedarf das Datum in UTC oder Greenwich Mean Time (GMT) ein: `set date <mm/dd/yyyy>`
6. Überprüfen Sie die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: `show time`
7. Stellen Sie bei Bedarf die Uhrzeit in UTC oder GMT ein: `set time <hh:mm:ss>`
8. Einstellungen speichern: `saveenv`
9. Umgebungsvariablen erfassen: `printenv`
10. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:
    `boot_ontap maint`
11. Überprüfen Sie, ob die Änderungen wirksam sind, und ucadmin zeigt FC Initiator-Ports online an.

Wenn Sie diesen Typ von HBA… haben	Verwenden Sie diesen Befehl…
CNA	`ucadmin show`
FC	`fcadmin show`

12. Überprüfen Sie den HA-config-Modus: `ha-config show`
    a. Stellen Sie sicher, dass Sie die folgende Ausgabe haben:

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Legen Sie den HA-Status für die neuen Controller und das Chassis fest

Sie müssen den HA-Status der Controller und des Chassis überprüfen. Bei Bedarf müssen Sie den Status entsprechend Ihrer Systemkonfiguration aktualisieren.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   `ha-config show`

   der HA-Status für alle Komponenten sollte mcc sein.

Wenn die MetroCluster-Konfiguration…	Der HA-Status sollte…
Zwei Nodes	mcc-2n
Vier oder acht Nodes	mcc

2. Wenn der angezeigte Systemzustand des Controllers nicht richtig ist, setzen Sie den HA-Status für das Controller-Modul und das Chassis:

Wenn die MetroCluster-Konfiguration…	Geben Sie diese Befehle ein…

Zwei Knoten	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Vier oder acht Knoten	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul unter Verwendung der zuvor gesammelten Sysiden wieder zu

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln von Informationen vor dem Upgrade".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Halten Sie das System an und starten Sie von der in den Wartungsmodus `LOADER` Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Laufwerke von Node_B_1-A700 an:

   ```
   disk show -a
   ```

   Die Beispielausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   `disk reassign -s old-sysid -d new-sysid`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden: `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. Zeigt den Aggregatstatus an: `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-A900).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten: `halt`
2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Anzeigen des Startmenüs: `boot_ontap menu`
4. Wenn die Stammverschlüsselung verwendet wird, geben Sie den Startmenü-Befehl für Ihre Verschlüsselungsmanagementkonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

5. Wenn Autoboot aktiviert ist, unterbrechen Sie den Autostart, indem Sie Control-C drücken
6. Führen Sie im Startmenü die Option (6) aus.

Mit Option 6 wird der Node vor Abschluss zweimal neu gestartet.

Antworten `y` Zu den Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist: `printenv partner-sysid`

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest: `setenv partner-sysid` *`partner-sysID`*

8. Wenn die Stammverschlüsselung verwendet wird, geben Sie den Startmenü-Befehl für Ihre Verschlüsselungsmanagementkonfiguration erneut aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option 10 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen
Externes Verschlüsselungskeymanagement	Option 11 und befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung oder Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen

   Möglicherweise müssen Sie die ausgeben `recover_xxxxxxxx_keymanager` Befehl wird mehrmals am Boot-Menü angezeigt, bis die Nodes vollständig gebootet werden.

9. Starten der Knoten: `boot_ontap`
10. Warten Sie, bis die ersetzten Nodes gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

       `network port broadcast-domain show`

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

       "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast Domain hostet.

d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

   Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

   "Erstellen einer Cluster-Peer-Beziehung"

f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

   VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

   "Erstellen eines VLANs"

"Verbinden von physischen Ports zum Erstellen von Schnittstellengruppen"

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

LIF-Konfiguration überprüfen

Stellen Sie vor dem Wechsel sicher, dass LIFs auf den entsprechenden Nodes/Ports gehostet werden. Folgende Schritte sind auszuführen

Über diese Aufgabe

Diese Aufgabe wird in Site_B ausgeführt, wo die Nodes mit Root-Aggregaten gestartet wurden.

Schritte

1. Stellen Sie vor dem Wechsel sicher, dass LIFs auf dem entsprechenden Node und den entsprechenden Ports gehostet werden.

   a. Ändern Sie die erweiterte Berechtigungsebene:

      ```
      set -privilege advanced
      ```

   b. Port-Konfiguration überschreiben, um korrekte LIF-Platzierung zu gewährleisten:

      ```
      vserver config override -command "network interface modify" -vserver
      vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
      new_node_name"
      ```

Wenn Sie den eingeben `network interface modify` Befehl im `vserver config override` Befehl, Sie können die Funktion Autovervollständigung auf der Registerkarte nicht verwenden. Sie können die erstellen `network interface modify` Verwenden Sie Autocomplete und schließen Sie es dann in das ein `vserver config override` Befehl.

a. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

2. Zurücksetzen der Schnittstellen auf ihren Home-Node:

   `network interface revert * -vserver` *`vserver-name`*

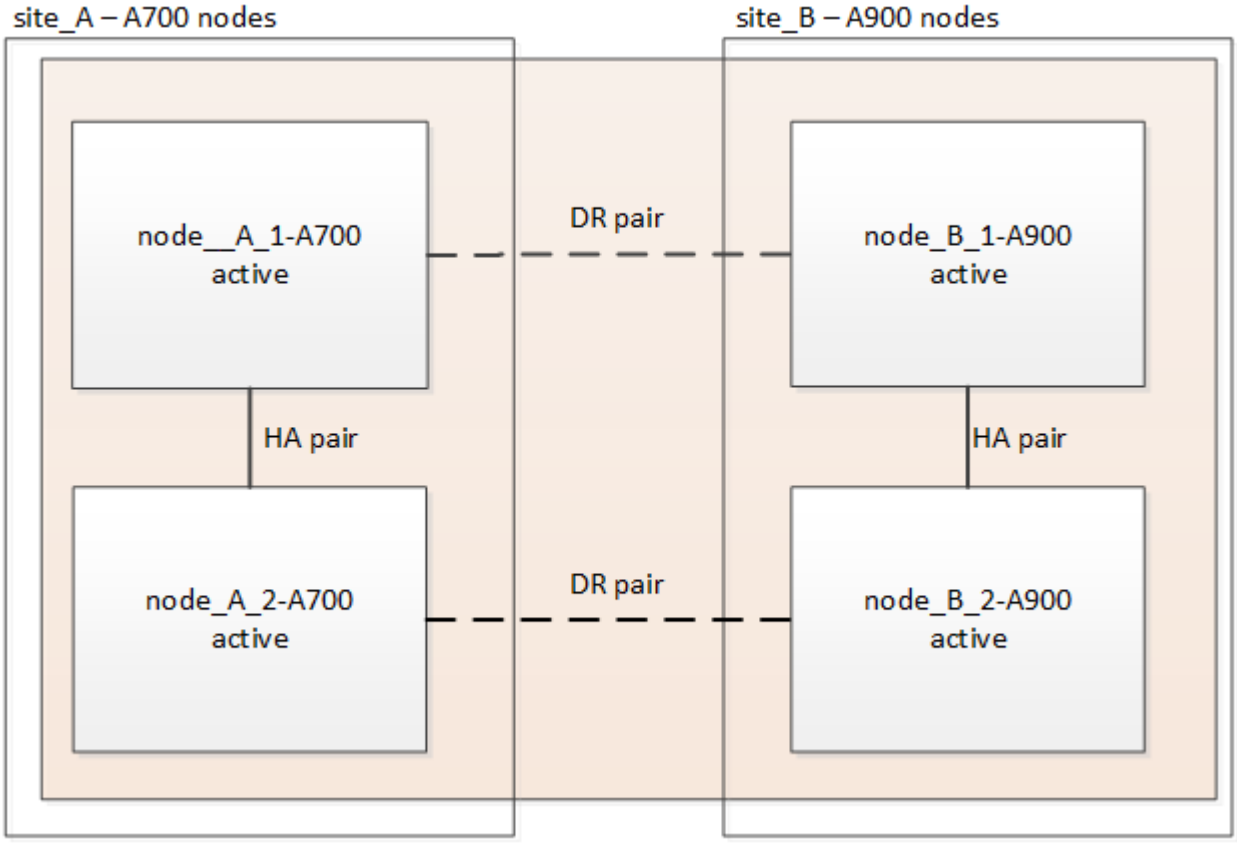
   Führen Sie diesen Schritt bei allen SVMs aus, falls erforderlich.

Schalten Sie die MetroCluster-Konfiguration zurück

Nachdem die neuen Controller konfiguriert wurden, schalten Sie die MetroCluster Konfiguration zurück und kehren den normalen Betrieb zurück.

Über diese Aufgabe

In dieser Aufgabe führen Sie den Vorgang zum Zurückkehren aus und kehren die MetroCluster-Konfiguration in den normalen Betrieb zurück. Die Knoten auf Site_A warten noch auf das Upgrade, wie in der folgenden Abbildung dargestellt. (Diese Abbildung gilt auch für das Upgrade einer FAS9000 auf einen FAS9500 Controller.)



Schritte

1. Stellen Sie das aus `metrocluster node show` Befehl auf Site_B und überprüfen Sie die Ausgabe.

a. Vergewissern Sie sich, dass die neuen Nodes korrekt dargestellt sind.
b. Überprüfen Sie, ob sich die neuen Nodes im Status „Warten auf den Wechsel zurück“ befinden.

2. Zurückwechseln des Clusters:

```
metrocluster switchback
```

3. Überprüfen Sie den Fortschritt des Umschalttaschens:

```
metrocluster show
```

Der Umkehrvorgang läuft noch, wenn die Ausgabe angezeigt wird `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umkehrvorgang ist abgeschlossen, wenn die Ausgabe angezeigt wird `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl. Dieser Befehl befindet sich auf der erweiterten Berechtigungsebene.

Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration

Nach dem Upgrade der Controller-Module müssen Sie den Systemzustand der MetroCluster Konfiguration überprüfen.

Über diese Aufgabe

Diese Aufgabe kann auf jedem Node der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster Konfiguration:

   a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

   ```
   metrocluster show
   ```

   b. Durchführen einer MetroCluster-Prüfung:

   ```
   metrocluster check run
   ```

   c. Ergebnisse der MetroCluster-Prüfung anzeigen:

   ```
   metrocluster check show
   ```

   Nach dem Ausführen des `metrocluster check run` Und `metrocluster check show` Zeigt möglicherweise einen Fehler an, der dem folgenden Beispiel ähnelt:

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+
Dieser Fehler tritt auf, weil der Controller während des Upgrades nicht stimmt. Sie können den Fehler ohne Bedenken ignorieren und mit dem Upgrade der Nodes auf Site_A fortfahren

Aktualisieren Sie die Knoten auf site_A

Sie müssen die Upgrade-Aufgaben auf Site_A wiederholen

Schritt

1. Wiederholen Sie die Schritte, um die Knoten auf Standort_A zu aktualisieren. Beginnen Sie mit "Bereiten Sie sich auf das Upgrade vor".

   Während Sie die Aufgaben ausführen, werden alle Beispielreferenzen zu den Standorten und Knoten umgekehrt. Wenn das Beispiel für die Umschaltung von Site_A verwendet wird, werden Sie von Site_B. umschalten

Senden Sie eine individuelle AutoSupport Nachricht nach der Wartung

Nach Abschluss des Upgrades sollten Sie eine AutoSupport Meldung mit Angaben zum Ende der Wartung senden. Die automatische Case-Erstellung kann also fortgesetzt werden.

Schritt

1. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.

   a. Geben Sie den folgenden Befehl ein:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

b. Wiederholen Sie den Befehl im Partner-Cluster.

Wiederherstellung des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte unter: "Hinzufügen von MetroCluster Konfigurationen" Im Abschnitt *MetroCluster Tiebreaker Installation and Configuration*.

Aktualisieren Sie Controller in einer MetroCluster FC-Konfiguration mit vier Knoten mithilfe von Switchover und Switchback mit den Befehlen „System Controller Replace“ (ONTAP 9.10.1 und höher).

Mithilfe dieses geführten automatisierten MetroCluster-Switchover-Vorgangs lässt sich ein unterbrechungsfreies Controller-Upgrade auf einer MetroCluster FC-Konfiguration mit vier Nodes durchführen. Andere Komponenten (wie Storage Shelves oder Switches) können nicht im Rahmen dieses Verfahrens aktualisiert werden.

Unterstützte Plattformkombinationen

- Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster FC-Upgrade-Tabelle in "Wählen Sie ein Controller-Upgrade-Verfahren".

Weitere Verfahren finden Sie unter"Wählen Sie eine Upgrade- oder Aktualisierungsmethode aus".

Über diese Aufgabe

- Sie können diese Vorgehensweise nur für Controller-Upgrades verwenden.

  Andere Komponenten in der Konfiguration, wie z. B. Storage Shelfs oder Switches, können nicht gleichzeitig aktualisiert werden.

- Dieses Verfahren gilt für Controller-Module in einer MetroCluster FC-Konfiguration mit vier Nodes.
- Die Plattformen müssen ONTAP 9.10.1 oder höher ausführen.

  "NetApp Hardware Universe"

- Mit diesem Verfahren können Controller in einer MetroCluster FC-Konfiguration mit vier Nodes mithilfe von NSO basierter, automatisierter Umschaltung und zurückwechseln. Wenn Sie ein Controller-Upgrade mithilfe von Aggregate Relocation (ARL) durchführen möchten, lesen Sie "Verwenden Sie „System Controller Replace“-Befehle, um das Upgrade der Controller Hardware mit ONTAP 9.8 oder höher durchzuführen". Es wird empfohlen, das NSO-basierte automatische Verfahren zu verwenden.
- Wenn sich die MetroCluster Standorte physisch an zwei verschiedenen Standorten befinden, sollten Sie das automatische NSO Controller-Upgrade-Verfahren einsetzen, um die Controller an beiden Standorten nacheinander zu aktualisieren.
- Durch dieses automatische NSO-basierte Controller-Upgrade-Verfahren können Sie den Controller-Ersatz an einen MetroCluster Disaster Recovery (DR)-Standort initiieren. Sie können jeweils nur einen Controller-Austausch an einem Standort initiieren.

- Um an Standort A einen Controller-Austausch zu initiieren, müssen Sie den Startbefehl für den Controller-Austausch von Standort B ausführen Der Vorgang leitet Sie weiter, Controller beider Nodes nur an Standort A zu ersetzen. Um die Controller an Standort B zu ersetzen, müssen Sie den Startbefehl für den Controller-Ersatz von Standort A ausführen Es wird eine Meldung angezeigt, in der der Standort identifiziert wird, an dem die Controller ersetzt werden.

Folgende Beispielnamen werden in diesem Verfahren verwendet:

- Standort_A
  - Vor dem Upgrade:
    - Node_A_1-alt
    - Node_A_2-alt
  - Nach dem Upgrade:
    - Node_A_1-neu
    - Node_A_2-neu
- Standort_B
  - Vor dem Upgrade:
    - Node_B_1-alt
    - Node_B_2-alt
  - Nach dem Upgrade:
    - Node_B_1-neu
    - Node_B_2-neu

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Bereiten Sie sich auf das Upgrade vor

Zur Vorbereitung auf das Controller Upgrade müssen Sie die System-Vorabprüfungen durchführen und die Konfigurationsinformationen erfassen.

Während des Upgrades können Sie die ausführen `system controller replace show` Oder `system controller replace show-details` Befehl von Standort A, um den Status zu überprüfen. Wenn die Befehle eine leere Ausgabe zurückgeben, warten Sie einige Minuten, und führen Sie den Befehl erneut aus.

Schritte

1. Führen Sie den folgenden Befehl von Standort A aus, um die Controller an Standort B zu ersetzen:

   `system controller replace start`

   > ◦ Wenn Sie den Vorgang an einem Standort wiederholen, nachdem Sie die Controller am anderen Standort bereits ausgetauscht haben, tritt aufgrund einer Nichtübereinstimmung der Knoten an beiden Standorten ein Fehler auf. Dies ist das erwartete Verhalten, wenn an beiden Standorten unterschiedliche Plattformmodelle vorhanden sind.
   >
   > Wenn nur der Fehler „Mismatch“ zurückgegeben wird, können Sie die `-skip -metrocluster-check true` Option mit der `system controller replace start` Befehl, um die MetroCluster-Prüfungen zu überspringen.

   Die Prüfungen werden im automatisierten Betrieb durchgeführt. Wenn keine Probleme gefunden werden, wird der Vorgang angehalten, sodass Sie die konfigurationsbezogenen Informationen manuell erfassen können.

   Das aktuelle Quellsystem und alle kompatiblen Zielsysteme werden angezeigt. Wenn Sie den Quellcontroller durch einen Controller mit einer anderen ONTAP-Version oder einer nicht kompatiblen Plattform ersetzt haben, wird der Automatisierungsvorgang nach dem Booten der neuen Knoten angehalten und meldet einen Fehler. Führen Sie die manuelle Wiederherstellung durch, um den Cluster wieder in einen fehlerfreien Zustand zu versetzen.

   Der `system controller replace start` Der Befehl meldet möglicherweise den folgenden Vorprüffehler:

   ```
   Cluster-A::*>system controller replace show
   Node        Status         Error-Action
   ----------- -------------- ------------------------------------
   Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
   showed errors in component aggregates
   ```

   Überprüfen Sie, ob dieser Fehler aufgetreten ist, weil Sie nicht gespiegelte Aggregate oder ein anderes Problem an Aggregaten haben. Vergewissern Sie sich, dass sich alle gespiegelten Aggregate in einem ordnungsgemäßen Zustand befinden und dass sie nicht beeinträchtigt bzw. gespiegelt werden. Wenn dieser Fehler nur auf nicht gespiegelte Aggregate zurückzuführen ist, können Sie diesen Fehler durch Auswahl des überschreiben `-skip-metrocluster-check true` Option auf der `system controller replace start` Befehl. Wenn auf Remote-Storage zugegriffen werden kann, sind die nicht gespiegelten Aggregate nach einer Umschaltung online. Falls die Remote-Storage-Verbindung ausfällt, können die nicht gespiegelten Aggregate nicht online geschaltet werden.

2. Erfassen Sie manuell die Konfigurationsinformationen, indem Sie sich bei Standort B anmelden und den Befehlen folgen, die in der Konsolenmeldung unter der aufgeführt sind `system controller replace show` Oder `system controller replace show-details` Befehl.

Sammeln Sie vor dem Upgrade Informationen

Vor dem Upgrade, wenn das Root-Volume verschlüsselt ist, müssen Sie den Sicherungsschlüssel und andere Informationen sammeln, um die neuen Controller mit den alten verschlüsselten Root-Volumes zu booten.

Über diese Aufgabe

Diese Aufgabe wird für die vorhandene MetroCluster FC-Konfiguration ausgeführt.

Schritte

1. Beschriften Sie die Kabel für die vorhandenen Controller, damit Sie bei der Einrichtung der neuen Controller problemlos die Kabel identifizieren können.
2. Zeigen Sie die Befehle an, um den Backup-Schlüssel und weitere Informationen zu erfassen:

   `system controller replace show`

   Führen Sie die unter aufgeführten Befehle aus `show` Befehl aus dem Partner-Cluster.

3. Ermitteln Sie die System-IDs der Nodes in der MetroCluster-Konfiguration:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Während der Aktualisierung ersetzen Sie diese alten System-IDs durch die System-IDs der neuen Controller-Module.

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1-alt: 4068741258
   - Node_A_2-alt: 4068741260
   - Node_B_1-alt: 4068741254
   - Node_B_2-alt: 4068741256

   ```
   metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
   partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
   dr-group-id        cluster           node            node-systemid
   ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
   -----------        ---------------   ----------      -------------
   -------------------     -------------------    ---------------------
   1                    Cluster_A       Node_A_1-old    4068741258
   4068741260              4068741256             4068741256
   1                    Cluster_A       Node_A_2-old    4068741260
   4068741258              4068741254             4068741254
   1                    Cluster_B       Node_B_1-old    4068741254
   4068741256              4068741258             4068741260
   1                    Cluster_B       Node_B_2-old    4068741256
   4068741254              4068741260             4068741258
   4 entries were displayed.
   ```

   In diesem Beispiel für eine MetroCluster FC-Konfiguration mit zwei Nodes werden die folgenden alten System-IDs abgerufen:

   - Node_A_1: 4068741258

- Knoten_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Sammeln von Port- und LIF-Informationen zu jedem alten Node

   Sie sollten die Ausgabe der folgenden Befehle für jeden Node erfassen:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node-name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`

5. Wenn sich die MetroCluster-Nodes in einer SAN-Konfiguration befinden, sammeln Sie die relevanten Informationen.

   Sie sollten die Ausgabe der folgenden Befehle erfassen:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Wenn das Root-Volume verschlüsselt ist, erfassen und speichern Sie die für das Schlüsselmanagement verwendete Passphrase:

   ```
   security key-manager backup show
   ```

7. Wenn die MetroCluster Nodes Verschlüsselung für Volumes oder Aggregate nutzen, kopieren Sie Informationen zu Schlüsseln und Passphrases.

   Weitere Informationen finden Sie unter "Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen".

a. Wenn Onboard Key Manager konfiguriert ist:

```
security key-manager onboard show-backup
```

Sie benötigen die Passphrase später im Upgrade-Verfahren.

b. Wenn das Enterprise-Verschlüsselungsmanagement (KMIP) konfiguriert ist, geben Sie die folgenden Befehle ein:

```
security key-manager external show -instance
```

```
security key-manager key query
```

8. Setzen Sie den Vorgang fort, nachdem Sie die Konfigurationsinformationen erfasst haben:

```
system controller replace resume
```

Entfernen Sie die vorhandene Konfiguration über den Tiebreaker oder eine andere Monitoring-Software

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Konfiguration oder anderen Applikationen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster Konfiguration über den Tiebreaker oder eine andere Software entfernen, bevor der alte Controller ersetzt wird.

Schritte

1. "Entfernen der vorhandenen MetroCluster-Konfiguration" Über die Tiebreaker Software.
2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Ersetzen Sie die alten Controller, und starten Sie die neuen Controller

Nachdem Sie Informationen gesammelt und den Vorgang fortgesetzt haben, wird die Automatisierung mit dem Switchover fortgesetzt.

Über diese Aufgabe

Der Automatisierungsvorgang initiiert die Umschaltung, `heal-aggregates`, und `heal root-aggregates` Betrieb: Nach Abschluss dieser Vorgänge wird der Vorgang bei **pausiert für Benutzereingriff** angehalten, sodass Sie die Controller racken und installieren können, die Partner-Controller hochfahren und die Root-Aggregat-Festplatten dem neuen Controller-Modul aus dem Flash-Backup mit dem neu zuweisen können `sysids` Früher gesammelt.

Bevor Sie beginnen

Vor dem Starten der Umschaltung hält der Automatisierungsvorgang pausiert, sodass Sie manuell überprüfen können, ob alle LIFs „`up`“ an Standort B. sind Ggf. Beliebige LIFs mit „`deigenen`“ bis „`up`“ bereitstellen und den Automatisierungsvorgang mit dem fortsetzen `system controller replace resume` Befehl.

Vorbereiten der Netzwerkkonfiguration der alten Controller

Um sicherzustellen, dass das Netzwerk auf den neuen Controllern ordnungsgemäß fortgesetzt wird, müssen Sie LIFs auf einen gemeinsamen Port verschieben und dann die Netzwerkkonfiguration der alten Controller

entfernen.

Über diese Aufgabe

- Diese Aufgabe muss an jedem der alten Knoten ausgeführt werden.
- Sie werden die in gesammelten Informationen verwenden Bereiten Sie sich auf das Upgrade vor.

Schritte

1. Booten Sie die alten Nodes, und melden Sie sich dann bei den Nodes an:

   `boot_ontap`

2. Weisen Sie den Home-Port aller Daten-LIFs des alten Controllers einem gemeinsamen Port zu, der auf den alten und den neuen Controller-Modulen identisch ist.

   a. Anzeigen der LIFs:

      `network interface show`

      Alle Daten-LIFS einschließlich SAN und NAS sind admin „`up`“ und betrieblich „`down`“, da sie sich am Switchover-Standort (Cluster_A) befinden.

   b. Überprüfen Sie die Ausgabe, um einen gemeinsamen physischen Netzwerk-Port zu finden, der auf den alten und den neuen Controllern identisch ist, die nicht als Cluster-Port verwendet werden.

      „`e0d`“ ist zum Beispiel ein physischer Port an alten Controllern und ist auch auf neuen Controllern vorhanden. „`e0d`“ wird nicht als Cluster-Port oder anderweitig auf den neuen Controllern verwendet.

      Informationen zur Portnutzung von Plattformmodellen finden Sie im "NetApp Hardware Universe"

   c. Ändern Sie alle Daten-LIFS, um den gemeinsamen Port als Home-Port zu verwenden:

      `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

      Im folgenden Beispiel lautet „`e0d`“.

      Beispiel:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Ändern Sie Broadcast-Domänen, um VLAN und physische Ports zu entfernen, die gelöscht werden müssen:

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Wiederholen Sie diesen Schritt für alle VLAN- und physischen Ports.

4. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und Schnittstellengruppen, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:

```
network port vlan delete -node node-name -vlan-name portid-vlandid
```

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

```
network port ifgrp remove-port -node node-name -ifgrp interface-group-name
-port portid
```

Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN- und Interface Group-Ports aus der Broadcast-Domäne:

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Ändern Sie die Schnittstellengruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Anhalten der Knoten:

```
halt -inhibit-takeover true -node node-name
```

Dieser Schritt muss auf beiden Knoten durchgeführt werden.

Richten Sie die neuen Controller ein

Sie müssen die neuen Controller im Rack unterbringen und verkabeln.

Schritte

1. Planen Sie die Positionierung der neuen Controller-Module und Storage Shelves je nach Bedarf.

   Der Rack-Platz hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Storage-Shelfs in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Wenn die neuen Controller-Module nicht eigene FC-VI-Karten enthalten und FC-VI-Karten von alten Controllern mit neuen Controllern kompatibel sind, tauschen Sie FC-VI-Karten aus und installieren Sie diese in den richtigen Steckplätzen.

Siehe "NetApp Hardware Universe" Für Slot-Informationen für FC-VI-Karten.

5. Verkabeln Sie die Strom-, seriellen Konsolen- und Managementverbindungen der Controller, wie in den *MetroCluster Installations- und Konfigurationsleitfäden* beschrieben.

   Schließen Sie derzeit keine anderen Kabel an, die von den alten Controllern getrennt wurden.

   "Dokumentation zu ONTAP Hardwaresystemen"

6. Schalten Sie die neuen Nodes ein, und drücken Sie bei der Eingabeaufforderung Strg-C, um die LOADER-Eingabeaufforderung anzuzeigen.

Booten Sie die neuen Controller ein

Nachdem Sie die neuen Nodes installiert haben, müssen Sie als Netzboot fahren, damit die neuen Nodes dieselbe Version von ONTAP wie die ursprünglichen Nodes ausführen. Der Begriff Netzboot bedeutet, dass Sie über ein ONTAP Image, das auf einem Remote Server gespeichert ist, booten. Wenn Sie das Netzboot vorbereiten, müssen Sie eine Kopie des ONTAP 9 Boot Images auf einem Webserver ablegen, auf den das System zugreifen kann.

Diese Aufgabe wird an jedem der neuen Controller-Module durchgeführt.

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	Extrahieren Sie den Inhalt der ontap-Version_image.tgzfile in das Zielverzeichnis: Tar -zxvf ontap-Version_image.tgz HINWEIS: Wenn Sie den Inhalt auf Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot Image zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: ontap-Version_image.tgz Sie müssen nicht die ontap-Version_image.tgz-Datei extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine Management-LIF:
   - Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

     ```
     ifconfig e0M -auto
     ```

- Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

  ```
  ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
  ```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Wählen Sie im Startmenü die Option **(7) Neue Software zuerst installieren** aus, um das neue Software-Image auf das Boot-Gerät herunterzuladen und zu installieren.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein
   `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie
   die URL der Bilddatei ein: `\http://web_server_ip/path_to_web-
   accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Starten Sie den Neustart durch Eingabe `y` Wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

Löschen Sie die Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

   ```
   boot_ontap menu
   ```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Wiederherstellung der HBA-Konfiguration

Je nach Vorhandensein und Konfiguration der HBA-Karten im Controller-Modul müssen Sie diese für die Verwendung Ihres Standorts richtig konfigurieren.

Schritte

1. Konfigurieren Sie im Wartungsmodus die Einstellungen für alle HBAs im System:

   a. Überprüfen Sie die aktuellen Einstellungen der Ports: `ucadmin show`

   b. Aktualisieren Sie die Porteinstellungen nach Bedarf.

Wenn Sie über diese Art von HBA und den gewünschten Modus verfügen…	Befehl
CNA FC	`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`*

2. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Warten Sie, bis der Node an der LOADER-Eingabeaufforderung angehalten wird, nachdem Sie den Befehl ausgeführt haben.

3. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

4. Überprüfen Sie die vorgenommenen Änderungen:

Wenn Sie über diese Art von HBA verfügen…	Befehl
CNA	`ucadmin show`
FC	`fcadmin show`

Neuzuweisung von Root-Aggregat-Festplatten

Weisen Sie die Root-Aggregat-Festplatten dem neuen Controller-Modul mithilfe des neu zu `sysids` Früher gesammelt

Über diese Aufgabe

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die alten System-IDs wurden in identifiziert "Sammeln Sie vor dem Upgrade Informationen".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Alte System-ID	Neue System-ID
Knoten_B_1	4068741254	1574774970

Schritte

1. Alle anderen Verbindungen mit den neuen Controller-Modulen (FC-VI, Storage, Cluster Interconnect usw.) verkabeln.
2. Beenden Sie das System und das Booten in den Wartungsmodus von der LOADER-Eingabeaufforderung:

   ```
   boot_ontap maint
   ```

3. Zeigen Sie die Datenträger von Node_B_1-old an:

   ```
   disk show -a
   ```

Die Befehlsausgabe zeigt die System-ID des neuen Controller-Moduls (1574774970). Allerdings sind die Root-Aggregat-Festplatten immer noch im Besitz der alten System-ID (4068741254). In diesem Beispiel werden keine Laufwerke angezeigt, die sich im Besitz anderer Nodes in der MetroCluster-Konfiguration befinden.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Weisen Sie die Root-Aggregat-Festplatten auf den Laufwerk-Shelfs dem neuen Controller zu:

   `disk reassign -s old-sysid -d new-sysid`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Überprüfen Sie, ob alle Festplatten wie erwartet neu zugewiesen wurden:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Zeigt den Aggregatstatus an:

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status            Options
   aggr0_node_b_1-root         online      raid_dp, aggr     root, nosnap=on,
                               mirrored
   mirror_resync_priority=high(fixed)
                               fast zeroed
                               64-bit
   ```

7. Wiederholen Sie die oben genannten Schritte auf dem Partner-Node (Node_B_2-New).

Booten der neuen Controller

Sie müssen die Controller aus dem Boot-Menü neu booten, um das Controller-Flash-Image zu aktualisieren. Bei Konfiguration der Verschlüsselung sind weitere Schritte erforderlich.

Sie können VLANs und Schnittstellengruppen neu konfigurieren. Falls erforderlich, ändern Sie die Ports für die Cluster-LIFs und Broadcast-Domänen manuell, bevor Sie den Vorgang mit der fortsetzen `system controller replace resume` Befehl.

Über diese Aufgabe

Diese Aufgabe muss für alle neuen Controller ausgeführt werden.

Schritte

1. Stoppen Sie den Knoten:

   ```
   halt
   ```

2. Wenn der externe Schlüsselmanager konfiguriert ist, legen Sie die zugehörigen Bootargs fest:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

4. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option für Ihre Konfiguration für die Schlüsselverwaltung aus.

Sie verwenden…	Diese Startmenüoption auswählen…

Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.
Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

5. Wenn Autoboot aktiviert ist, unterbrechen Sie die Autoboot-Taste, indem Sie Strg+C drücken
6. Führen Sie im Startmenü die Option „`6`“ aus.

   Mit der Option „`6`“ wird der Node vor Abschluss zweimal neu gestartet.

   Beantworten Sie „`y`“ auf die Eingabeaufforderungen zur Änderung der System-id. Warten Sie auf die zweite Neustartmeldung:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Überprüfen Sie doppelt, ob die Partner-Sysid korrekt ist:

   `printenv partner-sysid`

   Falls Partner-sysid nicht richtig ist, stellen Sie es fest:

   `setenv partner-sysid` *`partner-sysID`*

8. Wenn die Stammverschlüsselung verwendet wird, wählen Sie die Startmenü-Option erneut für Ihre Schlüsselverwaltungskonfiguration aus.

Sie verwenden…	Diese Startmenüoption auswählen…
Integriertes Verschlüsselungsmanagement	Option „`10`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Externes Verschlüsselungskeymanagement	Option „`11`“ Befolgen Sie die Anweisungen, um die erforderlichen Eingaben zur Wiederherstellung und Wiederherstellung der Schlüsselmanager-Konfiguration bereitzustellen.

Führen Sie je nach Einstellung des Schlüsselmanagers den Wiederherstellungsvorgang durch, indem Sie die Option „`10`“ oder die Option „`11`“ wählen, gefolgt von der ersten Eingabeaufforderung im Startmenü die Option „`6`“. Um die Knoten vollständig zu booten, müssen Sie möglicherweise den Wiederherstellungsvorgang mit Option „`1`“ (normaler Start) wiederholen.

9. Starten der Knoten:

   ```
   boot_ontap
   ```

10. Warten Sie, bis die ersetzten Nodes gestartet werden.

    Wenn sich einer der beiden Nodes im Übernahmemodus befindet, geben Sie sie mithilfe der wieder `storage failover giveback` Befehl.

11. Vergewissern Sie sich, dass sich alle Ports in einer Broadcast-Domäne befinden:

    a. Broadcast-Domänen anzeigen:

       ```
       network port broadcast-domain show
       ```

    b. Fügen Sie bei Bedarf beliebige Ports zu einer Broadcast-Domäne hinzu.

       "Hinzufügen oder Entfernen von Ports aus einer Broadcast-Domäne"

    c. Fügen Sie den physischen Port hinzu, der die Intercluster LIFs der entsprechenden Broadcast-Domäne hostet.

    d. Ändern Sie Intercluster LIFs, um den neuen physischen Port als Home-Port zu verwenden.

    e. Nachdem die Intercluster LIFs aktiviert sind, prüfen Sie den Cluster Peer-Status und stellen Sie bei Bedarf Cluster-Peering wieder her.

       Möglicherweise müssen Sie Cluster-Peering neu konfigurieren.

       "Erstellen einer Cluster-Peer-Beziehung"

    f. VLANs und Schnittstellengruppen nach Bedarf neu erstellen.

       VLAN und Interface Group Mitgliedschaft können sich von der des alten Node unterscheiden.

       "Erstellen Sie eine VLAN"

    "Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen"

    a. Überprüfen Sie, ob das Partner-Cluster erreichbar ist und ob die Konfiguration auf dem Partner-Cluster erfolgreich resynchronisiert ist:

       ```
       metrocluster switchback -simulate true
       ```

12. Stellen Sie bei Verwendung der Verschlüsselung die Schlüssel mithilfe des korrekten Befehls für Ihre Verschlüsselungsmanagementkonfiguration wieder her.

Sie verwenden…	Befehl
Integriertes Verschlüsselungsmanagement	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement".
Externes Verschlüsselungskeymanagement	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

13. Bevor Sie den Vorgang fortsetzen, überprüfen Sie, ob die MetroCluster ordnungsgemäß konfiguriert ist. Prüfen Sie den Knoten-Status:

    ```
    metrocluster node show
    ```

    Überprüfen Sie, ob sich die neuen Knoten (site_B) in **warten auf den Status wechseln** von site_A befinden

14. Vorgang fortsetzen:

    ```
    system controller replace resume
    ```

Schließen Sie das Upgrade ab

Der Automatisierungsvorgang führt Überprüfungen des Verifikationssystems durch und hält anschließend Pausen ein, um die Erreichbarkeit des Netzwerks zu überprüfen. Nach der Überprüfung wird die Rückgewinnungsphase für die Ressourcen eingeleitet und der Automatisierungsvorgang führt den Wechsel zurück an Standort A durch und hält die Prüfungen nach dem Upgrade an. Nachdem Sie den Automatisierungsvorgang fortgesetzt haben, führt er die Prüfungen nach dem Upgrade durch und markiert, wenn keine Fehler erkannt werden, das Upgrade als abgeschlossen.

Schritte

1. Überprüfen Sie die Netzwerkzuwachbarkeit, indem Sie die Konsolenmeldung ausführen.
2. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

    ```
    system controller replace resume
    ```

3. Der Automatisierungsvorgang kehrt an Standort A zurück und führt die Nachprüfung durch. Wenn der Vorgang angehalten wird, überprüfen Sie den SAN-LIF-Status manuell und überprüfen Sie die Netzwerkkonfiguration anhand der Konsolenmeldung.
4. Setzen Sie nach Abschluss der Verifizierung den Vorgang fort:

    ```
    system controller replace resume
    ```

5. Prüfen Sie den Status der Prüfungen nach der Aktualisierung:

```
system controller replace show
```

Wenn bei den Prüfungen nach der Aktualisierung keine Fehler gemeldet wurden, ist das Upgrade abgeschlossen.

6. Melden Sie sich nach Abschluss des Controller-Upgrades bei Standort B an und überprüfen Sie, ob die ersetzten Controller ordnungsgemäß konfiguriert sind.

Aktualisieren Sie die Nodes auf Cluster_A

Sie müssen die Upgrade-Tasks wiederholen, um die Nodes auf „Cluster_A“ an Standort A zu aktualisieren

Schritte

1. Wiederholen Sie die Schritte, um die Knoten auf Cluster_A zu aktualisieren, beginnend mit Bereiten Sie sich auf das Upgrade vor.

   Wenn Sie den Vorgang wiederholen, werden alle Beispielverweise auf die Cluster und Knoten umgekehrt.

Wiederherstellen des Tiebreaker Monitoring

Wenn die MetroCluster Konfiguration zuvor für das Monitoring über die Tiebreaker Software konfiguriert war, können Sie die Tiebreaker Verbindung wiederherstellen.

1. Verwenden Sie die Schritte in "Fügen Sie MetroCluster-Konfigurationen hinzu".

Aktualisieren einer MetroCluster FC-Konfiguration mit vier Nodes

Sie können die Controller und den Storage in einer MetroCluster Konfiguration mit vier Nodes aktualisieren, indem Sie die Konfiguration auf eine Konfiguration mit acht Nodes erweitern und anschließend die alte Disaster Recovery-Gruppe (DR) entfernen.

Über diese Aufgabe

Verweise auf „alte Knoten“ bedeuten die Knoten, die Sie ersetzen möchten.

- Mit diesem Verfahren können Sie nur bestimmte Plattformmodelle in einer MetroCluster FC-Konfiguration aktualisieren.
  - Informationen zu den unterstützten Kombinationen aus Plattform-Upgrades finden Sie in der MetroCluster-FC-Aktualisierungstabelle in "Auswahl der Methode zur Systemaktualisierung".

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

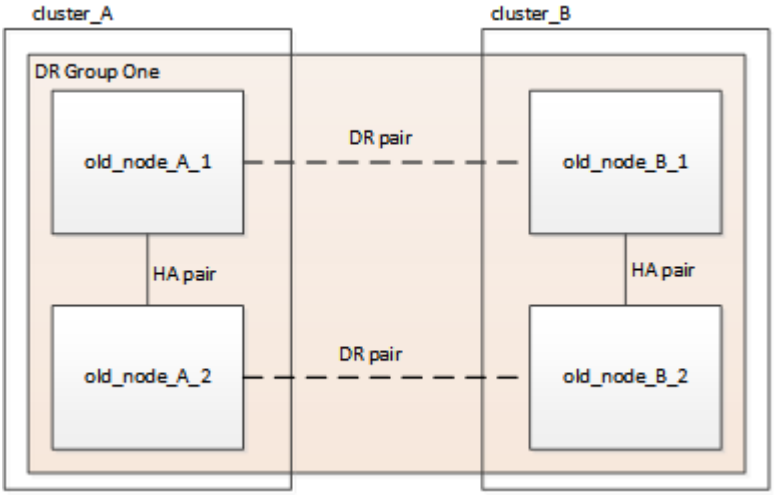
Führen Sie das Aktualisierungsverfahren durch

Führen Sie die folgenden Schritte aus, um die MetroCluster FC-Konfiguration zu aktualisieren.

Schritte

1. Erfassung von Informationen von den alten Knoten.

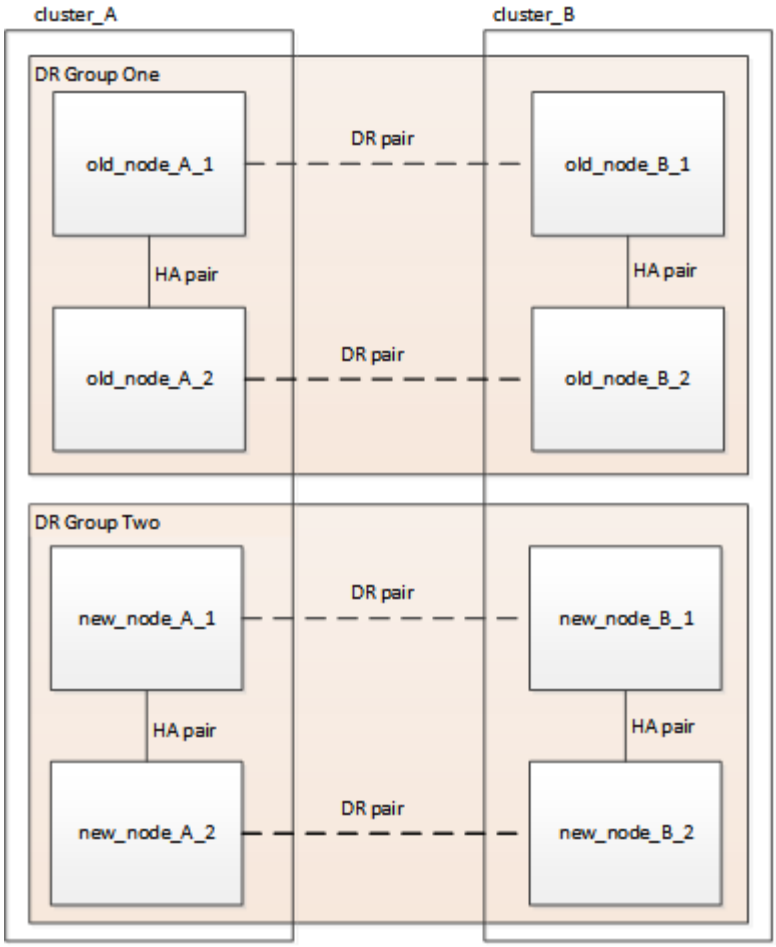
   In dieser Phase wird die Konfiguration mit vier Nodes wie in der folgenden Abbildung dargestellt angezeigt:



2. Führen Sie alle Schritte der Erweiterung mit vier Nodes für Ihren MetroCluster-Typ durch.

   "Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes"

   Wenn der Erweiterungsvorgang abgeschlossen ist, wird die Konfiguration wie in der folgenden Abbildung dargestellt angezeigt:



3. Verschieben Sie die CRS-Volumes.

   Führen Sie die Schritte unter aus "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

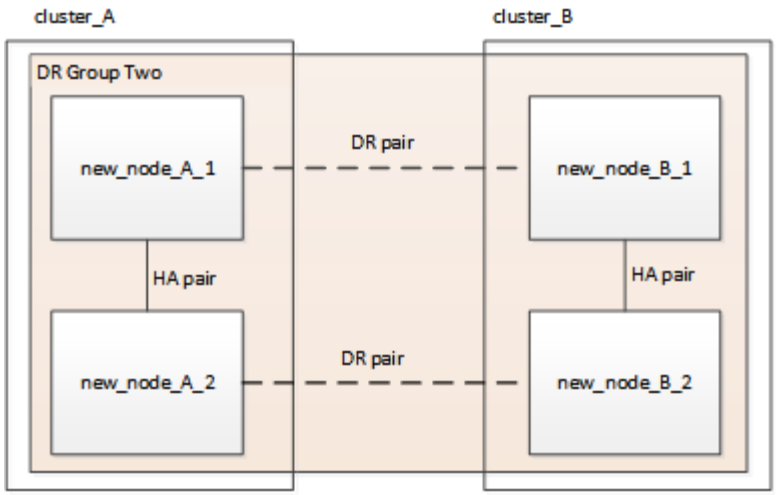
4. Verschieben Sie die Daten von den alten Knoten auf neue Knoten. Gehen Sie dabei wie folgt vor:
   a. Führen Sie alle Schritte in aus "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes".

      Sie könnten wählen, um das Aggregat zu spiegeln, wenn oder nachdem es erstellt wurde.

   b. Führen Sie alle Schritte in aus "Verschieben Sie LIFs für nicht-SAN-Daten und Clustermanagement-LIFs auf die neuen Nodes".
   c. Führen Sie alle Schritte in aus "Das Löschen von SAN LIFs ist von den ursprünglichen Nodes nicht mehr erforderlich".
5. Befolgen Sie die Schritte im Verfahren zum Entfernen der alten DR-Gruppe.

   "Entfernen einer Disaster Recovery-Gruppe"

   Nachdem Sie die alte DR-Gruppe (DR-Gruppe 1) entfernt haben, wird die Konfiguration wie im folgenden Bild dargestellt angezeigt:



Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher)

Mit diesem Verfahren können Sie Controller und Storage in Konfigurationen mit vier oder acht Nodes aktualisieren.

Ab ONTAP 9.13.1 können Sie die Controller und den Speicher in einer MetroCluster IP-Konfiguration mit acht Nodes aktualisieren, indem Sie die Konfiguration zu einer temporären Konfiguration mit zwölf Nodes erweitern und anschließend die alten Disaster Recovery (DR)-Gruppen entfernen.

Ab ONTAP 9.8 können Sie die Controller und den Storage in einer MetroCluster IP-Konfiguration mit vier Nodes aktualisieren, indem Sie die Konfiguration zu einer temporären Konfiguration mit acht Nodes erweitern und dann die alte DR-Gruppe entfernen.

Wichtige Informationen

Während der Umstellungs-, Aktualisierungs- und Erweiterungsvorgänge können Sie Ihrer MetroCluster-Konfiguration ein neues Plattformmodell hinzufügen. Wenn Ihre vorhandene MetroCluster-Konfiguration zu irgendeinem Zeitpunkt eine Plattform mit **gemeinsamen Cluster-/HA-Ports** enthält, können Sie der Konfiguration keine Plattform mit **gemeinsamen MetroCluster-/HA-Ports** hinzufügen, ohne Ihre ONTAP-Version auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher zu aktualisieren.

Bevor Sie sich für dieses Verfahren entscheiden, lesen Sie die Informationen in der folgenden Tabelle sorgfältig durch. Wenn Ihre vorhandene Plattform in der ersten Spalte und die Plattform, die Sie der Konfiguration hinzufügen möchten, in der zweiten Spalte aufgeführt ist, müssen alle Knoten in der Konfiguration ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen, um dieses Verfahren zu unterstützen.

> Sowohl die vorhandene Plattform als auch die Plattform, die Sie der Konfiguration hinzufügen möchten, müssen ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen.

Wenn Ihr vorhandener MetroCluster Folgendes enthält:		Und die Plattform, die Sie hinzufügen, ist …		Dann…
Ein AFF-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	Ein FAS-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • FAS50 • FAS70 • FAS90	Ein AFF-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	Ein FAS-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500	Bevor Sie die neue Plattform zu Ihrer vorhandenen MetroCluster-Konfiguration hinzufügen, aktualisieren Sie alle Knoten in der vorhandenen und neuen Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher.

Über diese Aufgabe

- Bei einer Konfiguration mit acht Nodes muss auf dem System ONTAP 9.13.1 oder höher ausgeführt werden.
- Bei einer Konfiguration mit vier Nodes muss auf dem System ONTAP 9.8 oder höher ausgeführt werden.
- Wenn Sie auch die IP-Switches aktualisieren, müssen Sie sie aktualisieren, bevor Sie diese Aktualisierung durchführen.
- In diesem Verfahren werden die Schritte beschrieben, die zum Aktualisieren einer DR-Gruppe mit vier Nodes erforderlich sind. Wenn Sie über eine Konfiguration mit acht Nodes (zwei DR-Gruppen) verfügen, können Sie eine oder beide DR-Gruppen aktualisieren.

  Wenn Sie beide DR-Gruppen aktualisieren, müssen Sie jeweils eine DR-Gruppe aktualisieren.

- Verweise auf „alte Knoten“ bedeuten die Knoten, die Sie ersetzen möchten.
- Bei Konfigurationen mit acht Nodes muss die Kombination aus MetroCluster-Plattform mit acht Quell- und Zielknoten unterstützt werden.

> Wenn Sie beide DR-Gruppen aktualisieren, wird die Plattformkombination möglicherweise nach dem Aktualisieren der ersten DR-Gruppe nicht unterstützt. Sie müssen beide DR-Gruppen aktualisieren, um eine unterstützte Konfiguration mit acht Nodes zu erreichen.

- Sie können nur bestimmte Plattformmodelle aktualisieren, indem Sie dieses Verfahren in einer MetroCluster IP-Konfiguration verwenden.
  - Informationen darüber, welche Plattformupgradekombinationen unterstützt werden, finden Sie in der Tabelle MetroCluster IP-Aktualisierung in "Auswahl der Methode zur Systemaktualisierung".
- Die unteren Limits der Quell- und Zielplattformen gelten. Wenn Sie zu einer höheren Plattform wechseln, gelten die Einschränkungen der neuen Plattform erst nach Abschluss der Technologieaktualisierung für alle DR-Gruppen.
- Wenn Sie eine Technologieaktualisierung für eine Plattform mit niedrigeren Limits als die Quellplattform durchführen, müssen Sie die Grenzwerte anpassen und verringern, um an oder unter den Grenzen der Zielplattform zu liegen, bevor Sie dieses Verfahren durchführen.

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Führen Sie das Aktualisierungsverfahren durch

Führen Sie die folgenden Schritte aus, um die MetroCluster IP-Konfiguration zu aktualisieren.

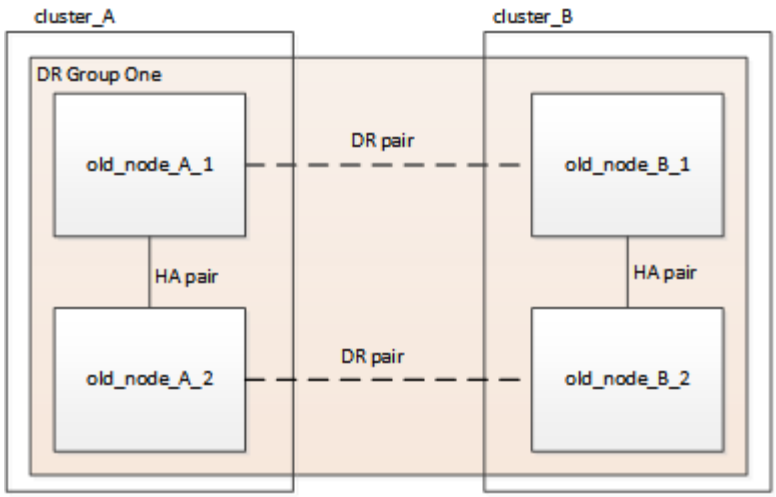
Schritte

1. Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

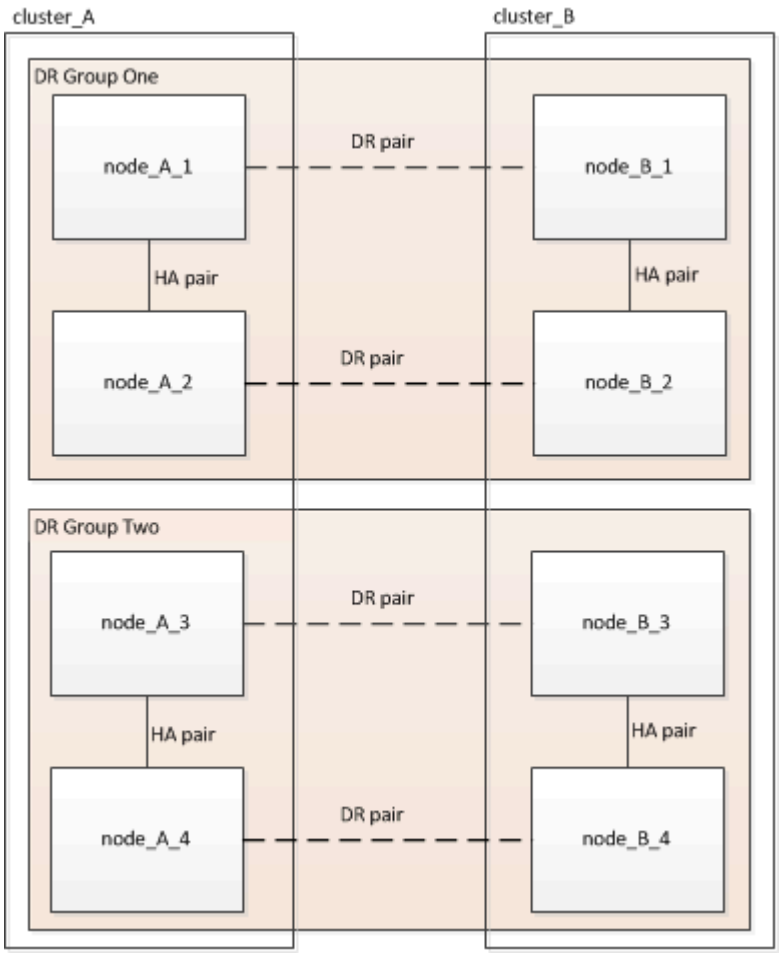
   Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden, sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

2. Erfassung von Informationen von den alten Knoten.

   In dieser Phase wird die Konfiguration mit vier Nodes wie in der folgenden Abbildung dargestellt angezeigt:



Die Konfiguration mit acht Nodes wird wie im folgenden Bild dargestellt angezeigt:



3. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit das Upgrade ausgeführt wird.

   a. Geben Sie den folgenden Befehl ein:
   `system node autosupport invoke -node * -type all -message "MAINT=10h Upgrading old-model to new-model"`

   Das folgende Beispiel gibt ein Wartungsfenster von 10 Stunden an. Je nach Plan sollten Sie

möglicherweise zusätzliche Zeit einplanen.

Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

a. Wiederholen Sie den Befehl im Partner-Cluster.

4. Wenn die End-to-End-Verschlüsselung aktiviert ist, führen Sie die Schritte bis aus "End-to-End-Verschlüsselung deaktivieren".
5. Entfernen Sie die vorhandene MetroCluster-Konfiguration von Tiebreaker, Mediator oder einer anderen Software, die die Umschaltung initiieren kann.

Sie verwenden…	Gehen Sie folgendermaßen vor:

Tiebreaker	a. Verwenden Sie die Tiebreaker CLI `monitor remove` Befehl zum Entfernen der MetroCluster-Konfiguration.
	
	Im folgenden Beispiel wird „`Cluster_A`“ aus der Software entfernt:
	
	`NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.`
	
	b. Stellen Sie sicher, dass die MetroCluster Konfiguration mithilfe der Tiebreaker CLI ordnungsgemäß entfernt wurde `monitor show -status` Befehl.
	
	`NetApp MetroCluster Tiebreaker :> monitor show -status`

Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

6. Führen Sie alle Schritte in aus "Erweitern einer MetroCluster IP-Konfiguration" Um die neuen Nodes und den neuen Storage zur Konfiguration hinzuzufügen.

   Wenn die Erweiterung abgeschlossen ist, wird die temporäre Konfiguration wie in den folgenden Bildern dargestellt angezeigt:

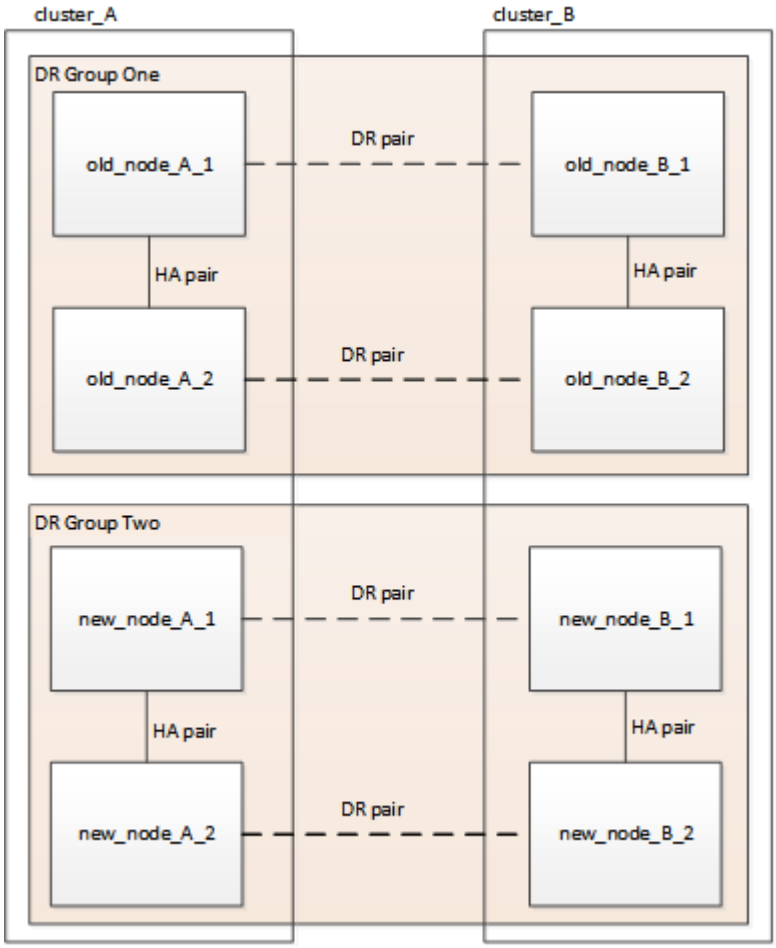


Abbildung 1. Temporäre Konfiguration mit acht Nodes

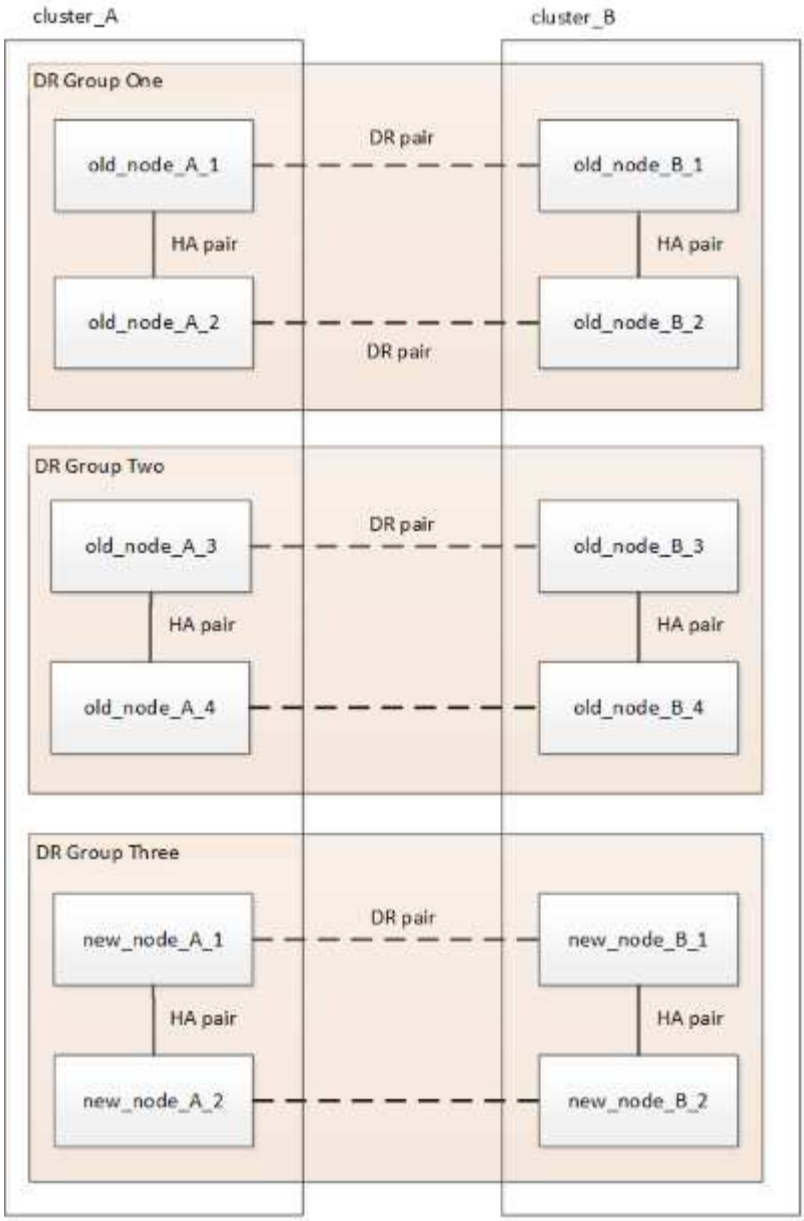


Abbildung 2. Temporäre Konfiguration mit zwölf Nodes

7. Mit dem folgenden Befehl auf beiden Clustern bestätigen Sie, dass ein Takeover möglich ist und die Nodes verbunden sind:

   `storage failover show`

```
cluster_A::> storage failover show
                                      Takeover
Node           Partner                Possible    State Description
-------------- --------------------- ---------   ------------------
Node_FC_1      Node_FC_2                true      Connected to Node_FC_2
Node_FC_2      Node_FC_1                true      Connected to Node_FC_1
Node_IP_1      Node_IP_2                true      Connected to Node_IP_2
Node_IP_2      Node_IP_1                true      Connected to Node_IP_1
```

8. Verschieben Sie die CRS-Volumes.

   Führen Sie die Schritte unter aus "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

9. Verschieben Sie die Daten von den alten Knoten auf die neuen Knoten, indem Sie die folgenden Verfahren durchführen:

   a. Führen Sie alle Schritte in aus "Erstellung eines Aggregats und Verschiebung von Volumes zu den neuen Nodes".

      Sie könnten wählen, um das Aggregat zu spiegeln, wenn oder nachdem es erstellt wurde.

   b. Führen Sie alle Schritte in aus "Verschieben Sie nicht-SAN-Daten-LIFs und Cluster-Management-LIFs auf die neuen Nodes".

10. Ändern Sie die IP-Adresse für den Cluster-Peer der transitionierten Nodes für jedes Cluster:

    a. Identifizieren Sie den Cluster_A-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

       i. Peer-IP-Adresse „Cluster_A“ ändern:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

    b. Identifizieren Sie den Cluster_B-Peer mithilfe der `cluster peer show` Befehl:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

       i. Peer-IP-Adresse für Cluster_B ändern:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

    c. Überprüfen Sie, ob die Cluster-Peer-IP-Adresse für jedes Cluster aktualisiert wurde:

i. Überprüfen Sie mithilfe der, ob die IP-Adresse für jedes Cluster aktualisiert wurde `cluster peer show -instance` Befehl.

   Der `Remote Intercluster Addresses` In den folgenden Beispielen wird die aktualisierte IP-Adresse angezeigt.

   Beispiel für Cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                      Remote Cluster Name: cluster_B
                      Active IP Addresses: 172.21.178.212,
172.21.178.204
                    Cluster Serial Number: 1-80-000011
                     Remote Cluster Nodes: node_B_3-IP,
                                           node_B_4-IP
                    Remote Cluster Health: true
                  Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                          Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+
Beispiel für „Cluster_B“

```
cluster_B::> cluster peer show -instance

                      Peer Cluster Name: cluster_A
           Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                       Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

11. Befolgen Sie die Schritte unter "Entfernen einer Disaster Recovery-Gruppe" Um die alte DR-Gruppe zu entfernen.
12. Wenn Sie beide DR-Gruppen in einer Konfiguration mit acht Nodes aktualisieren möchten, müssen Sie den gesamten Vorgang für jede DR-Gruppe wiederholen.

    Nachdem Sie die alte DR-Gruppe entfernt haben, wird die Konfiguration wie in den folgenden Bildern dargestellt angezeigt:

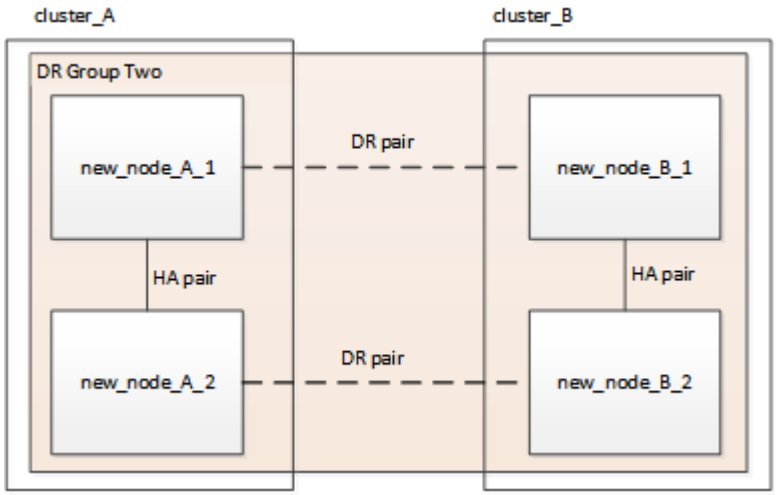


Abbildung 3. Konfiguration mit vier Nodes

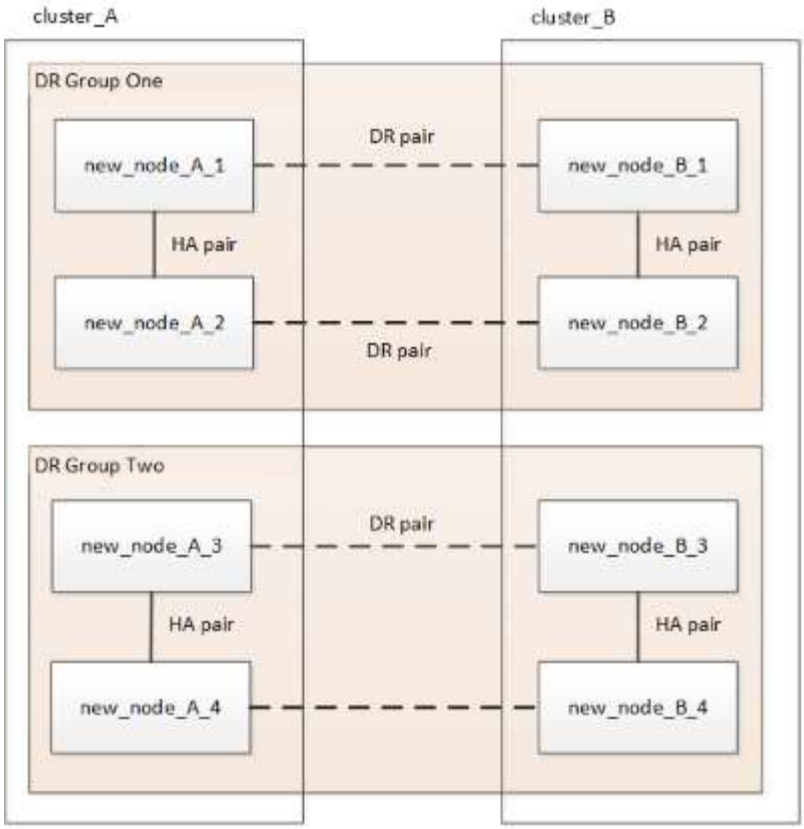


Abbildung 4. Konfiguration mit acht Nodes

13. Überprüfen Sie den Betriebsmodus der MetroCluster Konfiguration, und führen Sie eine MetroCluster-Prüfung durch.
    a. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

    ```
    metrocluster show
    ```

    b. Vergewissern Sie sich, dass alle erwarteten Knoten angezeigt werden:

    ```
    metrocluster node show
    ```

    c. Geben Sie den folgenden Befehl ein:

    ```
    metrocluster check run
    ```

    d. Ergebnisse der MetroCluster-Prüfung anzeigen:

    ```
    metrocluster check show
    ```

14. Wenn Sie die End-to-End-Verschlüsselung vor dem Hinzufügen der neuen Nodes deaktiviert haben, können Sie sie erneut aktivieren, indem Sie die Schritte unter ausführen "End-to-End-Verschlüsselung".
15. Stellen Sie ggf. die Überwachung mithilfe des Verfahrens für Ihre Konfiguration wieder her.

Sie verwenden…	Gehen Sie wie folgt vor

Tiebreaker	"Hinzufügen von MetroCluster Konfigurationen" In der *MetroCluster Tiebreaker Installation und Konfiguration*.
Mediator	"Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" in der *MetroCluster IP-Installation und -Konfiguration*.
Applikationen von Drittanbietern	Siehe Produktdokumentation.

16. Um mit der automatischen Erstellung von Support-Cases fortzufahren, senden Sie eine AutoSupport Meldung, um anzugeben, dass die Wartung abgeschlossen ist.
    a. Geben Sie den folgenden Befehl ein:

    ```
    system node autosupport invoke -node * -type all -message MAINT=end
    ```

    b. Wiederholen Sie den Befehl im Partner-Cluster.

Erweitern Sie eine MetroCluster FC Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes

Erweitern einer MetroCluster FC-Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes

Wenn Sie eine MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster FC-Konfiguration mit vier Nodes erweitern, muss jedem Cluster ein Controller hinzugefügt werden, um an jedem MetroCluster Standort ein HA-Paar zu bilden, und anschließend die MetroCluster FC-Konfiguration aktualisiert werden.

Bevor Sie beginnen

- Auf den Nodes muss ONTAP 9 oder höher in einer MetroCluster FC-Konfiguration ausgeführt werden.

  Frühere Versionen von ONTAP oder MetroCluster IP-Konfigurationen unterstützen dieses Verfahren nicht.

- Wenn die Plattformen in Ihrer Konfiguration mit zwei Nodes in ONTAP 9.2 nicht unterstützt werden und Sie ein Upgrade auf Plattformen planen, die in ONTAP 9.2 *und* zu einem Cluster mit vier Nodes unterstützt werden, müssen Sie die Plattformen in der Konfiguration mit zwei Nodes _aktualisieren, bevor Sie die MetroCluster FC-Konfiguration erweitern.
- Die vorhandene MetroCluster FC-Konfiguration muss sich in einem ordnungsgemäßen Zustand befindet.
- Die Ausrüstung, die Sie hinzufügen, muss unterstützt werden und alle Anforderungen erfüllen, die in den folgenden Verfahren beschrieben sind:

  "Installation und Konfiguration von Fabric-Attached MetroCluster"

  "Installation und Konfiguration von Stretch MetroCluster"

- Sie benötigen verfügbare FC-Switch-Ports, um die neuen Controller und neue Bridges aufnehmen zu können.

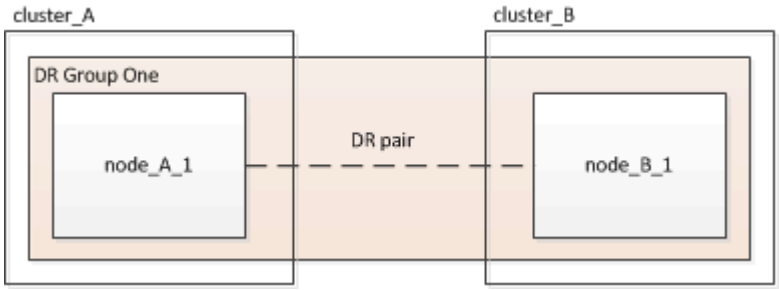
- Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

  Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden, sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

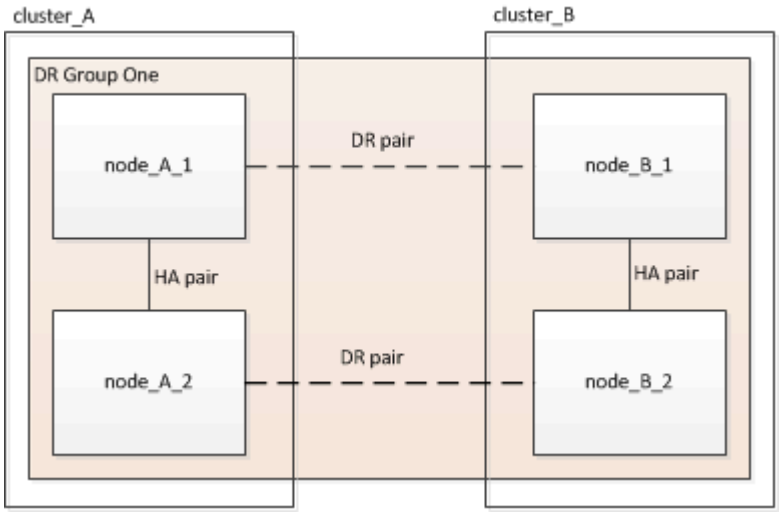
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.

Über diese Aufgabe

- Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen.
- Dieser Vorgang ist mit Unterbrechungen verbunden und dauert etwa vier Stunden.
- Bevor Sie dieses Verfahren durchführen, besteht die MetroCluster FC-Konfiguration aus zwei Single-Node-Clustern:



  Nach Abschluss dieses Verfahrens besteht die MetroCluster FC-Konfiguration aus zwei HA-Paaren an jedem Standort:



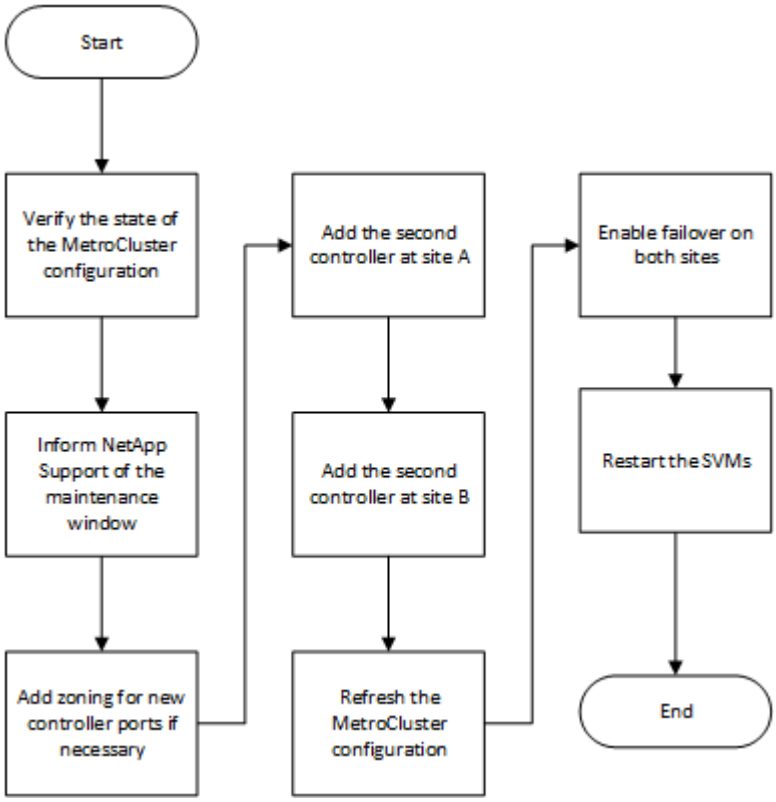
- Beide Standorte müssen gleichermaßen erweitert werden.

  Eine MetroCluster-Konfiguration darf nicht aus einer ungleichmäßigen Anzahl von Nodes bestehen.

- Dieses Verfahren kann pro Standort eine Stunde dauern, wobei zusätzliche Zeit für Aufgaben wie das Initialisieren der Festplatten und das Booten der neuen Nodes ansteht.

  Die Zeit zum Initialisieren der Festplatten hängt von der Größe der Festplatten ab.

- Bei diesem Verfahren wird folgender Workflow verwendet:



Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie diese Aufgabe ausführen.

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Überprüfen des Status der MetroCluster-Konfiguration

Sie sollten die vorhandenen Controller identifizieren und die Disaster Recovery (DR)-Beziehungen zwischen ihnen bestätigen, dass sich die Controller im normalen Modus befinden und die Aggregate gespiegelt werden.

Schritte

1. Zeigt die Details der Nodes in der MetroCluster-Konfiguration von jedem beliebigen Node in der Konfiguration an:

   ```
   metrocluster node show -fields node,dr-partner,dr-partner-systemid
   ```

   Die folgenden Ausgaben zeigen, dass diese MetroCluster Konfiguration über eine einzelne DR-Gruppe und einen Node pro Cluster verfügt.

   ```
   cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
   systemid

   dr-group-id  cluster         node            dr-partner      dr-partner-
   systemid
   -----------  -------------   -------         ----------
   -------------------
   1            cluster_A       controller_A_1  controller_B_1  536946192
   1            cluster_B       controller_B_1  controller_A_1  536946165
   2 entries were displayed.
   ```

2. Zeigt den Status der MetroCluster-Konfiguration an:

   ```
   metrocluster show
   ```

   Die folgende Ausgabe zeigt, dass sich die vorhandenen Nodes in der MetroCluster Konfiguration im normalen Modus befinden:

   ```
   cluster_A::> metrocluster show

   Configuration: two-node-fabric

   Cluster                         Entry Name             State
   ------------------------------- -----------------------
   ---------------------
   Local: cluster_A                Configuration State    configured
                                   Mode                   normal
                                   AUSO Failure Domain    auso-on-cluster-
   disaster
   Remote: controller_B_1_siteB
                                   Configuration State    configured
                                   Mode                   normal
                                   AUSO Failure Domain    auso-on-cluster-
   disaster
   ```

3. Überprüfen Sie den Status der Aggregate auf jedem Node in der MetroCluster Konfiguration:

   ```
   storage aggregate show
   ```

Die folgende Ausgabe zeigt, dass die Aggregate auf Cluster_A online und gespiegelt sind:

```
cluster_A::> storage aggregate show


Aggregate                Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

Senden einer benutzerdefinierten AutoSupport Meldung, bevor Nodes zur MetroCluster Konfiguration hinzugefügt werden

Sie sollten eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei Site_A beim Cluster an
2. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   Der `maintenance-window-in-hours` Der Parameter gibt die Länge des Wartungsfensters an und kann maximal 72 Stunden betragen. Wenn Sie die Wartung vor Ablauf der Zeit abgeschlossen haben, können Sie den folgenden Befehl eingeben, um anzugeben, dass der Wartungszeitraum beendet wurde:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Zoning für die neuen Controller-Ports beim Hinzufügen eines Controller-Moduls in einer Fabric-Attached MetroCluster-Konfiguration

Das FC-Switch-Zoning muss die neuen Controller-Verbindungen aufnehmen. Wenn Sie die von NetApp zur Konfiguration der Switches bereitgestellten Referenzkonfigurationsdateien (RCFs) verwendet haben, ist das Zoning vorkonfiguriert und Sie müssen keine Änderungen vornehmen.

Wenn Sie Ihre FC-Switches manuell konfiguriert haben, müssen Sie sicherstellen, dass das Zoning für die Initiator-Verbindungen der neuen Controller-Module richtig ist. Siehe Abschnitte zum Zoning in "Installation und Konfiguration von Fabric-Attached MetroCluster".

Fügen Sie jedem Cluster ein neues Controller-Modul hinzu

Hinzufügen eines neuen Controller-Moduls zu jedem Cluster

Sie müssen jedem Standort ein neues Controller-Modul hinzufügen, wodurch an jedem Standort ein HA-Paar erstellt wird. Dies ist ein mehrstufiger Prozess, der sowohl Hardware- als auch Softwareänderungen einschließt, die in der richtigen Reihenfolge an jedem Standort durchgeführt werden müssen.

Über diese Aufgabe

- Das neue Controller-Modul muss von NetApp im Rahmen des Upgrade Kits eingehen.

  Sie sollten überprüfen, ob PCIe-Karten im neuen Controller-Modul kompatibel sind und vom neuen Controller-Modul unterstützt werden.

  "NetApp Hardware Universe"

- Ihr System muss beim Upgrade auf ein HA-Paar in einem Chassis über einen leeren Steckplatz für das neue Controller-Modul verfügen (ein HA-Paar, in dem sich beide Controller-Module im selben Chassis befinden).

  > Diese Konfiguration wird nicht auf allen Systemen unterstützt. In ONTAP 9 unterstützte Plattformen mit Einzel-Chassis sind AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080 UND FAS9000.

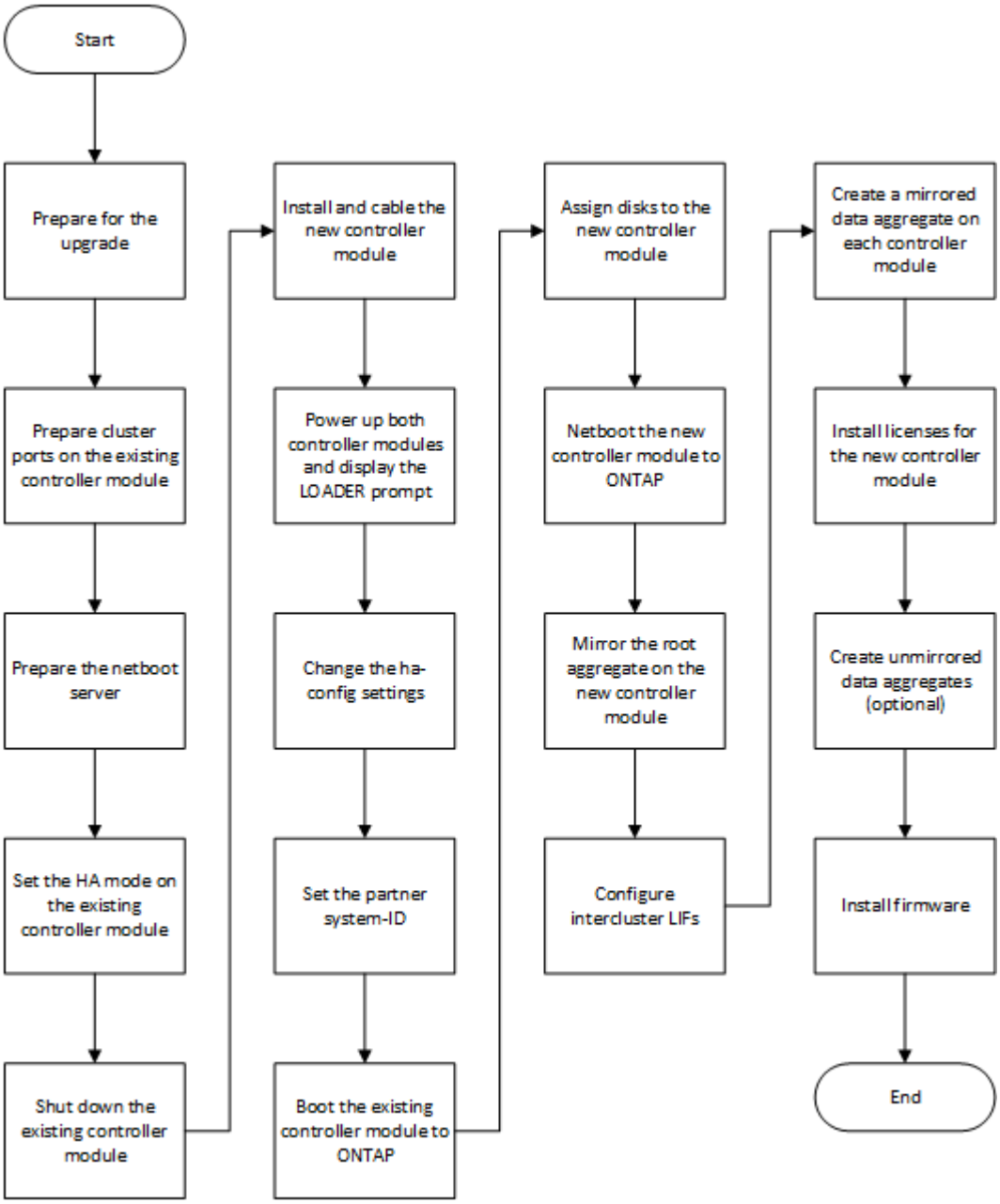
- Bei einem Upgrade auf ein HA-Paar mit zwei Chassis (ein HA-Paar, in dem sich die Controller-Module in einem separaten Chassis befinden) müssen Sie Rack-Platz und Kabel für das neue Controller-Modul haben.

  > Diese Konfiguration wird nicht auf allen Systemen unterstützt.

- Sie müssen jedes Controller-Modul über seinen e0a Port mit dem Management-Netzwerk verbinden, oder, wenn Ihr System einen hat, können Sie als Management-Port eine Verbindung mit dem E0M Port herstellen.
- Diese Aufgaben müssen an jedem Standort wiederholt werden.
- Die bestehenden Controller-Module werden als *vorhandene* Controller-Module bezeichnet.

  Die Beispiele in diesem Verfahren enthalten die Konsolenaufforderung `existing_ctlr>`.

- Die hinzugefügten Controller-Module werden als *neue* Controller-Module bezeichnet; die Beispiele in diesem Verfahren haben die Konsolenaufforderung `new_ctlr>`.
- Diese Aufgabe verwendet den folgenden Workflow:



Vorbereitung auf das Upgrade

Vor dem Upgrade auf ein HA-Paar müssen Sie sicherstellen, dass das System alle Anforderungen erfüllt und alle erforderlichen Informationen enthält.

Schritte

1. Identifizieren Sie nicht zugewiesene Festplatten oder Ersatzfestplatten, die Sie dem neuen Controller-Modul mithilfe folgender Befehle zuweisen können:
    - `storage disk show -container-type spare`
    - `storage disk show -container-type unassigned`

2. Führen Sie die folgenden Teilschritte durch:
   a. Ermitteln Sie, wo sich die Aggregate für den vorhandenen Node befinden:

      ```
      storage aggregate show
      ```

   b. Wenn die automatische Zuweisung für die Festplatteneigentümer aktiviert ist, deaktivieren Sie sie:

      ```
      storage disk option modify -node node_name -autoassign off
      ```

   c. Entfernen Sie sich auf Festplatten, die über keine Aggregate verfügen:

      ```
      storage disk removeowner disk_name
      ```

   d. Wiederholen Sie den vorherigen Schritt für so viele Festplatten wie für den neuen Node.
3. Stellen Sie sicher, dass die Kabel für die folgenden Anschlüsse bereit sind:
   - Cluster-Verbindungen

     Wenn Sie einen 2-Node-Cluster ohne Switches erstellen, müssen Sie die Controller-Module mit zwei Kabeln verbinden. Andernfalls sind mindestens vier Kabel erforderlich, zwei für jede Controller-Modulverbindung zum Cluster-Netzwerk-Switch. Andere Systeme (wie die 80xx Serie) verfügen standardmäßig über vier oder sechs Cluster-Verbindungen.

   - HA Interconnect-Verbindungen, wenn sich das System in einem HA-Paar mit Dual-Chassis befindet
4. Überprüfen Sie, ob eine serielle Port-Konsole für die Controller-Module verfügbar ist.
5. Vergewissern Sie sich, dass die Umgebung den Standort- und Systemanforderungen entspricht.

   "NetApp Hardware Universe"

6. Sammeln Sie alle IP-Adressen und anderen Netzwerkparameter für das neue Controller-Modul.

Löschen der Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

   ```
   boot_ontap menu
   ```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Vorbereiten von Cluster-Ports auf einem vorhandenen Controller-Modul

Vor dem Installieren eines neuen Controller-Moduls müssen Sie Cluster-Ports auf dem vorhandenen Controller-Modul konfigurieren, damit die Cluster-Ports mit dem neuen Controller-Modul kommunizieren können.

Über diese Aufgabe

Wenn Sie einen 2-Node-Cluster ohne Switches erstellen (ohne Cluster-Netzwerk-Switches), müssen Sie den Switch-freien Cluster-Netzwerkmodus aktivieren.

Ausführliche Informationen zur Port-, LIF- und Netzwerkkonfiguration in ONTAP finden Sie unter "Netzwerkmanagement".

Schritte

1. Legen Sie fest, welche Ports als Cluster-Ports des Node verwendet werden sollen.

   Eine Liste der Standard-Portrollen für Ihre Plattform finden Sie im "Hardware Universe"

   Die Anweisungen *Installation and Setup* für Ihre Plattform auf der NetApp Support Site enthalten Informationen zu den Ports für Cluster-Netzwerkverbindungen.

2. Geben Sie für jeden Cluster-Port die Port-Rollen an:

   ```
   network port show
   ```

   Im folgenden Beispiel müssen die Ports „`e0a`“, „`e0b`“, „`e0c`“ und „`e0d`“ in Cluster-Ports geändert werden:

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. Ändern Sie für alle Daten-LIFs, die einen Cluster-Port als Home-Port oder aktuellen Port verwenden, die LIF, um einen Daten-Port als Home-Port zu verwenden:

   `network interface modify`

   Im folgenden Beispiel wird der Home-Port einer Daten-LIF auf einen Daten-Port geändert:

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. Setzen Sie für jede geänderte LIF auf ihren neuen Home-Port zurück:

   `network interface revert`

   Das folgende Beispiel setzt das LIF „`datalif1`“ auf seinen neuen Home-Port „`e1b`“ zurück:

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Entfernen Sie alle VLAN-Ports mithilfe von Cluster-Ports als Mitgliedsports und ifgrps, die Cluster-Ports als Mitgliedsports verwenden.

   a. VLAN-Ports löschen:
      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

Beispiel:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Entfernen Sie physische Ports aus den Schnittstellengruppen:

   `network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

   Beispiel:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Entfernen Sie VLAN und Interface Group Ports aus Broadcast-Domäne:

   `network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname,..`*

b. Ändern Sie die Schnittstellen-Gruppen-Ports, um bei Bedarf andere physische Ports als Mitglied zu verwenden.:
   `ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

6. Vergewissern Sie sich, dass sich die Portrollen geändert haben:

   `network port show`

   Das folgende Beispiel zeigt, dass die Ports „`e0a`“, „`e0b`“, „`e0c`“ und „`e0d`“ nun Cluster-Ports sind:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Fügen Sie die Ports zur Cluster Broadcast Domain hinzu:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id, port-id, port-id…`*

   Beispiel:

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. Wenn Ihr System Teil eines geswitchten Clusters ist, erstellen Sie Cluster-LIFs auf den Cluster-Ports: `network interface create`

   Im folgenden Beispiel wird eine Cluster-LIF auf einem der Cluster-Ports des Node erstellt. Der `-auto` Mit dem Parameter wird das LIF so konfiguriert, dass eine Link-lokale IP-Adresse verwendet wird.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. Wenn Sie einen 2-Node-Cluster ohne Switches erstellen, aktivieren Sie den Cluster-Netzwerkmodus ohne Switch:

   a. Ändern Sie von jedem Node auf die erweiterte Berechtigungsebene:

      `set -privilege advanced`

Sie können antworten `y` Wenn Sie gefragt werden, ob Sie den erweiterten Modus fortsetzen möchten. Die Eingabeaufforderung für den erweiterten Modus wird angezeigt (`*>`).

a. Aktivieren Sie den Cluster-Netzwerkmodus ohne Switches:

```
network options switchless-cluster modify -enabled true
```

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

> Die Erstellung der Cluster-Schnittstelle für den vorhandenen Node in einem 2-Node-Cluster-System ohne Switches wird abgeschlossen, nachdem das Cluster-Setup per Netzboot des neuen Controller-Moduls abgeschlossen wurde.

Vorbereiten des Netzboots-Servers zum Herunterladen des Images

Wenn Sie den Netzboot-Server vorbereiten möchten, müssen Sie das korrekte ONTAP-Netzboot-Image von der NetApp Support Site auf den Netzboot-Server herunterladen und die IP-Adresse beachten.

Über diese Aufgabe

- Sie müssen vor und nach dem Hinzufügen des neuen Controller-Moduls auf einen HTTP-Server aus dem System zugreifen können.
- Sie müssen auf die NetApp Support-Website zugreifen können, um die erforderlichen Systemdateien für Ihre Plattform und Ihre Version von ONTAP herunterzuladen.

  "NetApp Support Website"

- Beide Controller-Module im HA-Paar müssen dieselbe Version von ONTAP ausführen.

Schritte

1. Laden Sie die entsprechende ONTAP Software im Bereich Software Downloads auf der NetApp Support Website herunter und speichern Sie die `<ontap_version>_image.tgz` Datei in einem webbasierten Verzeichnis.

   Der `<ontap_version>_image.tgz` Die Datei wird zum Ausführen eines Netzboots des Systems verwendet.

2. Wechseln Sie in das Verzeichnis für den Zugriff über das Internet, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Für…	Dann…

SYSTEME DER FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 SERIE	Extrahieren Sie den Inhalt der Datei <ontap_version>_image.tgz in das Zielverzeichnis:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Wenn Sie die Inhalte unter Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot-Bild zu extrahieren.
	
	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten:
	
	`netboot/kernel`

Alle anderen Systeme	Ihre Verzeichnisliste sollte die folgende Datei enthalten: `<ontap_version>_image.tgz` Der Dateiinhalt muss nicht extrahiert werden.

3. Ermitteln Sie die IP-Adresse des vorhandenen Controller-Moduls.

   Diese Adresse wird später in diesem Verfahren als bezeichnet *ip-address-of-existing controller*.

4. Ping *ip-address-of-existing controller* Um zu überprüfen, ob die IP-Adresse erreichbar ist.

Einstellen des HA-Modus auf dem vorhandenen Controller-Modul

Sie müssen den Befehl Storage Failover modify verwenden, um den Modus des vorhandenen Controller-Moduls einzustellen. Der Modus-Wert wird später aktiviert, nachdem Sie das Controller-Modul neu gebootet haben.

Schritte

1. Setzen Sie den Modus auf HA:

   ```
   storage failover modify -mode ha -node existing_node_name
   ```

Herunterfahren des vorhandenen Controller-Moduls

Sie müssen das vorhandene Controller-Modul sauber herunterfahren, um zu überprüfen, ob alle Daten auf die Festplatte geschrieben wurden. Sie müssen auch die Netzteile trennen.

Über diese Aufgabe

Sie müssen ein sauberes System herunterfahren, bevor Sie die Systemkomponenten ersetzen, um zu vermeiden, dass die nicht geschriebenen Daten in NVRAM oder NVMEM verloren gehen.

Schritte

1. Stoppen Sie den Knoten von der vorhandenen Eingabeaufforderung für das Controller-Modul:

   ```
   halt local -inhibit-takeover true
   ```

   Wenn Sie aufgefordert werden, den Vorgang zum Anhalten fortzusetzen, geben Sie ein `y` Wenn Sie dazu aufgefordert werden, und warten Sie, bis das System an der LOADER-Eingabeaufforderung angehalten wird.

   In einem 80xx-System befindet sich die NVRAM-LED auf dem Controller-Modul rechts neben den Netzwerkports, die mit einem Batteriesymbol gekennzeichnet sind.

   Diese LED blinkt, wenn nicht geschriebene Daten im NVRAM vorhanden sind. Wenn diese LED gelb blinkt, nachdem Sie den Befehl zum Anhalten eingegeben haben, müssen Sie das System neu booten und versuchen, das System erneut zu stoppen.

2. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
3. Schalten Sie die Netzteile aus und trennen Sie die Stromversorgung mit der richtigen Methode für Ihr System und Ihren Netzteiltyp:

Setzt Ihr System Folgendes ein:	Dann…
Netzteile	Ziehen Sie die Netzkabel von der Stromversorgung ab, und entfernen Sie anschließend die Netzkabel.
Gleichstromnetzteile	Trennen Sie die Stromversorgung an der Gleichstromquelle, und entfernen Sie ggf. die Gleichstromkabel.

Installieren und verkabeln Sie das neue Controller-Modul

Installieren und Verkabeln des neuen Controller-Moduls

Sie müssen das neue Controller-Modul physisch im Chassis installieren und anschließend verkabeln.

Schritte

1. Wenn Sie ein I/O-Erweiterungsmodul (IOXM) in Ihrem System haben und ein HA-Paar mit einem Chassis erstellen, müssen Sie das IOXM aufheben und entfernen.

   Anschließend können Sie den leeren Schacht für das neue Controller-Modul verwenden. Allerdings bietet die neue Konfiguration nicht die zusätzliche I/O-Leistung des IOXM.

2. Installieren Sie das neue Controller-Modul physisch und installieren Sie bei Bedarf weitere Lüfter:

Wenn Sie ein Controller-Modul hinzufügen…	Führen Sie dann folgende Schritte aus…

Bei einem leeren Schacht für das Erstellen eines HA-Paars mit einem Chassis gehört das System zu einer der folgenden Plattformen:	a. Entfernen Sie die leere Platte auf der Rückseite des Gehäuses, die den leeren Schacht, der das neue Controller-Modul enthält, abdeckt. b. Schieben Sie das Controller-Modul vorsichtig zur Hälfte in das Gehäuse. Um zu verhindern, dass das Controller-Modul automatisch gebootet werden kann, setzen Sie es erst später in diesem Verfahren vollständig im Chassis ein.
In einem separaten Chassis vom HA-Partner zur Erstellung eines HA-Paares mit Dual-Chassis, wenn sich die vorhandene Konfiguration in einer Controller-IOX-Modul-Konfiguration befindet. • FAS8200 • 80xx	Installieren Sie das neue System im Rack oder Systemschrank.

3. Netzwerkkabel des Clusters nach Bedarf verkabeln:

   a. Identifizieren Sie die Ports auf dem Controller-Modul für die Cluster-Verbindungen.

      "AFF A320-Systeme: Installation und Einrichtung"

      "Installations- und Setup-Anleitung für AFF A220/FAS2700 Systeme"

      "Installations- und Setup-Anleitung für AFF A800 Systeme"

      "Installations- und Setup-Anleitung für AFF A300 Systeme"

      "FAS8200 Systems Installation and Setup instructions"

   b. Wenn Sie ein Switch-Cluster konfigurieren, geben Sie die Ports an, die Sie auf den Cluster-Netzwerk-Switches verwenden möchten.

      Siehe "Konfigurationsleitfaden für Clustered Data ONTAP Switches für Cisco Switches", "^NetApp 10G Cluster-Mode-Switch Installationshandbuch" Oder "Installationshandbuch für den NetApp 1G Cluster-Mode Switch", Je nachdem, welche Schalter Sie verwenden.

   c. Verbinden Sie die Kabel mit den Cluster-Ports:

Falls das Cluster…	Dann…
Zwei-Node-Cluster ohne Switches	Verbinden Sie die Cluster-Ports des vorhandenen Controller-Moduls direkt mit den entsprechenden Cluster-Ports des neuen Controller-Moduls.
Cluster mit Switches	Verbinden Sie die Cluster-Ports an jedem Controller mit den Ports auf den in Unterschritt B angegebenen Cluster-Netzwerk-Switches

Verkabelung der FC-VI- und HBA-Ports des neuen Controller-Moduls an die FC-Switches

Die FC-VI-Ports und HBAs (Host Bus Adapter) des neuen Controller-Moduls müssen mit den FC-Switches am Standort verbunden sein.

Schritte

1. Verkabeln Sie die FC-VI-Ports und HBA-Ports mit der Tabelle für Ihre Konfiguration und Ihr Switch-Modell.
   - "Portzuweisungen für FC-Switches"
   - "Port-Zuweisungen für Systeme mit zwei Initiator-Ports"

Verkabelung der Cluster-Peering-Verbindungen des neuen Controller-Moduls

Sie müssen das neue Controller-Modul mit dem Cluster-Peering-Netzwerk verkabeln, damit es eine Verbindung mit dem Cluster am Partnerstandort hat.

Über diese Aufgabe

Mindestens zwei Ports auf jedem Controller-Modul sollten für Cluster-Peering verwendet werden.

Die empfohlene minimale Bandbreite für die Ports und Netzwerkkonnektivität ist 1 GbE.

Schritte

1. Identifizieren und verkabeln Sie mindestens zwei Ports für Cluster-Peering und vergewissern Sie sich, dass sie über eine Netzwerkverbindung mit dem Partner-Cluster verfügen.

Einschalten beider Controller-Module und Anzeigen der LOADER-Eingabeaufforderung

Sie schalten das vorhandene Controller-Modul und das neue Controller-Modul ein, um die LOADER-Eingabeaufforderung anzuzeigen.

Schritte

Schalten Sie die Controller-Module aus und unterbrechen Sie den Bootvorgang, indem Sie die Schritte für Ihre Konfiguration verwenden:

Wenn die Controller-Module…	Dann…

Im gleichen Chassis	1. Vergewissern Sie sich, dass das neue Controller-Modul **nicht** vollständig in den Schacht eingesetzt ist. Das vorhandene Controller-Modul sollte vollständig in den Schacht eingesetzt werden, da es nie aus dem Chassis entfernt wurde, das neue Controller-Modul jedoch nicht sein sollte. 2. Schließen Sie das Netzteil an, und schalten Sie die Netzteile ein, sodass das vorhandene Controller-Modul mit Strom versorgt wird. 3. Unterbrechen Sie den Boot-Vorgang des vorhandenen Controller-Moduls, indem Sie Strg-C drücken 4. Drücken Sie das neue Controller-Modul fest in den Schacht. Wenn das neue Controller-Modul voll eingesetzt ist, wird es mit Strom versorgt und wird automatisch gestartet. 5. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken 6. Ziehen Sie ggf. die Daumenschraube am Nockengriff fest. 7. Installieren Sie das Kabelverwaltungsgerät, falls vorhanden. 8. Verbinden Sie die Kabel mit dem Haken- und Schlaufenband mit dem Kabelmanagement-Gerät.
In einem separaten Chassis	1. Schalten Sie die Netzteile des vorhandenen Controller-Moduls ein. 2. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken 3. Wiederholen Sie diese Schritte für das neue Controller-Modul

Jedes Controller-Modul sollte die LOADER-Eingabeaufforderung anzeigen (`LOADER>`, `LOADER-A>`, Oder `LOADER-B>`).

> Wenn keine LOADER-Eingabeaufforderung angezeigt wird, notieren Sie die Fehlermeldung. Wenn das Startmenü angezeigt wird, starten Sie den Neustart neu, und versuchen Sie erneut, den Bootvorgang zu unterbrechen.

Ändern der HA-Konfigurationseinstellung für die vorhandenen und neuen Controller-Module

Wenn Sie eine MetroCluster-Konfiguration erweitern, müssen Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls und des neuen Controller-Moduls aktualisieren. Sie müssen außerdem die System-ID des neuen Controller-Moduls bestimmen.

Über diese Aufgabe

Diese Aufgabe wird sowohl bei vorhandenen als auch bei neuen Controller-Modulen im Wartungsmodus ausgeführt.

Schritte

1. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls:

a. Zeigen Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls und des Gehäuses an:

```
ha-config show
```

Die HA-Konfigurationseinstellung ist für alle Komponenten „`mcc-2n`“, da sich das Controller-Modul in einer MetroCluster-Konfiguration mit zwei Knoten befand.

b. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Controller-Moduls in „`mcc`“:
`ha-config modify controller mcc`

c. Ändern Sie die HA-Konfigurationseinstellung des vorhandenen Gehäuses in „`mcc`“:

```
ha-config modify chassis mcc
```

d. Rufen Sie die System-ID für das vorhandene Controller-Modul ab:

```
sysconfig
```

Notieren Sie die System-ID. Sie benötigen es, wenn Sie die Partner-ID auf dem neuen Controller-Modul einstellen.

a. Beenden Sie den Wartungsmodus, um zur LOADER-Eingabeaufforderung zurückzukehren:

```
halt
```

2. Ändern Sie die HA-Konfigurationseinstellung und rufen Sie die System-ID des neuen Controller-Moduls ab:

a. Wenn sich das neue Controller-Modul nicht bereits im Wartungsmodus befindet, starten Sie es in den Wartungsmodus:

```
boot_ontap maint
```

b. Ändern Sie die HA-Konfigurationseinstellung des neuen Controller-Moduls in „`mcc`“:

```
ha-config modify controller mcc
```

c. Ändern Sie die HA-Konfigurationseinstellung des neuen Chassis in mcc:

```
ha-config modify chassis mcc
```

d. Rufen Sie die System-ID für das neue Controller-Modul ab:

```
sysconfig
```

Notieren Sie die System-ID. Sie benötigen es, wenn Sie die Partner-ID festlegen und dem neuen Controller-Modul Festplatten zuweisen.

a. Beenden Sie den Wartungsmodus, um zur LOADER-Eingabeaufforderung zurückzukehren:

```
halt
```

Festlegen der Partner-System-ID für beide Controller-Module

Sie müssen die Partner-System-ID auf beiden Controller-Modulen festlegen, damit sie ein HA-Paar bilden können.

Über diese Aufgabe

Dieser Task wird an der LOADER-Eingabeaufforderung mit beiden Controller-Modulen ausgeführt.

Schritte

1. Legen Sie im vorhandenen Controller-Modul die Partner-System-ID auf die des neuen Controller-Moduls fest:

   ```
   setenv partner-sysid sysID_of_new_controller
   ```

2. Stellen Sie bei dem neuen Controller-Modul die Partner-System-ID auf die des vorhandenen Controller-Moduls ein:

   ```
   setenv partner-sysid sysID_of_existing_controller
   ```

Booten des vorhandenen Controller-Moduls

Sie müssen das vorhandene Controller-Modul bei ONTAP booten.

Schritte

1. Booten Sie an der LOADER-Eingabeaufforderung das vorhandene Controller-Modul in ONTAP:

   ```
   boot_ontap
   ```

Zuweisen von Festplatten zum neuen Controller-Modul

Bevor Sie die Konfiguration des neuen Controller-Moduls über einen Netzboot ausführen, müssen Sie ihm Festplatten zuweisen.

Über diese Aufgabe

Sie müssen sicherstellen, dass genügend Ersatzteile, nicht zugewiesene Festplatten oder zugewiesene Festplatten nicht Teil eines vorhandenen Aggregats sind.

"Vorbereitung auf das Upgrade"

Diese Schritte werden am vorhandenen Controller-Modul durchgeführt.

Schritte

1. Weisen Sie die Root-Festplatte dem neuen Controller-Modul zu:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

   Wenn Ihr Plattformmodell die ADP-Funktion (Advanced Drive Partitioning) verwendet, müssen Sie den Parameter -root true angeben:

   ```
   storage disk assign -disk disk_name -root true -sysid new_controller_sysID
   -force true
   ```

2. Weisen Sie dem neuen Controller-Modul die verbleibenden erforderlichen Festplatten zu, indem Sie für jede Festplatte den folgenden Befehl eingeben:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

3. Vergewissern Sie sich, dass die Festplattenzuordnungen korrekt sind:

   ```
   storage disk show -partitionownership*
   ```

   Stellen Sie sicher, dass Sie alle Laufwerke zugewiesen haben, die Sie dem neuen Knoten zuweisen möchten.

Booten und Einrichten von ONTAP auf dem neuen Controller-Modul

Sie müssen eine bestimmte Sequenz von Schritten zum Netzboot ausführen und das ONTAP Betriebssystem auf dem neuen Controller-Modul installieren, wenn Sie einer vorhandenen MetroCluster Konfiguration Controller-Module hinzufügen.

Über diese Aufgabe

- Diese Aufgabe wird bei der LOADER-Eingabeaufforderung des neuen Controller-Moduls gestartet.
- Diese Aufgabe umfasst die Initialisierung von Datenträgern.

  Die Dauer, die zur Initialisierung der Festplatten benötigt wird, hängt von der Größe der Festplatten ab.

- Das System weist dem neuen Controller-Modul automatisch zwei Festplatten zu.

  "Festplatten- und Aggregatmanagement"

Schritte

1. Konfigurieren Sie an der LOADER-Eingabeaufforderung die IP-Adresse des neuen Controller-Moduls basierend auf der DHCP-Verfügbarkeit:

DHCP ist…	Geben Sie dann den folgenden Befehl ein…
Verfügbar	**`ifconfig e0M -auto`**

Nicht verfügbar	`ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain` *`filer_addr`* Ist die IP-Adresse des Storage-Systems. *`netmask`* Ist die Netzwerkmaske des Storage-Systems. *`gateway`* Ist das Gateway für das Storage-System. *`dns_addr`* Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk. *`dns_domain`* Der Domain Name (DNS) ist der Domain-Name. Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie in der Netzboot-Server-URL keinen vollqualifizierten Domänennamen. Sie benötigen nur den Host-Namen des Servers. Andere Parameter können für Ihre Schnittstelle erforderlich sein. Verwenden Sie für Details den `help ifconfig` Befehl an der LOADER-Eingabeaufforderung.

2. An der LOADER-Eingabeaufforderung „Netzboot“ des neuen Node:

Für…	Geben Sie diesen Befehl aus…
SYSTEME DER FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 SERIE	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Alle anderen Systeme	`netboot \http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

Der *`path_to_the_web-accessible_directory`* Befindet sich der Speicherort des heruntergeladenen `<ontap_version>_image.tgz` Datei:

3. Wählen Sie im angezeigten Menü die Option **Neue Software zuerst installieren** aus.

   Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

   - Sie sollten „`y`“ eingeben, wenn Sie dazu aufgefordert werden, dass dieses Verfahren nicht für ein unterbrechungsfreies Upgrade auf einem HA-Paar unterstützt wird.
   - Sie sollten „`y`“ eingeben, wenn Sie darauf hingewiesen werden, dass dieser Prozess die vorhandene ONTAP-Software durch neue Software ersetzt.
   - Sie sollten bei der Aufforderung zur URL der Datei image.tgz den Pfad wie folgt eingeben:

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Geben Sie „`y`“ ein, wenn Sie dazu aufgefordert werden, ein unterbrechungsfreies Upgrade oder Austausch der Software zu starten.

5. Geben Sie den Pfad zur Datei image.tgz ein, wenn Sie zur URL des Pakets aufgefordert werden.

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. Geben Sie „n“ ein, um die Backup-Wiederherstellung zu überspringen, wenn Sie dazu aufgefordert werden, die Backup-Konfiguration wiederherzustellen.

```
*****************************************************************
*             Restore Backup Configuration                      *
*  This procedure only applies to storage controllers that      *
*  are configured as an HA pair.                                *
*                                                               *
*  Choose Yes to restore the "varfs" backup configuration       *
*  from the SSH server.  Refer to the Boot Device Replacement   *
*  guide for more details.                                      *
*  Choose No to skip the backup recovery and return to the      *
*  boot menu.                                                   *
*****************************************************************

Do you want to restore the backup configuration
now? {y|n} `n`
```

7. Geben Sie „y“ ein, wenn Sie dazu aufgefordert werden, den Neustart jetzt durchzuführen.

```
The node must be rebooted to start using the newly installed software.
Do you want to
reboot now? {y|n} `y`
```

8. Wählen Sie bei Bedarf die Option **Clean Configuration aus und initialisieren Sie alle Festplatten**, nachdem der Knoten gestartet wurde.

   Da Sie ein neues Controller-Modul konfigurieren und die Festplatten des neuen Controller-Moduls leer sind, können Sie „y“ antworten, wenn das System Sie darauf warnt, dass alle Festplatten gelöscht werden.

   > Die Zeit, die zum Initialisieren von Festplatten benötigt wird, hängt von der Größe der Festplatten und der Konfiguration ab.

9. Nachdem die Festplatten initialisiert wurden und der Setup-Assistent für das Cluster gestartet wurde, richten Sie den Node ein:

   Geben Sie die LIF-Informationen zum Node-Management auf der Konsole ein.

10. Melden Sie sich bei dem Node an, und geben Sie den ein `cluster setup` Und geben Sie dann „`join`“ ein, wenn Sie dazu aufgefordert werden, dem Cluster beizutreten.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. Beantworten Sie die verbleibenden Eingabeaufforderungen für Ihren Standort.

    Der "Einrichtung von ONTAP" Für Ihre Version von ONTAP enthält zusätzliche Details.

12. Wenn sich das System in einer 2-Node-Konfiguration ohne Switches befindet, erstellen Sie die Cluster-Schnittstellen auf dem vorhandenen Node. Verwenden Sie dabei den Befehl „Network Interface create“, um Cluster LIFs auf den Cluster-Ports zu erstellen.

    Der folgende Befehl ist ein Beispiel zum Erstellen einer Cluster-LIF auf einem der Cluster-Ports des Node. Der Parameter -Auto konfiguriert das LIF so, dass eine Link-lokale IP-Adresse verwendet wird.

    ```
    cluster_A::> network interface create -vserver Cluster -lif clus1 -role
    cluster -home-node node_A_1 -home-port e1a -auto true
    ```

13. Nach Abschluss der Einrichtung vergewissern Sie sich, dass der Node sich in einem ordnungsgemäßen Zustand befindet und berechtigt ist, am Cluster teilzunehmen:

    ```
    cluster show
    ```

    Das folgende Beispiel zeigt einen Cluster, nachdem der zweite Node (cluster1-02) damit verbunden wurde:

    ```
    cluster_A::> cluster show
    Node                  Health  Eligibility
    --------------------- ------- ------------
    node_A_1              true    true
    node_A_2              true    true
    ```

    Sie können mit dem Cluster Setup-Assistenten einen der Werte, die Sie für die SVM (Admin Storage Virtual Machine) oder Node-SVM eingegeben haben, über den Cluster-Setup-Befehl ändern.

14. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

    ```
    network port show
    ```

    Das folgende Beispiel zeigt die Ausgabe für zwei Controller-Module in „Cluster_A“:

```
cluster_A::> network port show
                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

Spiegelung des Root-Aggregats auf dem neuen Controller

Sie müssen das Root-Aggregat spiegeln, um Datensicherung zu ermöglichen, wenn Sie einer MetroCluster-Konfiguration einen Controller hinzufügen.

Diese Aufgabe muss am neuen Controller-Modul ausgeführt werden.

1. Root-Aggregat spiegeln:

   `storage aggregate mirror` *`aggr_name`*

   Der folgende Befehl spiegelt das Root-Aggregat für Controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

Konfigurieren Sie Intercluster LIFs

Erfahren Sie, wie Sie Intercluster LIFs auf dedizierten und gemeinsam genutzten Ports konfigurieren.

Konfigurieren Sie Intercluster-LIFs auf dedizierten Ports

Es können Intercluster LIFs an dedizierten Ports konfiguriert werden, um die verfügbare Bandbreite für den Replizierungsdatenverkehr zu erhöhen.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                                    Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   `network interface show -fields home-port,curr-port`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   ```
   network interface failover-groups create -vserver <system_SVM> -failover
   -group <failover_group> -targets <physical_or_logical_ports>
   ```

   Das folgende Beispiel weist den Failover-Gruppe „intercluster01“ auf der System-SVM „cluster01“ die Ports „e0e“ und „e0f“ zu:

   ```
   cluster01::> network interface failover-groups create -vserver
   cluster01 -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   ```
   network interface failover-groups show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  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
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>`
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_ic.01“ und „cluster01_ic02“ in der Failover-Gruppe „intercluster01“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:

`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem SVM „e0e“-Port an den „e0f“-Port scheitern.

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Konfigurieren Sie Intercluster-LIFs an gemeinsam genutzten Datenports

Es können Intercluster LIFs an Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden, um die Anzahl der Ports zu reduzieren, die Sie für ein Intercluster-Netzwerk benötigen.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

Im ONTAP 9.6 und höher:
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
In ONTAP 9.5 und früher:
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:

`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern wird.

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

  In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-

Konfiguration ermittelt haben.

"Festplatten- und Aggregatmanagement"

> Es wird empfohlen, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   ```
   storage disk show -spare -owner node_name
   ```

2. Erstellen Sie das Aggregat:

   ```
   storage aggregate create -mirror true
   ```

   Wenn Sie 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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke

     > In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

     Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Installieren von Lizenzen für das neue Controller-Modul

Lizenzen für das neue Controller-Modul müssen für alle ONTAP Services hinzugefügt werden, die Standard-Lizenzen (mit Nodes gesperrt) erfordern. Bei Standardlizenzen muss jeder Node im Cluster über seinen eigenen Schlüssel für die Funktion verfügen.

Ausführliche Informationen zur Lizenzierung finden Sie in der Knowledge Base-Artikel 3013749: Übersicht über die Data ONTAP 8.2 Lizenzierung und Referenzen auf der NetApp Support Site und *System Administration Reference*.

Schritte

1. Falls erforderlich, beziehen Sie Lizenzschlüssel für den neuen Node auf der NetApp Support Site im Abschnitt „My Support“ unter „Software-Lizenzen“.

   Weitere Informationen zum Austausch von Lizenzen finden Sie im Knowledge Base-Artikel "Verfahren zum Austausch der Hauptplatine zur Aktualisierung der Lizenzierung auf einem All Flash FAS/FAS System"

2. Geben Sie den folgenden Befehl ein, um jeden Lizenzschlüssel zu installieren:

   `system license add -license-code` *`license_key`*

   Der *`license_key`* Ist 28 Ziffern lang.

3. Wiederholen Sie diesen Schritt für jede erforderliche Standard-Lizenz (Node-locked).

Erstellen von nicht gespiegelten Datenaggregaten

Optional können Sie nicht gespiegelte Datenaggregate für Daten erstellen, für die keine redundante Spiegelung von MetroCluster-Konfigurationen erforderlich ist.

Über diese Aufgabe

- Stellen Sie sicher, dass Sie wissen, welche Laufwerke im neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie überprüfen können, ob der richtige Laufwerkstyp ausgewählt ist.

> In MetroCluster IP-Konfigurationen können Remote-Aggregate nach einem Switchover nicht zugänglich gemacht werden

Die nicht gespiegelten Aggregate müssen sich lokal an dem Node halten, auf dem sie sich enthalten.

- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- *Festplatten- und Aggregatmanagement* enthält weitere Informationen zur Spiegelung von Aggregaten.

Schritte

1. Installieren und verkabeln Sie die Festplatten-Shelfs, die die nicht gespiegelten Aggregate enthalten.

   Sie können die Verfahren in der Dokumentation *Installation and Setup* für Ihre Plattform und Platten-Shelfs verwenden.

   "Dokumentation zu ONTAP Hardwaresystemen"

2. Weisen Sie alle Festplatten auf dem neuen Shelf dem entsprechenden Node manuell zu:

   ```
   disk assign -disk <disk-id> -owner <owner-node-name>
   ```

3. Erstellen Sie das Aggregat:

   ```
   storage aggregate create
   ```

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Node erstellt wird, sollten Sie das verwenden `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

   Vergewissern Sie sich, dass Sie nur Laufwerke auf dem nicht gespiegelten Shelf zum Aggregat hinzufügen.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

Mit dem folgenden Befehl wird ein nicht gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

+

> Sie können auch mit dem `-disklist` Parameter im Befehl die Festplatten angeben, die Sie für das Aggregat verwenden möchten.

4. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   ```
   storage aggregate show-status -aggregate <aggregate-name>
   ```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Installieren der Firmware nach dem Hinzufügen eines Controller-Moduls

Nach dem Hinzufügen des Controller-Moduls müssen Sie die aktuelle Firmware auf dem neuen Controller-Modul installieren, damit das Controller-Modul ordnungsgemäß mit ONTAP funktioniert.

Schritte

1. Laden Sie die aktuelle Firmware-Version für Ihr System herunter und befolgen Sie die Anweisungen zum Herunterladen und Installieren der neuen Firmware.

   "NetApp Downloads: System-Firmware und -Diagnose"

Aktualisierung der MetroCluster Konfiguration durch neue Controller

Sie müssen die MetroCluster Konfiguration aktualisieren, wenn Sie sie von einer Konfiguration mit zwei Nodes auf eine Konfiguration mit vier Nodes erweitern.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Rufen Sie den erweiterten Berechtigungsmodus auf:
      `set -privilege advanced`

   b. Aktualisieren Sie die MetroCluster-Konfiguration:
      `metrocluster configure -refresh true -allow-with-one-aggregate true`

      Mit dem folgenden Befehl wird die MetroCluster-Konfiguration auf allen Nodes in der DR-Gruppe aktualisiert, die Controller_A_1 enthält:

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

a. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

```
network port show
```

Im folgenden Beispiel wird die Verwendung von Netzwerkports in einer MetroCluster Konfiguration mit vier Nodes angezeigt:

```
cluster_A::> network port show
                                                          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
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

a. Überprüfen Sie die Konfiguration von Standort A:

```
metrocluster show
```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Überprüfen Sie die Konfiguration von Standort B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

c. Überprüfen Sie, ob die DR-Beziehungen korrekt erstellt wurden:

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
```

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Aktivieren von Storage Failover auf beiden Controller-Modulen und Aktivieren von Cluster HA

Nachdem Sie der MetroCluster Konfiguration neue Controller-Module hinzugefügt haben, müssen Sie Storage Failover auf beiden Controller-Modulen aktivieren und die separat aktiviert werden.

Bevor Sie beginnen

Die MetroCluster Konfiguration muss zuvor mit dem aktualisiert worden sein `metrocluster configure -refresh true` Befehl.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Storage-Failover:

   `storage failover modify -enabled true -node` *`existing-node-name`*

   Der einzelne Befehl ermöglicht ein Storage Failover beider Controller-Module.

2. Vergewissern Sie sich, dass Storage-Failover aktiviert ist:

   `storage failover show`

   Die Ausgabe sollte wie folgt aussehen:

```
Node            Partner         Possible State Description
--------------- --------------- -------- ----------------------
old-ctlr         new-ctlr       true      Connected to new-ctlr
new-ctlr         old-ctlr       true      Connected to old-ctlr
2 entries were displayed.
```

3. Cluster-HA aktivieren:

   ```
   cluster ha modify -configured true
   ```

   Cluster High Availability (HA) muss in einem Cluster konfiguriert werden, wenn es nur zwei Nodes enthält und sich von der durch Storage Failover gelieferten HA unterscheidet.

Starten Sie die SVMs neu

Nach erweitern der MetroCluster Konfiguration müssen Sie die SVMs neu starten.

Schritte

1. Identifizieren Sie die SVMs, die neu gestartet werden müssen:

   ```
   metrocluster vserver show
   ```

   Dieser Befehl zeigt die SVMs auf beiden MetroCluster Clustern.

2. Starten Sie die SVMs auf dem ersten Cluster neu:
   a. Rufen Sie den erweiterten Berechtigungsmodus auf, und drücken Sie **y** Wenn Sie dazu aufgefordert werden:

      ```
      set -privilege advanced
      ```

   b. Starten Sie die SVMs neu:

      ```
      vserver start -vserver SVM_name -force true
      ```

   c. Zurück zum Admin-Berechtigungsmodus:

      ```
      set -privilege admin
      ```

3. Wiederholen Sie den vorherigen Schritt im Partner-Cluster.
4. Vergewissern Sie sich, dass sich die SVMs in einem ordnungsgemäßen Zustand befinden:

   ```
   metrocluster vserver show
   ```

Erweitern Sie eine MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes

Erweitern einer MetroCluster FC-Konfiguration mit vier Nodes auf eine Konfiguration mit acht Nodes

Um eine MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes zu erweitern, müssen jedem Cluster zwei Controller hinzugefügt werden. So bilden sie an jedem MetroCluster Standort ein zweites HA-Paar, und anschließend werden der MetroCluster FC-Konfigurationsvorgang ausgeführt.

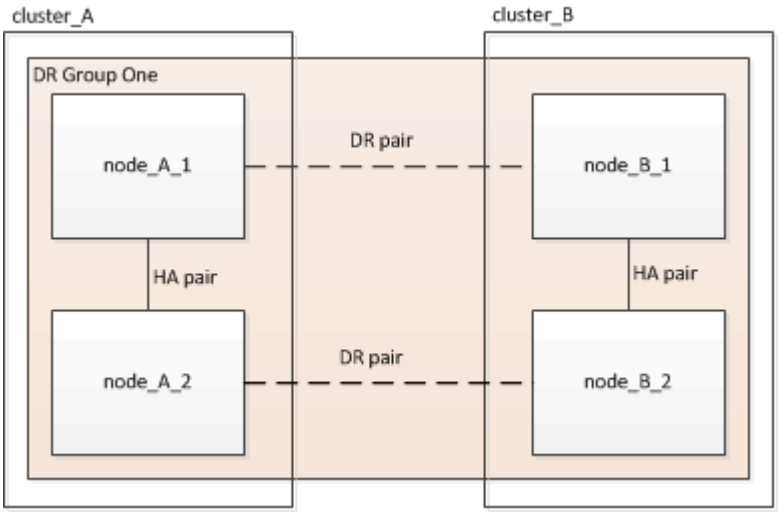
Über diese Aufgabe

- Die Knoten müssen ONTAP 9 in einer MetroCluster FC-Konfiguration ausführen.

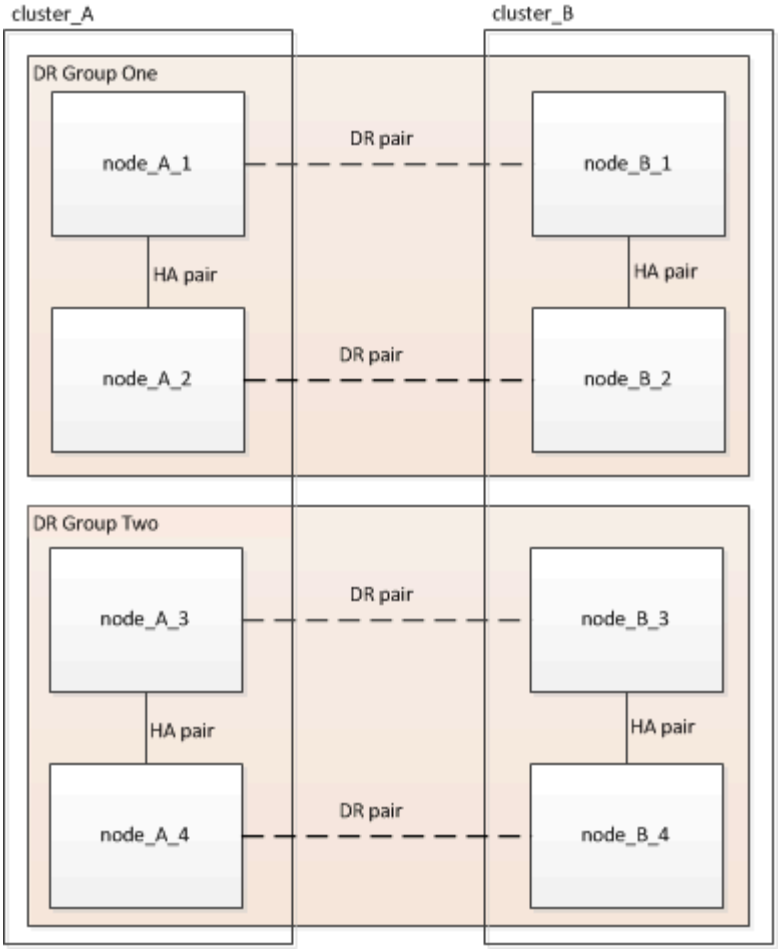
  Frühere Versionen von ONTAP oder MetroCluster IP-Konfigurationen unterstützen dieses Verfahren nicht.

- Die vorhandene MetroCluster FC-Konfiguration muss sich in einem ordnungsgemäßen Zustand befindet.
- Die Geräte, die Sie hinzufügen, müssen unterstützt werden und alle in beschriebenen Anforderungen erfüllen "Installation und Konfiguration von Fabric-Attached MetroCluster"
- Sie benötigen verfügbare FC-Switch-Ports, um die neuen Controller und neue Bridges aufnehmen zu können.
- Sie benötigen das Admin-Passwort und den Zugriff auf einen FTP- oder SCP-Server.
- Dieses Verfahren gilt nur für MetroCluster FC-Konfigurationen.
- Diese Vorgehensweise verursacht keine Unterbrechungen und dauert etwa einen Tag (ausgenommen Rack und Stack), wenn Festplatten gelöscht werden.

Bevor Sie dieses Verfahren durchführen, besteht die MetroCluster FC-Konfiguration aus vier Nodes mit einem HA-Paar an jedem Standort:



Nach Abschluss dieses Verfahrens besteht die MetroCluster FC-Konfiguration aus zwei HA-Paaren an jedem Standort:



Beide Standorte müssen gleichermaßen erweitert werden. Eine MetroCluster FC-Konfiguration darf nicht aus einer ungleichmäßigen Anzahl von Nodes bestehen.

Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für MetroCluster FC-Konfigurationen mit acht Nodes aufgeführt.

- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen.
- Die Kombinationen in dieser Tabelle gelten nur für normale oder permanente Konfigurationen mit acht Nodes.
- Die Plattformkombinationen in dieser Tabelle **nicht** gelten, wenn Sie die Umstiegs- oder Aktualisierungsverfahren verwenden.
- Alle Nodes in einer DR-Gruppe müssen vom gleichen Typ und von derselben Konfiguration sein.

Unterstützte AFF- und FAS MetroCluster-FC-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum erweitern eines AFF oder FAS Systems in einer MetroCluster FC-Konfiguration aufgeführt:

FAS and AFF		Eight-node DR group 2							
		FAS8200	AFF A300	FAS8300	AFF A400	FAS9000	AFF A700	FAS9500	AFF A900
Eight-node DR group 1	FAS8200								
	AFF A300								
	FAS8300								
	AFF A400								
	FAS9000								
	AFF A700								
	FAS9500								
	AFF A900								

Unterstützte ASA MetroCluster FC-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen zum erweitern eines ASA Systems in einer MetroCluster FC-Konfiguration aufgeführt:

DR-Gruppe 1 mit acht Nodes	DR-Gruppe 2 mit acht Nodes	Unterstützt?
ASA A400	ASA A400	Ja.
	ASA A900	Nein
ASA A900	ASA A400	Nein
	ASA A900	Ja.

Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie die Konsolenprotokollierung auf Ihren Geräten, bevor Sie diese Aufgabe ausführen.

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Bestimmen des neuen Verkabelungslayouts

Sie müssen die Verkabelung der neuen Controller-Module und aller neuen Platten-Shelfs zu den vorhandenen FC-Switches bestimmen.

Über diese Aufgabe

Diese Aufgabe muss an jedem MetroCluster Standort ausgeführt werden.

Schritte

1. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um ein Verkabelungslayout für Ihren Switch-Typ zu erstellen, verwenden Sie die Portnutzung für eine MetroCluster-Konfiguration mit acht Nodes.

   Die Verwendung des FC-Switch-Ports muss mit der in dem Verfahren beschriebenen Verwendung übereinstimmen, sodass die RCFs (Reference Configuration Files) verwendet werden können.

   > Wenn Ihre Umgebung nicht so verkabelt werden kann, dass RCF-Dateien verwendet werden können, müssen Sie das System manuell gemäß den Anweisungen in konfigurieren "Installation und Konfiguration von Fabric-Attached MetroCluster". Verwenden Sie dieses Verfahren nicht, wenn die Verkabelung keine RCF-Dateien verwenden kann.

Die neue Ausrüstung in den Racks zu bringen

Sie müssen die Geräte für die neuen Nodes im Rack unterbringen.

Schritte

1. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um neue Storage-Systeme, Platten-Shelfs und FC-to-SAS-Bridges Rack zu bilden.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie sollten den Systemzustand der MetroCluster-Konfiguration überprüfen, um einen ordnungsgemäßen Betrieb zu gewährleisten.

Schritte

1. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist:

   ```
   metrocluster node show
   ```

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

3. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind:

   `metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

   `system health alert show`

5. Simulation eines Switchover-Vorgangs:

   a. Ändern Sie in der Eingabeaufforderung eines beliebigen Nodes die erweiterte Berechtigungsebene: `set -privilege advanced`

      Sie müssen mit reagieren **y** Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*>) anzuzeigen.

   b. Führen Sie den Umschaltvorgang mit dem Parameter -Simulate: + aus `metrocluster switchover -simulate`

c. Zurück zur Administrator-Berechtigungsebene:
   `set -privilege admin`

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor

Sie können die NetApp Support-Website besuchen und das Config Advisor-Tool herunterladen, um häufige Konfigurationsfehler zu überprüfen.

Über diese Aufgabe

Config Advisor ist ein Tool zur Konfigurationsvalidierung und Statusüberprüfung. Sie können die Lösung sowohl an sicheren Standorten als auch an nicht sicheren Standorten zur Datenerfassung und Systemanalyse einsetzen.

> Der Support für Config Advisor ist begrenzt und steht nur online zur Verfügung.

Schritte

1. Rufen Sie die Config Advisor Download-Seite auf und laden Sie das Tool herunter.

   "NetApp Downloads: Config Advisor"

2. Führen Sie Config Advisor aus, überprüfen Sie die Ausgabe des Tools und folgen Sie den Empfehlungen in der Ausgabe, um erkannte Probleme zu beheben.

Senden einer benutzerdefinierten AutoSupport Meldung vor dem Hinzufügen von Nodes zur MetroCluster Konfiguration

Sie sollten eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei Site_A beim Cluster an
2. Rufen Sie eine AutoSupport-Meldung auf, die den Beginn der Wartung angibt:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Der `maintenance-window-in-hours` Der Parameter gibt die Länge des Wartungsfensters an und kann maximal 72 Stunden betragen. Wenn die Wartung vor Ablauf der Zeit abgeschlossen ist, können Sie den folgenden Befehl eingeben, um anzugeben, dass der Wartungszeitraum beendet ist:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Reverkable und Zone A Switch Fabric für die neuen Nodes

Bestehende DR-Gruppe von der Fabric trennen

Sie müssen die vorhandenen Controller-Module von den FC-Switches in der Fabric trennen.

Über diese Aufgabe

Diese Aufgabe muss an jedem MetroCluster Standort ausgeführt werden.

Schritte

1. Deaktivieren Sie die HBA-Ports, die die vorhandenen Controller-Module mit der zu Wartungszwecken laufenden Switch-Fabric verbinden:

   ```
   storage port disable -node node-name -port port-number
   ```

2. Entfernen Sie bei den lokalen FC-Switches die Kabel von den Ports für die HBA-, FC-VI- und ATTO-Brücken des vorhandenen Controller-Moduls.

   Sie sollten die Kabel so kennzeichnen, dass sie sich leicht identifizieren lassen, wenn Sie sie erneut verkabeln. Nur die ISL-Ports sollten verkabelt bleiben.

Die Switches können neu konfiguriert und neu konfiguriert werden

Sie müssen die RCF-Dateien anwenden, um das Zoning neu zu konfigurieren, um die neuen Nodes aufzunehmen.

Wenn Sie die RCF-Dateien nicht zur Konfiguration der Switches verwenden können, müssen Sie die Switches manuell konfigurieren. Siehe:

- "Konfigurieren Sie die Brocade FC-Switches manuell"
- "Konfigurieren Sie Cisco FC-Switches manuell"

Schritte

1. Suchen Sie die RCF-Dateien für Ihre Konfiguration.

   Sie müssen die RCF-Dateien für eine Konfiguration mit acht Nodes verwenden, die Ihrem Switch-Modell entspricht.

2. Wenden Sie die RCF-Dateien an, indem Sie den Anweisungen auf der Download-Seite folgen und die ISL-Einstellungen nach Bedarf anpassen.
3. Stellen Sie sicher, dass die Switch-Konfiguration gespeichert ist.
4. Starten Sie die FC-Switches neu.
5. Verkabelung der vorhandenen und der neuen FC-to-SAS-Bridges zu den FC-Switches, wobei Sie das zuvor erstellte Verkabelungslayout verwenden.

   Die Verwendung von FC-Switch-Ports muss mit der in beschriebenen Verwendung von acht MetroCluster-Nodes übereinstimmen "Installation und Konfiguration von Fabric-Attached MetroCluster" Damit die Referenzkonfigurationsdateien (RCfs) verwendet werden können.

6. Überprüfen Sie, ob die Ports online sind, indem Sie den korrekten Befehl für Ihren Switch verwenden.

Switch-Anbieter	Befehl
Brocade	switchshow
Cisco	Schnittstellenübersicht anzeigen

7. Verwenden Sie das Verfahren unter "Installation und Konfiguration von Fabric-Attached MetroCluster" Um die FC-VI-Ports mithilfe des zuvor erstellten Verkabelungslayouts von den vorhandenen und neuen Controllern zu verkabeln.

   Die Verwendung von FC-Switch-Ports muss mit der in beschriebenen Verwendung von acht MetroCluster-Nodes übereinstimmen "Installation und Konfiguration von Fabric-Attached MetroCluster" Damit die Referenzkonfigurationsdateien (RCfs) verwendet werden können.

8. Vergewissern Sie sich von den vorhandenen Nodes, dass die FC-VI-Ports online sind:

   ```
   metrocluster interconnect adapter show
   ```

   ```
   metrocluster interconnect mirror show
   ```

9. Verkabeln Sie die HBA-Ports der aktuellen und der neuen Controller.
10. Aktivieren Sie bei den vorhandenen Controller-Modulen die Ports, die im Rahmen der Wartung an die Switch-Fabric angeschlossen sind:

    ```
    storage port enable -node node-name -port port-ID
    ```

11. Starten Sie die neuen Controller, und starten Sie sie in den Wartungsmodus:

    ```
    boot_ontap maint
    ```

12. Vergewissern Sie sich, dass nur Storage sichtbar ist, der von der neuen DR-Gruppe verwendet wird.

    Keiner der Storage, der von der anderen DR-Gruppe verwendet wird, sollte sichtbar sein.

13. Kehren Sie zu Beginn dieses Prozesses zurück, um die zweite Switch-Fabric wieder zu verkabeln.

Konfigurieren Sie ONTAP auf den neuen Controllern

Löschen der Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

   ```
   boot_ontap menu
   ```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Zuweisung der Festplatteneigentümer für AFF Systeme

Wenn Sie in einer Konfiguration mit AFF Systemen und gespiegelten Aggregaten einsetzen und die Nodes die Festplatten (SSDs) nicht korrekt zugewiesen sind, sollten Sie den HA-Partner-Node jeweils halb so viele Festplatten an jedem Shelf einem lokalen Node und der anderen Hälfte der Festplatten zuweisen. Sie sollten eine Konfiguration erstellen, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Über diese Aufgabe

Die Storage Controller müssen sich im Wartungsmodus befinden.

Dies gilt nicht für Konfigurationen mit nicht gespiegelten Aggregaten, einer aktiv/Passiv-Konfiguration oder einer ungleichen Anzahl von Festplatten in lokalen und Remote-Pools.

Dieser Task ist nicht erforderlich, wenn Festplatten beim Empfang vom Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören, während Pool 1 immer die Festplatten enthält, die sich dem Speichersystem, dem sie gehören, fernhalten.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Festplatten den Nodes des ersten Standorts (Standort A) zu:

   Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

   a. Weisen Sie beim ersten Knoten systematisch die Hälfte der Disks jedem Shelf zu, um 0 und die andere Hälfte dem Pool des HA-Partners 0: + zuzuweisen
      `disk assign -disk disk-name -p pool -n number-of-disks`

Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Wiederholen Sie den Vorgang für den zweiten Knoten am lokalen Standort, indem Sie in jedem Shelf systematisch die Hälfte der Festplatten dem Pool 1 und der anderen Hälfte dem Pool des HA-Partners 1: + zuweisen
`disk assign -disk disk-name -p pool`

Wenn der Storage Controller Controller_A_1 vier Shelves mit jeweils 8 SSDs aufweist, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Weisen Sie die Festplatten den Nodes des zweiten Standorts (Standort B) zu:

Jedem Pool sollte eine gleiche Anzahl an Festplatten zugewiesen werden.

a. Weisen Sie auf dem ersten Knoten am Remote-Standort systematisch die Hälfte der Festplatten auf jedem Shelf zu Pool 0 und die andere Hälfte dem Pool des HA-Partners 0: + zu
`disk assign -disk disk-name -p pool`

Wenn der Storage Controller Controller_B_1 vier Shelves mit jeweils 8 SSDs hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. Wiederholen Sie diesen Vorgang für den zweiten Node am Remote-Standort, indem Sie in jedem Shelf systematisch die Hälfte der Festplatten dem Pool 1 und der anderen Hälfte dem Pool des HA-Partners 1 zuweisen:

`disk assign -disk disk-name -p pool`

Wenn der Storage Controller Controller_B_2 vier Shelfs mit jeweils 8 SSDs aufweist, geben Sie die

folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Bestätigen Sie die Festplattenzuordnungen:

   ```
   storage show disk
   ```

5. Beenden des Wartungsmodus:

   ```
   halt
   ```

6. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

Zuweisung der Festplatteneigentümer in anderen Systemen außerhalb von All Flash FAS

Wenn auf den MetroCluster Nodes die Festplatten nicht korrekt zugewiesen sind oder wenn Sie in Ihrer Konfiguration DS460C Platten-Shelfs verwenden, müssen Sie jedem der Nodes der MetroCluster Konfiguration Shelf-einzeln Festplatten zuweisen. Sie erstellen eine Konfiguration, in der jeder Knoten die gleiche Anzahl von Festplatten in seinen lokalen und Remote-Laufwerk-Pools hat.

Über diese Aufgabe

Die Storage Controller müssen sich im Wartungsmodus befinden.

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs nicht umfasst, ist diese Aufgabe nicht erforderlich, wenn die Festplatten bereits im Werk korrekt zugewiesen wurden.

> Pool 0 enthält immer die Laufwerke, die sich an demselben Standort wie das Speichersystem befinden, zu dem sie gehören.
>
> Pool 1 enthält immer die Festplatten, die sich dem Speichersystem, zu dem sie gehören, fernhalten.

Wenn Ihre Konfiguration DS460C Festplatten-Shelfs umfasst, sollten Sie die Festplatten anhand der folgenden Richtlinien für jedes Laufwerk mit 12 Festplatten manuell zuweisen:

Diese Festplatten in der Schublade zuweisen…	Zu diesem Knoten und Pool…
0-2	Pool des lokalen Node 0

3 - 5	Pool 0 des HA-Partner-Node
6 - 8	DR-Partner des lokalen Knotens Pool 1
9 - 11	DR-Partner des HA-Partners Pool 1

Mit diesem Zuweisungsmuster wird sichergestellt, dass ein Aggregat minimal beeinträchtigt wird, wenn ein Einschub offline geht.

Schritte

1. Wenn Sie dies noch nicht getan haben, starten Sie jedes System in den Wartungsmodus.
2. Weisen Sie die Platten-Shelfs den Nodes des ersten Standorts (Standort A) zu:

   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. Weisen Sie beim ersten Knoten systematisch die lokalen Festplatten-Shelfs dem Pool 0 und den Remote-Festplatten-Shelfs zu, und Pool 1:

      ```
      disk assign -shelf local-switch-name:shelf-name.port -p pool
      ```

      Wenn der Storage Controller Controller_A_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
      ```

   b. Wiederholen Sie den Vorgang für den zweiten Node am lokalen Standort, indem Sie den Pool 0 und die Remote-Festplatten-Shelfs systematisch den Pool 1 zuweisen:

      ```
      disk assign -shelf local-switch-name:shelf-name.port -p pool
      ```

      Wenn der Storage Controller Controller_A_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

   ```
   *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
   *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

   *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
   *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
   ```

3. Weisen Sie die Platten-Shelfs den Nodes am zweiten Standort (Standort B) zu:

   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. Weisen Sie beim ersten Knoten am Remote-Standort systematisch seine lokalen Festplatten-Shelfs dem Pool 0 und seinen Remote-Festplatten-Shelfs zu 1:

   `disk assign -shelf local-switch-nameshelf-name -p pool`

   Wenn der Storage Controller_B_1 vier Shelves hat, geben Sie die folgenden Befehle ein:

   ```
   *> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
   *> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

   *> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
   *> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
   ```

b. Wiederholen Sie den Vorgang für den zweiten Node am Remote-Standort, indem Sie seine lokalen Festplatten-Shelfs systematisch dem Pool 0 und den Remote-Festplatten-Shelfs Pool 1 zuordnen:

   `disk assign -shelf shelf-name -p pool`

   Wenn der Storage Controller_B_2 vier Shelves hat, geben Sie die folgenden Befehle ein:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Bestätigen Sie die Shelf-Zuweisungen:

   `storage show shelf`

5. Beenden des Wartungsmodus:

   `halt`

6. Anzeigen des Startmenüs:

   `boot_ontap menu`

7. Wählen Sie auf jedem Knoten die Option **4**, um alle Festplatten zu initialisieren.

Überprüfen des HA-Konfigurationsstatus von Komponenten

In einer MetroCluster-Konfiguration muss der HA-Konfigurationszustand des Controller-Moduls und der Gehäusekomponenten auf **mcc** eingestellt sein, damit sie ordnungsgemäß hochfahren.

Über diese Aufgabe

- Das System muss sich im Wartungsmodus befinden.
- Diese Aufgabe muss an jedem neuen Controller-Modul ausgeführt werden.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der HA-Status für alle Komponenten sollte „mcc“ sein.

2. Wenn der angezeigte Systemzustand des Controllers nicht korrekt ist, setzen Sie den HA-Status für das Controller-Modul ein:

   ```
   ha-config modify controller mcc
   ```

3. Wenn der angezeigte Systemzustand des Chassis nicht korrekt ist, setzen Sie den HA-Status für das Chassis ein:

   ```
   ha-config modify chassis mcc
   ```

4. Wiederholen Sie diese Schritte auf dem anderen Ersatzknoten.

Booten der neuen Controller und Verbinden der Controller mit dem Cluster

Damit Sie die neuen Controller dem Cluster beitreten können, müssen Sie jedes neue Controller-Modul booten und den ONTAP Cluster Setup-Assistenten verwenden, um zu ermitteln, dass der Cluster Beitritt.

Bevor Sie beginnen

Sie müssen die MetroCluster-Konfiguration verkabelt haben.

Sie müssen den Service-Prozessor nicht konfiguriert haben, bevor Sie diese Aufgabe ausführen.

Über diese Aufgabe

Diese Aufgabe muss für jeden der neuen Controller bei beiden Clustern in der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Falls noch nicht geschehen, schalten Sie jeden Knoten ein und lassen Sie ihn vollständig booten.

   Wenn sich das System im Wartungsmodus befindet, geben Sie den aus `halt` Befehl zum Beenden des Wartungsmodus und geben Sie dann den folgenden Befehl von der LOADER-Eingabeaufforderung aus:

   ```
   boot_ontap
   ```

   Das Controller-Modul wechselt in den Node-Setup-Assistenten.

   Die Ausgabe sollte wie folgt aussehen:

```
Welcome to node setup

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
                 Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. Aktivieren Sie das AutoSupport-Tool, indem Sie den vom System bereitgestellten Anweisungen folgen.
3. Befolgen Sie die Aufforderungen zur Konfiguration der Node-Managementoberfläche.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Sicherstellen, dass die Nodes im Hochverfügbarkeits-Modus konfiguriert sind:

   `storage failover show -fields mode`

   Wenn dies nicht der Fall ist, müssen Sie für jeden Node den folgenden Befehl eingeben und dann den Node neu booten:

   `storage failover modify -mode ha -node localhost`

   Dieser Befehl konfiguriert den Hochverfügbarkeits-Modus, ermöglicht jedoch kein Storage Failover. Storage-Failover wird automatisch aktiviert, wenn Sie das ausgeben `metrocluster configure` Befehl später im Konfigurationsprozess.

5. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

   `network port show`

   Im folgenden Beispiel wird die Ausgabe für zwei Controller in „Cluster_A“ angezeigt Wenn es sich um eine MetroCluster-Konfiguration mit zwei Nodes handelt, wird in der Ausgabe nur ein Node angezeigt.

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       1500
auto/1000
       e0b       Cluster      Cluster          up       1500
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Da Sie das Cluster mit der CLI einrichten, beenden Sie den Node Setup-Assistenten:

   ```
   exit
   ```

7. Loggen Sie sich mit dem beim Administratorkonto ein `admin` Benutzername:
8. Starten Sie den Cluster Setup-Assistenten und fügen Sie ihn dem vorhandenen Cluster hinzu:

   ```
   cluster setup
   ```

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`
```

9. Nachdem Sie den **Cluster Setup**-Assistenten abgeschlossen und beendet haben, überprüfen Sie, ob der Cluster aktiv ist und der Knoten ordnungsgemäß ist:

   `cluster show`

   Das folgende Beispiel zeigt ein Cluster, in dem der erste Node (cluster1-01) sich in einem ordnungsgemäßen Zustand befindet und zur Teilnahme berechtigt ist:

   ```
   cluster_A::> cluster show
   Node                  Health  Eligibility
   ------------------ ------- ------------
   node_A_1              true    true
   node_A_2              true    true
   node_A_3              true    true
   ```

   Wenn eine der Einstellungen, die Sie für die Admin-SVM oder Node-SVM eingegeben haben, geändert werden muss, können Sie über den auf den Assistenten * Cluster Setup* zugreifen `cluster setup command`.

Konfigurieren Sie die Cluster in einer MetroCluster-Konfiguration

Konfigurieren Sie Intercluster LIFs

Erfahren Sie, wie Sie Intercluster LIFs auf dedizierten und gemeinsam genutzten Ports konfigurieren.

Konfigurieren Sie Intercluster-LIFs auf dedizierten Ports

Es können Intercluster LIFs an dedizierten Ports konfiguriert werden, um die verfügbare Bandbreite für den Replizierungsdatenverkehr zu erhöhen.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                                    Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
       e0e       Default      Default          up     1500
auto/1000
       e0f       Default      Default          up     1500
auto/1000
```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   `network interface show -fields home-port,curr-port`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   ```
   network interface failover-groups create -vserver <system_SVM> -failover
   -group <failover_group> -targets <physical_or_logical_ports>
   ```

   Das folgende Beispiel weist den Failover-Gruppe „intercluster01“ auf der System-SVM „cluster01“ die Ports „e0e“ und „e0f“ zu:

   ```
   cluster01::> network interface failover-groups create -vserver
   cluster01 -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   ```
   network interface failover-groups show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  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
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>`
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_ic.01“ und „cluster01_ic02“ in der Failover-Gruppe „intercluster01“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0e     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0f     true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:

`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:
`network interface show -role intercluster -failover`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem SVM „e0e“-Port an den „e0f“-Port scheitern.

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Konfigurieren Sie Intercluster-LIFs an gemeinsam genutzten Datenports

Es können Intercluster LIFs an Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden, um die Anzahl der Ports zu reduzieren, die Sie für ein Intercluster-Netzwerk benötigen.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in cluster01 angezeigt:

```
cluster01::> network port show
                                                                   Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500
auto/1000
       e0b       Cluster      Cluster          up     1500
auto/1000
       e0c       Default      Default          up     1500
auto/1000
       e0d       Default      Default          up     1500
auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

Im ONTAP 9.6 und höher:
`network interface create -vserver <system_SVM> -lif <LIF_name> -service -policy default-intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`
In ONTAP 9.5 und früher:
`network interface create -vserver <system_SVM> -lif <LIF_name> -role intercluster -home-node <node> -home-port <port> -address <port_IP> -netmask <netmask>`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Im ONTAP 9.6 und höher:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:
`network interface show -role intercluster`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-
intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01
e0c     true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02
e0c     true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Im ONTAP 9.6 und höher:

```
network interface show –service-policy default-intercluster -failover
```

In ONTAP 9.5 und früher:

```
network interface show -role intercluster -failover
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern wird.

```
cluster01::> network interface show -service-policy default-
intercluster –failover
         Logical         Home                  Failover
Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
--------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Spiegelung der Root-Aggregate

Um Datensicherung zu ermöglichen, müssen Sie die Root-Aggregate spiegeln.

Standardmäßig wird das Root-Aggregat als RAID-DP Typ Aggregat erstellt. Sie können das Root-Aggregat von RAID-DP zu einem Aggregat des RAID4-Typs ändern. Mit dem folgenden Befehl wird das Root-Aggregat für das RAID4-Typ-Aggregat modifiziert:

```
storage aggregate modify –aggregate aggr_name -raidtype raid4
```

> Auf Systemen anderer Hersteller kann der RAID-Typ des Aggregats von dem Standard RAID-DP zu RAID4 vor oder nach der Spiegelung des Aggregats geändert werden.

Schritte

1. Root-Aggregat spiegeln:

`storage aggregate mirror aggr_name`

Der folgende Befehl spiegelt das Root-Aggregat für Controller_A_1:

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

2. Wiederholen Sie den vorherigen Schritt für jeden Node in der MetroCluster-Konfiguration.

Implementieren der MetroCluster-Konfiguration

Sie müssen den ausführen `metrocluster configure -refresh true` Befehl zum Starten der Datensicherung auf den Nodes, die Sie einer MetroCluster-Konfiguration hinzugefügt haben.

Über diese Aufgabe

Sie stellen das aus `metrocluster configure -refresh true` Befehl einmal auf einem der neu hinzugefügten Nodes, um die MetroCluster-Konfiguration zu aktualisieren. Sie müssen den Befehl nicht an jedem Standort bzw. jeder Node ausgeben.

Der `metrocluster configure -refresh true` Befehl koppelt die beiden Nodes automatisch mit den niedrigsten System-IDs in jedem der beiden Cluster als Disaster Recovery (DR) Partner. In einer MetroCluster Konfiguration mit vier Nodes gibt es zwei DR-Partnerpaare. Das zweite DR-Paar wird aus den beiden Knoten mit höheren System-IDs erstellt.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Wechseln Sie in den erweiterten Berechtigungsmodus:

      `set -privilege advanced`

   b. Aktualisieren Sie die MetroCluster Konfiguration auf einem der neuen Nodes:
      `metrocluster configure -refresh true`

      Im folgenden Beispiel wird die auf beiden DR-Gruppen aktualisierte MetroCluster Konfiguration angezeigt:

```
controller_A_2::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

+

```
controller_A_4::*> metrocluster configure -refresh true

[Job 740] Job succeeded: Configure is successful.
```

a. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

```
network port show
```

Im folgenden Beispiel wird die Verwendung von Netzwerkports in einer MetroCluster Konfiguration mit vier Nodes angezeigt:

```
cluster_A::> network port show
                                                          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
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration:

a. Überprüfen Sie die Konfiguration von Standort A:

```
metrocluster show
```

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

a. Überprüfen Sie die Konfiguration von Standort B:
`metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

  In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

> Es wird empfohlen, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   ```
   storage disk show -spare -owner node_name
   ```

2. Erstellen Sie das Aggregat:

   ```
   storage aggregate create -mirror true
   ```

   Wenn Sie 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 spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke

     > In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie im `storage aggregate create` Man-Page.

     Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Konfiguration von FC-to-SAS-Bridges für das Monitoring des Systemzustands

Erfahren Sie, wie Sie die FC-zu-SAS-Bridges für die Zustandsüberwachung konfigurieren.

Über diese Aufgabe

- SNMP-Überwachungstools anderer Anbieter werden für FibreBridge-Brücken nicht unterstützt.
- Ab ONTAP 9.8 werden FC-to-SAS-Bridges standardmäßig über in-Band-Verbindungen überwacht, keine zusätzliche Konfiguration erforderlich.

> Ab ONTAP 9.8 beginnt der `storage bridge` Befehl wird durch 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.

Schritt

1. Fügen Sie von der ONTAP Cluster-Eingabeaufforderung die Bridge zur Statusüberwachung hinzu:

   a. Fügen Sie die Bridge mit dem Befehl für Ihre ONTAP-Version hinzu:

ONTAP-Version	Befehl
9.5 und höher	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
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 bis zu 15 Minuten dauern, bis alle Daten aufgrund des Abrufintervalls reflektiert wurden. Die ONTAP Systemzustandsüberwachung kann die Brücke kontaktieren und überwachen, wenn der Wert in der Spalte „Status“ „ok“ lautet und weitere Informationen, z. B. der weltweite Name (WWN), angezeigt werden.

   Das folgende Beispiel zeigt, dass die FC-to-SAS-Bridges konfiguriert sind:

```
controller_A_1::> storage bridge show

Bridge              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::>
```

Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen

Sie können ein Metadaten-Volume in eine MetroCluster Konfiguration von einem Aggregat zu einem anderen Aggregat verschieben. Unter Umständen möchten Sie ein Metadaten-Volume verschieben, wenn das Quellaggregat deaktiviert oder nicht gespiegelt wird, oder aus anderen Gründen, aus denen das Aggregat nicht mehr berechtigt ist.

Über diese Aufgabe

- Um diese Aufgabe ausführen zu können, müssen Sie über Cluster-Administratorrechte verfügen.
- Das Zielaggregat muss gespiegelt werden und darf nicht im eingeschränkten Zustand sein.
- Der verfügbare Speicherplatz im Zielaggregat muss größer sein als das zu bewegende Metadaten-Volume.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Identifizierung des zu verschiebenden Metadaten-Volumes:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Ermittlung eines geeigneten Zielaggregats:

   `metrocluster check config-replication show-aggregate-eligibility`

   Mit dem folgenden Befehl werden die Aggregate in „Cluster_A“ identifiziert, die zum Hosten von Metadaten-Volumes geeignet sind:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

In dem vorherigen Beispiel können Node_A_1_aggr2 und Node_A_2_aggr2 ausgewählt werden.

4. Starten Sie die Volume-Verschiebung:

   `volume move start -vserver` *`svm_name`* `-volume` *`metadata_volume_name`* `-destination -aggregate` *`destination_aggregate_name`*`*`

   Der folgende Befehl verschiebt Metadaten-Volume „MDV_CRS_14c00d4ac9f311e7922800a0984395f1“ von „Aggregate Node_A_1_aggr1“ in „Aggregate Node_A_1_aggr2“:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Überprüfung des Status der Verschiebung eines Volumes:

   ```
   volume move show -volume vol_constituent_name
   ```

6. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Überprüfen der MetroCluster-Konfiguration

Sie können überprüfen, ob die Komponenten und Beziehungen in der MetroCluster Konfiguration ordnungsgemäß funktionieren. Nach der Erstkonfiguration und nach sämtlichen Änderungen an der MetroCluster-Konfiguration sollten Sie einen Check durchführen. Sie sollten auch vor einer ausgehandelten (geplanten) Umschaltung oder einem Switchback prüfen.

Über diese Aufgabe

Wenn der `metrocluster check run` Befehl wird zweimal innerhalb kürzester Zeit auf einem oder beiden Clustern ausgegeben. Ein Konflikt kann auftreten, und der Befehl erfasst möglicherweise nicht alle Daten. Danach `metrocluster check show` Befehle zeigen nicht die erwartete Ausgabe an.

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

   Der Befehl wird als Hintergrundjob ausgeführt und wird möglicherweise nicht sofort ausgeführt.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Zeigen Sie detailliertere Ergebnisse der letzten Zeit an `metrocluster check run` Befehl:

   ```
   metrocluster check aggregate show

   metrocluster check cluster show

   metrocluster check config-replication show

   metrocluster check lif show

   metrocluster check node show
   ```

   Der `metrocluster check show` Befehle zeigen die Ergebnisse der letzten `metrocluster check run` Befehl. Sie sollten immer den ausführen `metrocluster check run` Befehl vor Verwendung des `metrocluster check show` Befehle, sodass die angezeigten Informationen aktuell sind.

   Das folgende Beispiel zeigt die `metrocluster check aggregate show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
```

```
                      controller_A_1_aggr1
                                                      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.
```

Überprüfen auf MetroCluster-Konfigurationsfehler mit Config Advisor

Sie können die NetApp Support-Website besuchen und das Config Advisor-Tool herunterladen, um häufige Konfigurationsfehler zu überprüfen.

Über diese Aufgabe

Config Advisor ist ein Tool zur Konfigurationsvalidierung und Statusüberprüfung. Sie können die Lösung sowohl an sicheren Standorten als auch an nicht sicheren Standorten zur Datenerfassung und Systemanalyse einsetzen.

> Der Support für Config Advisor ist begrenzt und steht nur online zur Verfügung.

Schritte

1. Rufen Sie die Config Advisor Download-Seite auf und laden Sie das Tool herunter.

   "NetApp Downloads: Config Advisor"

2. Führen Sie Config Advisor aus, überprüfen Sie die Ausgabe des Tools und folgen Sie den Empfehlungen in der Ausgabe, um erkannte Probleme zu beheben.

Senden einer benutzerdefinierten AutoSupport Meldung nach dem Hinzufügen von Nodes zur MetroCluster Konfiguration

Sie sollten eine Meldung von AutoSupport senden, um den technischen Support von NetApp über die Wartung zu informieren.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Melden Sie sich bei Site_A beim Cluster an
2. Rufen Sie eine AutoSupport-Meldung auf, die das Ende der Wartung angibt:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Wiederholen Sie diesen Schritt auf der Partner-Site.

Überprüfung von Umschaltung, Reparatur und Wechsel zurück

Sie sollten die Umschalttavorgänge, die Reparatur und den Wechsel der MetroCluster Konfiguration überprüfen.

Schritte

1. Verwenden Sie die Verfahren für die ausgehandelte Umschaltung, Heilung und zurückwechseln "MetroCluster Management und Disaster Recovery".

Erweitern Sie eine MetroCluster IP-Konfiguration

Je nach ONTAP Version können Sie Ihre MetroCluster IP-Konfiguration erweitern, indem Sie vier neue Nodes als neue DR-Gruppe hinzufügen.

Ab ONTAP 9.13.1 können Sie eine MetroCluster Konfiguration mit acht Nodes vorübergehend erweitern, um die Controller und Storage zu aktualisieren. Siehe "Aktualisieren einer MetroCluster IP-Konfiguration mit vier oder acht Nodes (ONTAP 9.8 und höher)" Finden Sie weitere Informationen.

Ab ONTAP 9.9 können Sie der MetroCluster IP-Konfiguration vier neue Nodes als zweite DR-Gruppe hinzufügen. Dadurch wird eine MetroCluster-Konfiguration mit acht Nodes erstellt.

Wichtige Informationen

Während der Umstellung, Aktualisierung, Installation von acht Knoten und Erweiterung von vier Knoten können Sie Ihrer MetroCluster-Konfiguration ein neues Plattformmodell hinzufügen. Wenn Ihre bestehende MetroCluster-Konfiguration zu irgendeinem Zeitpunkt eine Plattform mit **gemeinsamen Cluster-/HA-Ports** enthält, können Sie der Konfiguration keine Plattform mit **gemeinsamen MetroCluster-/HA-Ports** hinzufügen, ohne Ihre ONTAP-Version auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher zu aktualisieren.

Bevor Sie sich für dieses Verfahren entscheiden, lesen Sie die Informationen in der folgenden Tabelle sorgfältig durch. Wenn Ihre vorhandene Plattform in der ersten Spalte und die Plattform, die Sie der Konfiguration hinzufügen möchten, in der zweiten Spalte aufgeführt ist, müssen alle Knoten in der Konfiguration ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen, um dieses Verfahren zu unterstützen.

> Sowohl die vorhandene Plattform als auch die Plattform, die Sie der Konfiguration hinzufügen möchten, müssen ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher ausführen.

Wenn Ihr vorhandener MetroCluster Folgendes enthält:		Und die Plattform, die Sie hinzufügen, ist …		Dann…
Ein AFF-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	Ein FAS-System, das **gemeinsam genutzte Cluster-/HA-Ports** verwendet: • FAS50 • FAS70 • FAS90	Ein AFF-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	Ein FAS-System, das **gemeinsam genutzte MetroCluster/HA-Ports** verwendet: • FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500	Bevor Sie die neue Plattform zu Ihrer vorhandenen MetroCluster-Konfiguration hinzufügen, aktualisieren Sie alle Knoten in der vorhandenen und neuen Konfiguration auf ONTAP 9.15.1P11 oder ONTAP 9.16.1P4 oder höher.

Bevor Sie beginnen

- Die alten und neuen Nodes müssen dieselbe Version von ONTAP ausführen.
- In diesem Verfahren werden die Schritte beschrieben, die erforderlich sind, um eine DR-Gruppe mit vier Nodes einer vorhandenen MetroCluster IP-Konfiguration hinzuzufügen. Wenn Sie eine Konfiguration mit acht Nodes aktualisieren, müssen Sie den gesamten Vorgang für jede DR-Gruppe wiederholen und nacheinander hinzufügen.
- Stellen Sie sicher, dass die alten und neuen Plattformmodelle für die gemeinsame Verwendung der Plattformen unterstützt werden.

  "NetApp Hardware Universe"

- Überprüfen Sie, ob die alten und die neuen Plattformmodelle von den IP-Switches unterstützt werden.

  "NetApp Hardware Universe"

- Wenn Sie es sind "Aktualisieren einer MetroCluster-IP-Konfiguration mit vier oder acht Nodes", Die neuen Knoten müssen über genügend Speicher verfügen, um die Daten der alten Knoten aufzunehmen, zusammen mit geeigneten Platten für Root-Aggregate und freie Platten.

- Vergewissern Sie sich, dass auf den alten Knoten eine Standard-Broadcast-Domäne erstellt wurde.

  Wenn Sie einem vorhandenen Cluster neue Nodes ohne standardmäßige Broadcast-Domäne hinzufügen, werden für die neuen Nodes Node-Management-LIFs erstellt, die nicht die erwarteten Namen verwenden, sondern UIDs (Universal Unique Identifiers). Weitere Informationen finden Sie im Knowledge Base-Artikel "LIFs für das Node-Management, die auf neu hinzugefügten Nodes erstellt wurden und mit UUID-Namen generiert wurden".

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Beispiel für die Benennung in diesem Verfahren

Bei diesem Verfahren werden durchgängig Beispielnamen verwendet, um die involvierten DR-Gruppen, Nodes und Switches zu identifizieren.

DR-Gruppen	Cluster_A an Standort_A	Cluster_B an Standort_B
dr_Group_1-alt	• Node_A_1-alt • Node_A_2-alt	• Node_B_1-alt • Node_B_2-alt
dr_Group_2-neu	• Node_A_3-neu • Node_A_4-neu	• Node_B_3-neu • Node_B_4-neu

Unterstützte Plattformkombinationen beim Hinzufügen einer zweiten DR-Gruppe

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für MetroCluster IP-Konfigurationen mit acht Nodes aufgeführt.

- Auf allen Nodes in der MetroCluster-Konfiguration muss dieselbe ONTAP-Version ausgeführt werden. Wenn Sie beispielsweise über eine Konfiguration mit acht Nodes verfügen, müssen alle acht Nodes dieselbe ONTAP-Version ausführen. Die unterstützte Mindestversion ONTAP für Ihre Kombination finden Sie im"Hardware Universe".
- Die Kombinationen in dieser Tabelle gelten nur für normale oder permanente Konfigurationen mit acht Nodes.
- Die Plattformkombinationen in dieser Tabelle **nicht** gelten, wenn Sie die Umstiegs- oder Aktualisierungsverfahren verwenden.
- Alle Nodes in einer DR-Gruppe müssen vom gleichen Typ und von derselben Konfiguration sein.

Unterstützte AFF- und FAS MetroCluster-IP-Erweiterungskombinationen

Die folgenden Tabellen zeigen die unterstützten Plattformkombinationen für die Erweiterung eines AFF- oder FAS-Systems in einer MetroCluster IP-Konfiguration. Die Tabellen sind in zwei Gruppen aufgeteilt:

- **Gruppe 1** zeigt Kombinationen für AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF C400, AFF A400, AFF A220, AFF A300, AFF A320 und FAS8700 Systeme.
- **Gruppe 2** zeigt Kombinationen für AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

Die folgenden Hinweise gelten für beide Gruppen:

- Hinweis 1: Für diese Kombinationen ist ONTAP 9.9.1 oder höher (oder die minimale ONTAP-Version, die auf der Plattform unterstützt wird) erforderlich.
- Hinweis 2: Für diese Kombinationen ist ONTAP 9.13.1 oder höher (oder die minimale ONTAP-Version, die auf der Plattform unterstützt wird) erforderlich.

AFF- und FAS-Kombinationen, Gruppe 1

Prüfen Sie die Erweiterungskombinationen für AFF A150, AFF A20, FAS2750, FAS8300, FAS500f, AFF C250, AFF A250, FAS50, AFF C30, AFF A30, FAS8200, AFF A300, AFF A400, AFF A220, AFF C400, AFF A320 und FAS8700 Systeme.

AFF and FAS		Eight-node DR group 2									
		AFF A150	AFF A20	FAS2750 AFF A220	FAS500f AFF C250 AFF A250	FAS50	AFF C30 AFF A30	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 AFF A400	FAS8700
Eight-node DR group 1	AFF A150	Note 2									
	AFF A20										
	FAS2750 AFF A220										
	FAS500f AFF C250 AFF A250										
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300							Note 1			
	AFF A320							Note 1			
	FAS8300 AFF C400 AFF A400								Note 1	Note 1	
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70										
	FAS9000 AFF A700										
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

AFF und FAS Kombinationsgruppe 2

Prüfen Sie die Erweiterungskombinationen für AFF C60, AFF A50, FAS70, FAS9000, AFF A700, AFF A70, AFF C800, AFF A800, FAS9500, AFF A900, AFF C80, FAS90, AFF A90 und AFF A1K Systeme.

AFF and FAS		Eight-node DR group 2									
		AFF C60	AFF A50	FAS70	FAS9000 AFF A700	AFF A70	AFF C800 AFF A800	FAS9500 AFF A900	AFF C80	FAS90 AFF A90	AFF A1K
Eight-node DR group 1	AFF A150										
	AFF A20										
	FAS2750 AFF A220										
	FAS500f AFF C250 AFF A250										
	FAS50										
	AFF C30 AFF A30										
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 AFF A400	Note 1									
	FAS8700										
	AFF C60										
	AFF A50										
	FAS70				Note 1						
	FAS9000 AFF A700			Note 1	Note 1						
	AFF A70										
	AFF C800 AFF A800										
	FAS9500 AFF A900										
	AFF C80										
	FAS90										
	AFF A90										
	AFF A1K										

Unterstützte ASA MetroCluster IP-Erweiterungskombinationen

In der folgenden Tabelle sind die unterstützten Plattformkombinationen für die Erweiterung eines ASA-Systems in einer MetroCluster IP-Konfiguration aufgeführt:

ASA		Eight-node DR group 2							
		ASA A150	ASA C250	ASA A250	ASA C400	ASA A400	ASA C800	ASA A800	ASA A900
Eight-node DR group 1	ASA A150								
	ASA C250								
	ASA A250								
	ASA C400								
	ASA A400								
	ASA C800								
	ASA A800								
	ASA A900								

Senden einer benutzerdefinierten AutoSupport Meldung vor der Wartung

Bevor Sie die Wartung durchführen, sollten Sie eine AutoSupport Meldung ausgeben, um den technischen Support von NetApp über die laufende Wartung zu informieren. Die Mitteilung des technischen Supports über laufende Wartungsarbeiten verhindert, dass ein Fall eröffnet wird, wenn eine Störung aufgetreten ist.

Über diese Aufgabe

Diese Aufgabe muss auf jedem MetroCluster-Standort ausgeführt werden.

Schritte

1. Um eine automatische Erstellung von Support-Cases zu verhindern, senden Sie eine AutoSupport Meldung, damit das Upgrade ausgeführt wird.

   a. Geben Sie den folgenden Befehl ein:

   ```
   system node autosupport invoke -node * -type all -message "MAINT=10h
   Upgrading <old-model> to <new-model>
   ```

   Dieses Beispiel gibt ein Wartungsfenster von 10 Stunden an. Je nach Plan sollten Sie möglicherweise zusätzliche Zeit einplanen.

   Wenn die Wartung vor dem Vergehen der Zeit abgeschlossen ist, können Sie eine AutoSupport-Meldung mit dem Ende des Wartungszeitraums aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Wiederholen Sie den Befehl im Partner-Cluster.

Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe

- Beim erweitern einer MetroCluster-IP-Konfiguration gelten die folgenden VLAN-Überlegungen:

  Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

  Falls unterstützt, können Sie auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben. Verwenden Sie dazu den `-vlan-id` Parameter im `metrocluster configuration-settings interface create` Befehl.

  Die folgenden Plattformen unterstützen **Not** den `-vlan-id` Parameter:

  - FAS8200 UND AFF A300
  - AFF A320
  - FAS9000 und AFF A700
  - AFF C800, ASA C800, AFF A800 und ASA A800

    Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.

    Die Standard- und gültigen VLAN-Zuweisungen hängen davon ab, ob die Plattform den folgenden Parameter unterstützt `-vlan-id` :

Plattformen, die <code>-vlan-</code> unterstützen

Standard-VLAN:

- Wenn der `-vlan-id` Parameter nicht angegeben wird, werden die Schnittstellen mit VLAN 10 für die „A“-Ports und VLAN 20 für die „B“-Ports erstellt.
- Das angegebene VLAN muss mit dem im RCF ausgewählten VLAN übereinstimmen.

Gültige VLAN-Bereiche:

- Standard-VLAN 10 und 20
- VLANs 101 und höher (zwischen 101 und 4095)

Plattformen, die <code>-vlan-</code> nicht unterstützen

Standard-VLAN:

- Keine Angabe. Für die Schnittstelle muss kein VLAN auf der MetroCluster-Schnittstelle angegeben werden. Der Switch-Port definiert das verwendete VLAN.

Gültige VLAN-Bereiche:

- Alle VLANs werden beim Generieren der RCF nicht explizit ausgeschlossen. Die RCF warnt Sie, wenn das VLAN ungültig ist.

- Beide DR-Gruppen nutzen die gleichen VLANs, wenn Sie eine MetroCluster-Konfiguration mit vier Nodes auf acht Nodes erweitern.
- Wenn beide DR-Gruppen nicht mit demselben VLAN konfiguriert werden können, müssen Sie die DR-Gruppe, die den Parameter nicht unterstützt, aktualisieren `vlan-id` , um ein VLAN zu verwenden, das von der anderen DR-Gruppe unterstützt wird.

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Vor der Erweiterung müssen Sie den Zustand und die Konnektivität der MetroCluster-Konfiguration überprüfen.

Schritte

1. Überprüfen Sie den Betrieb der MetroCluster-Konfiguration in ONTAP:
   a. Prüfen Sie, ob das System multipathed ist:

      ```
      node run -node <node-name> sysconfig -a
      ```

   b. Überprüfen Sie auf beiden Clustern auf Zustandswarnmeldungen:

      ```
      system health alert show
      ```

   c. Bestätigen Sie die MetroCluster-Konfiguration und den normalen Betriebsmodus:

      ```
      metrocluster show
      ```

   d. Durchführen einer MetroCluster-Prüfung:

      ```
      metrocluster check run
      ```

e. Ergebnisse der MetroCluster-Prüfung anzeigen:

```
metrocluster check show
```

f. Nutzen Sie Config Advisor.

"NetApp Downloads: Config Advisor"

g. Überprüfen Sie nach dem Ausführen von Config Advisor die Ausgabe des Tools und befolgen Sie die Empfehlungen in der Ausgabe, um die erkannten Probleme zu beheben.

2. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

```
cluster_A::> cluster show
Node            Health  Eligibility
-------------- ------  -----------
node_A_1        true    true
node_A_2        true    true

cluster_A::>
```

3. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

```
network port show -ipspace Cluster
```

```
cluster_A::> network port show -ipspace Cluster

Node: node_A_1-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

   `network interface show -vserver Cluster`

   Jede Cluster-LIF sollte True für IS Home anzeigen und einen Status Admin/Oper von up/Up haben

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Vergewissern Sie sich, dass die automatische Umrüstung auf allen Cluster-LIFs aktiviert ist:

   ```
   network interface show -vserver Cluster -fields auto-revert
   ```

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Entfernen der Konfiguration aus Überwachungsanwendungen

Wenn die vorhandene Konfiguration mit der MetroCluster Tiebreaker Software, dem ONTAP Mediator oder anderen Anwendungen von Drittanbietern (z. B. ClusterLion) überwacht wird, die eine Umschaltung initiieren können, müssen Sie die MetroCluster-Konfiguration vor dem Upgrade von der Monitoring-Software entfernen.

Schritte

1. Entfernen Sie die vorhandene MetroCluster-Konfiguration von Tiebreaker, Mediator oder einer anderen Software, die die Umschaltung initiieren kann.

Sie verwenden…	Gehen Sie folgendermaßen vor:
Tiebreaker	"Entfernen von MetroCluster-Konfigurationen".
Mediator	Geben Sie den folgenden Befehl an der ONTAP-Eingabeaufforderung ein: `metrocluster configuration-settings mediator remove`
Applikationen von Drittanbietern	Siehe Produktdokumentation.

2. Entfernen Sie die vorhandene MetroCluster Konfiguration von jeder Anwendung eines Drittanbieters, die eine Umschaltung initiieren kann.

   Informationen zur Anwendung finden Sie in der Dokumentation.

Vorbereiten der neuen Controller-Module

Sie müssen die vier neuen MetroCluster-Knoten vorbereiten und die korrekte ONTAP-Version installieren.

Über diese Aufgabe

Diese Aufgabe muss auf jedem der neuen Knoten ausgeführt werden:

- Node_A_3-neu
- Node_A_4-neu
- Node_B_3-neu
- Node_B_4-neu

Löschen Sie in diesen Schritten die Konfiguration auf den Knoten und löschen Sie den Mailbox-Bereich auf neuen Laufwerken.

Schritte

1. Für die neuen Controller
2. Verkabeln Sie die neuen MetroCluster IP-Knoten wie in dargestellt mit den IP-Switches "Verkabeln Sie die IP-Switches".
3. Konfigurieren Sie die MetroCluster IP-Nodes wie folgt:
   a. "Sammeln Sie die erforderlichen Informationen"
   b. "Systemstandardwerte auf einem Controller-Modul wiederherstellen"
   c. "Überprüfen Sie den Status der HA-Konfiguration der Komponenten"
   d. "Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.4 und höher)"
4. Geben Sie im Wartungsmodus den Befehl stop ein, um den Wartungsmodus zu beenden, und geben Sie dann den Boot_ontap-Befehl aus, um das System zu booten und zum Cluster-Setup zu gelangen.

   Schließen Sie derzeit den Cluster-Assistenten oder den Node-Assistenten nicht ab.

RCF-Dateien aktualisieren

Wenn Sie neue Switch-Firmware installieren, müssen Sie die Switch-Firmware installieren, bevor Sie die RCF-Datei aktualisieren.

Über diese Aufgabe

Dieses Verfahren unterbricht den Datenverkehr auf dem Switch, auf dem die RCF-Datei aktualisiert wird. Der Datenverkehr wird wieder aufgenommen, sobald die neue RCF-Datei angewendet wurde.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration.
   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

      `metrocluster check run`

      ```
      cluster_A::*> metrocluster check run
      ```

Der Vorgang wird im Hintergrund ausgeführt.

b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführung `metrocluster check show` Um die Ergebnisse anzuzeigen.

Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id 38
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Bereiten Sie die IP-Schalter für die Anwendung der neuen RCF-Dateien vor.

Befolgen Sie die Schritte für Ihren Switch-Anbieter:

- "Setzen Sie den Broadcom IP-Switch auf die Werkseinstellungen zurück"
- "Setzen Sie den Cisco IP-Switch auf die Werkseinstellungen zurück"
- "Setzen Sie den NVIDIA IP SN2100-Switch auf die Werkseinstellungen zurück"

3. Laden Sie je nach Switch-Anbieter die IP RCF-Datei herunter, und installieren Sie sie.

> Aktualisieren Sie die Schalter in folgender Reihenfolge: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

- "Laden Sie die Broadcom IP RCF-Dateien herunter, und installieren Sie sie"
- "Laden Sie die Cisco IP RCF-Dateien herunter, und installieren Sie sie"
- "Laden Sie die NVIDIA IP RCF-Dateien herunter, und installieren Sie sie"

Wenn Sie über eine freigegebene L2- oder L3-Netzwerkkonfiguration verfügen, müssen Sie möglicherweise die ISL-Ports an den Zwischen-/Kunden-Switches anpassen. Der Switch-Port-Modus wechselt möglicherweise vom „Access“- in den „Trunk“-Modus. Fahren Sie nur mit dem Upgrade des zweiten Switch-Paares (A_2, B_2) fort, wenn die Netzwerkverbindung zwischen den Switches A_1 und B_1 voll funktionsfähig ist und das Netzwerk ordnungsgemäß ist.

Verbinden Sie die neuen Nodes mit den Clustern

Sie müssen die vier neuen MetroCluster IP-Nodes der bestehenden MetroCluster-Konfiguration hinzufügen.

Über diese Aufgabe

Sie müssen diese Aufgabe für beide Cluster ausführen.

Schritte

1. Fügen Sie die neuen MetroCluster IP-Knoten zur bestehenden MetroCluster-Konfiguration hinzu.
   a. Fügen Sie den ersten neuen MetroCluster-IP-Knoten (Node_A_1-New) der bestehenden MetroCluster-IP-Konfiguration hinzu.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster
setup".
To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.

Enabling AutoSupport can significantly speed problem determination
and
resolution, should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: 172.17.8.93
```

```
172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Fügen Sie den zweiten neuen MetroCluster-IP-Knoten (Node_A_2-New) der bestehenden MetroCluster-IP-Konfiguration hinzu.

2. Wiederholen Sie diese Schritte, um Node_B_1-New und Node_B_2-New zu Cluster_B. zu verbinden

Konfigurieren von Intercluster-LIFs, Erstellen der MetroCluster-Schnittstellen und Spiegeln von Root-Aggregaten

Sie müssen Cluster-Peering-LIFs erstellen, die MetroCluster-Schnittstellen auf den neuen MetroCluster IP-Nodes erstellen.

Über diese Aufgabe

- Der in den Beispielen verwendete Home-Port ist plattformspezifisch. Sie sollten den für Ihre MetroCluster IP Node-Plattform spezifischen Home Port verwenden.
- Überprüfen Sie die Informationen in Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe , bevor Sie diese Aufgabe ausführen.

Schritte

1. Konfigurieren Sie auf den neuen MetroCluster IP-Nodes die Intercluster-LIFs wie folgt:

   "Konfigurieren von Intercluster-LIFs auf dedizierten Ports"

   "Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports"

2. Vergewissern Sie sich an jedem Standort, dass Cluster-Peering konfiguriert ist:

   ```
   cluster peer show
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   Das folgende Beispiel zeigt die Cluster-Peering-Konfiguration auf Cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. Erstellen der DR-Gruppe für die MetroCluster IP-Knoten:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   Weitere Informationen zu den MetroCluster-Konfigurationseinstellungen und -Verbindungen finden Sie im Folgenden:

"Überlegungen für MetroCluster IP-Konfigurationen"

"Erstellen der DR-Gruppe"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Vergewissern Sie sich, dass die DR-Gruppe erstellt wurde.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                       node_A_1-old        node_B_1-old
                                       node_A_2-old        node_B_2-old
            cluster_B
                                       node_B_1-old        node_A_1-old
                                       node_B_2-old        node_A_2-old
2           cluster_A
                                       node_A_1-new        node_B_1-new
                                       node_A_2-new        node_B_2-new
            cluster_B
                                       node_B_1-new        node_A_1-new
                                       node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Konfigurieren Sie die MetroCluster IP-Schnittstellen für die neu verbundenen MetroCluster IP-Knoten:

- Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.
- Wenn unterstützt, können Sie ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) mit dem Parameter im Befehl angeben `-vlan-id` `metrocluster configuration-settings interface create`. Informationen zu unterstützten Plattformen finden Sie unter Überlegungen für VLANs beim Hinzufügen einer neuen DR-Gruppe .
- Sie können die MetroCluster-IP-Schnittstellen von beiden Clustern konfigurieren.

```
metrocluster configuration-settings interface create -cluster-name
```

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Überprüfen Sie, ob die MetroCluster-IP-Schnittstellen erstellt wurden:

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                 Home Port: e1a
                      172.17.28.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                 Home Port: e1a
                      172.17.28.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                 Home Port: e1a
                      172.17.28.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Verbinden Sie die MetroCluster IP-Schnittstellen:

   `metrocluster configuration-settings connection connect`

   Dieser Befehl kann einige Minuten dauern.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Überprüfen Sie, ob die Verbindungen ordnungsgemäß aufgebaut sind: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_1-new
                Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Überprüfen der automatischen Zuweisung und Partitionierung der Festplatte:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Root-Aggregate spiegeln:

```
storage aggregate mirror -aggregate aggr0_node_A_1-new
```

> Diesen Schritt müssen Sie bei jedem MetroCluster IP Node abschließen.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Überprüfen Sie, ob die Root-Aggregate gespiegelt wurden:

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Beenden des Hinzufügung der neuen Nodes

Sie müssen die neue DR-Gruppe in die MetroCluster Konfiguration einbinden und gespiegelte Datenaggregate auf den neuen Nodes erstellen.

Schritte

1. Aktualisieren Sie die MetroCluster-Konfiguration:

   a. Wechseln Sie in den erweiterten Berechtigungsmodus:

      ```
      set -privilege advanced
      ```

   b. Aktualisieren Sie die MetroCluster -Konfiguration auf einem der neu hinzugefügten Knoten:

Wenn Ihre MetroCluster Konfiguration…	Dann tun Sie das…
Mehrere Datenaggregate	Führen Sie an der Eingabeaufforderung eines beliebigen Knotens Folgendes aus: `metrocluster configure <node-name>`
Ein einziges gespiegeltes Datenaggregat an einem oder beiden Standorten	Konfigurieren Sie an einer beliebigen Node-Eingabeaufforderung die MetroCluster mit dem `-allow-with-one-aggregate true` Parameter: `metrocluster configure -allow-with-one-aggregate true <node-name>`

c. Starten Sie jeden der neuen Nodes neu:

```
node reboot -node <node_name> -inhibit-takeover true
```

> Die Nodes müssen nicht in einer bestimmten Reihenfolge neu gebootet werden. Sie sollten jedoch warten, bis ein Node vollständig gebootet wurde und alle Verbindungen hergestellt sind, bevor Sie den nächsten Node neu booten.

a. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

2. Erstellen von gespiegelten Datenaggregaten auf jedem der neuen MetroCluster Nodes:

```
storage aggregate create -aggregate <aggregate-name> -node <node-name>
-diskcount <no-of-disks> -mirror true
```

> Sie müssen mindestens ein gespiegeltes Datenaggregat pro Standort erstellen. Es wird empfohlen, zwei gespiegelte Datenaggregate pro Standort auf MetroCluster IP-Knoten zu haben, um die MDV-Volumes zu hosten. Allerdings wird ein einzelnes Aggregat pro Standort unterstützt (jedoch nicht empfohlen). Es ist akzeptabel, dass ein Standort der MetroCluster ein einziges gespiegeltes Datenaggregat hat und der andere Standort mehr als ein gespiegeltes Datenaggregat hat.

Das folgende Beispiel zeigt die Erstellung eines Aggregats auf Node_A_1-New.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex
```

```
        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. Vergewissern Sie sich, dass die Nodes zu ihrer DR-Gruppe hinzugefügt werden.

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Verschieben Sie die MDV_CRS-Volumes im erweiterten Berechtigungsmodus.

   a. Anzeigen der Volumes zur Identifizierung der MDV-Volumes:

      Wenn Sie ein einzelnes gespiegeltes Datenaggregat pro Standort haben, dann verschieben Sie beide MDV-Volumen zu diesem einzigen Aggregat. Wenn Sie zwei oder mehr gespiegelte Datenaggregate haben, dann verschieben Sie jedes MDV-Volume zu einem anderen Aggregat.

      Wenn Sie eine MetroCluster-Konfiguration mit vier Knoten auf eine permanente Konfiguration mit acht Knoten erweitern, sollten Sie eines der MDV-Volumes in die neue DR-Gruppe verschieben.

      Das folgende Beispiel zeigt die MDV-Volumes im `volume show` Ausgabe:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Legen Sie die erweiterte Berechtigungsebene fest:

```
set -privilege advanced
```

c. Verschieben Sie die MDV-Volumes nacheinander:

```
volume move start -volume <mdv-volume> -destination-aggregate <aggr-on-new-
node> -vserver <svm-name>
```

Das folgende Beispiel zeigt den Befehl und die Ausgabe für das Verschieben von "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A", um "Data_a3" auf "Node_A_3" zu aggregieren.

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Überprüfen Sie mit dem Befehl Volume show, ob das MDV-Volume erfolgreich verschoben wurde:

```
volume show <mdv-name>
```

Die folgende Ausgabe zeigt, dass das MDV-Volume erfolgreich verschoben wurde.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

5. Verschieben Sie Epsilon von einem alten Knoten auf einen neuen Knoten:

a. Identifizieren Sie, welcher Knoten derzeit über Epsilon verfügt:

```
cluster show -fields epsilon
```

```
cluster_B::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Stellen Sie das Epsilon auf „false“ auf dem alten Knoten (Node_A_1-old) ein:

```
cluster modify -node <old-node> -epsilon false*
```

c. Setzen Sie das Epsilon auf „true“ (Node_A_3-New):

```
cluster modify -node <new-node> -epsilon true
```

d. Vergewissern Sie sich, dass sich das Epsilon auf den richtigen Knoten bewegt hat:

```
cluster show -fields epsilon
```

```
cluster_A::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

6. Wenn Ihr System End-to-End-Verschlüsselung unterstützt, können Sie dies tun "End-to-End-Verschlüsselung" Auf der neuen DR-Gruppe.

Entfernen einer Disaster Recovery-Gruppe

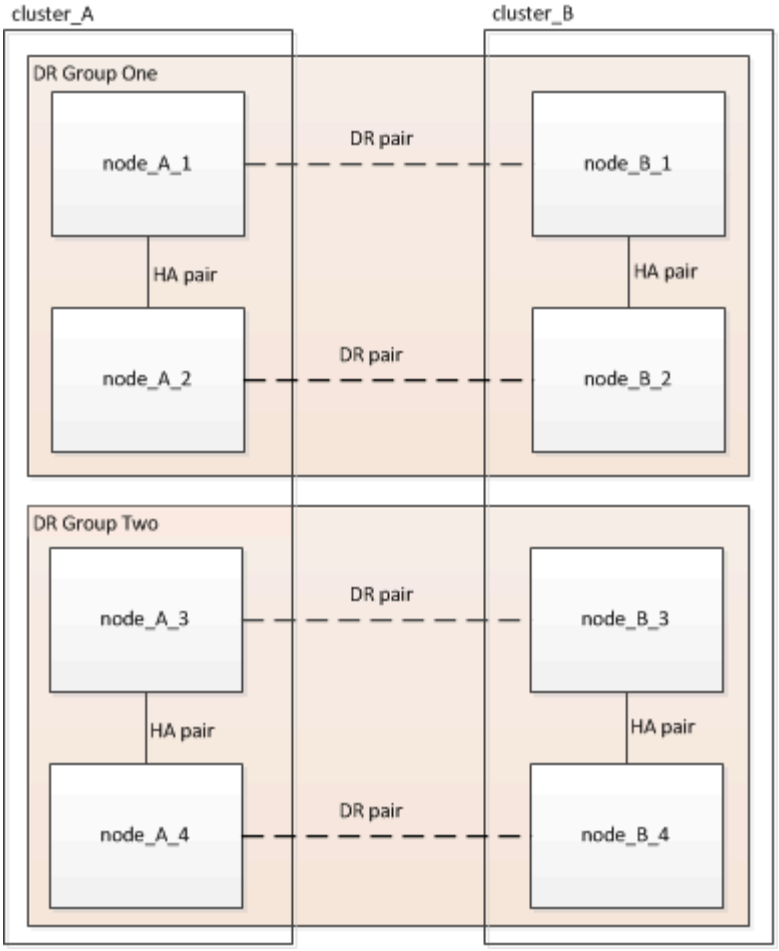
Ab ONTAP 9.8 können Sie eine DR-Gruppe aus einer MetroCluster Konfiguration mit acht Nodes entfernen, um eine MetroCluster Konfiguration mit vier Nodes zu erstellen.

Dieses Verfahren wird unter ONTAP 9.8 und höher unterstützt. Informationen zu Systemen mit ONTAP 9.7 oder einer älteren Version finden Sie im Knowledge Base-Artikel

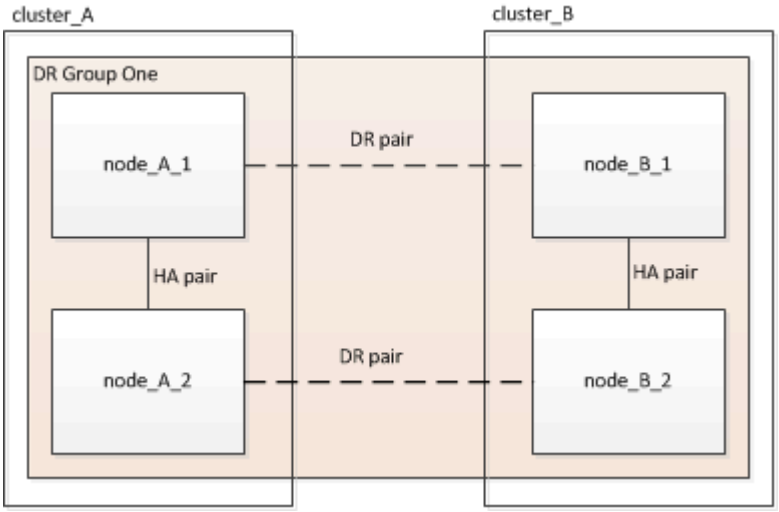
"So entfernen Sie eine DR-Gruppe aus einer MetroCluster-Konfiguration"

"NetApp Support"

Eine Konfiguration mit acht Nodes umfasst acht Nodes, die als zwei DR-Gruppen mit vier Nodes organisiert sind.



Durch Entfernen einer DR-Gruppe verbleiben vier Knoten in der Konfiguration.



Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für

die Dauer der Wartungsaktivität zu deaktivieren.

Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Entfernen der DR-Gruppen-Nodes aus jedem Cluster

Bevor Sie beginnen

- Sie müssen diesen Schritt auf beiden Clustern durchführen.
- Der `metrocluster remove-dr-group` Befehl wird nur auf ONTAP 9.8 und höher unterstützt.

Schritte

1. Bereiten Sie sich auf das Entfernen der DR-Gruppe vor, falls noch nicht.

   a. Verschieben Sie alle Daten-Volumes in eine andere DR-Gruppe.

   b. Wenn die zu entfernende DR-Gruppe Spiegelvolumes mit der Lastverteilung enthält, können sie nicht verschoben werden. Erstellen Sie alle Spiegelvolumes mit Lastenfreigabe in einer anderen DR-Gruppe erneut, und löschen Sie dann die Spiegelvolumes mit Lastenfreigabe in der zu entfernenden DR-Gruppe.

   c. Verschieben Sie alle MDV_CRS-Metadaten-Volumes in eine andere DR-Gruppe, indem Sie die befolgen "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen" Verfahren.

   d. Löschen Sie alle MDV_aud-Metadaten-Volumes, die in der zu entfernenden DR-Gruppe vorhanden sein könnten.

   e. Löschen Sie alle Datenaggregate in der DR-Gruppe, die entfernt werden sollen, wie im folgenden Beispiel gezeigt:

   ```
   ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
   -fields aggregate ,node
   ClusterA::> aggr delete -aggregate aggregate_name
   ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
   -fields aggregate ,node
   ClusterB::> aggr delete -aggregate aggregate_name
   ```

   Root-Aggregate werden nicht gelöscht.

   f. Verschieben Sie die Daten-LIFs offline.
   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin down`

   g. Migrieren Sie alle Daten-LIFs auf Home Nodes in einer anderen DR-Gruppe.
   `network interface show -home-node` *`old_node`*

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-node` *`new_node`* `-home-port` *`port-id`*

h. Verschieben Sie die Daten-LIFs wieder online.
`network interface modify -vserver svm-name -lif data-lif -status-admin up`

i. Migrieren Sie die Cluster-Management-LIF auf einen Home-Node in einer anderen DR-Gruppe.

```
network interface show -role cluster-mgmt

network interface modify -vserver svm-name -lif cluster_mgmt -home-node
new_node -home-port port-id
```

Das Node-Management und logische Schnittstellen zwischen Clustern werden nicht migriert.

a. Übertragen Sie Epsilon auf einen Node in einer anderen DR-Gruppe, falls erforderlich.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identifizieren und entfernen Sie die DR-Gruppe.

a. Identifizieren Sie die richtige DR-Gruppe für das Entfernen:

```
metrocluster node show
```

b. Entfernen Sie die Knoten der DR-Gruppe:
`metrocluster remove-dr-group -dr-group-id 1`

Im folgenden Beispiel wird das Entfernen der Konfiguration der DR-Gruppe auf „Cluster_A“ gezeigt

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B"to remove the remote nodes in the DR
group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not completed
on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Wiederholen Sie den vorherigen Schritt im Partner-Cluster.
4. Entfernen Sie bei einer MetroCluster IP-Konfiguration die MetroCluster-Verbindungen auf den Nodes der alten DR-Gruppe.

   Diese Befehle können von beiden Clustern ausgegeben werden und gelten für die gesamte DR-Gruppe, die beide Cluster abdeckt.

   a. Trennen Sie die Verbindungen:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Löschen Sie die MetroCluster-Schnittstellen auf den Knoten der alten DR-Gruppe:

```
metrocluster configuration-settings interface delete
```

c. Löschen Sie die Konfiguration der alten DR-Gruppe.
```
metrocluster configuration-settings dr-group delete
```

5. Heben Sie die Verbindung zu den Knoten in der alten DR-Gruppe auf.

   Sie müssen diesen Schritt für jedes Cluster durchführen.

   a. Legen Sie die erweiterte Berechtigungsebene fest:

   ```
   set -privilege advanced
   ```

   b. Deaktivieren des Speicher-Failover:

   ```
   storage failover modify -node node-name -enable false
   ```

   c. Heben Sie die Verbindung zum Knoten auf:
   ```
   cluster unjoin -node node-name
   ```

   Wiederholen Sie diesen Schritt für den anderen lokalen Knoten in der alten DR-Gruppe.

   d. Legen Sie die Administrator-Berechtigungsebene fest:
   ```
   set -privilege admin
   ```

6. Cluster-HA in der neuen DR-Gruppe erneut aktivieren:

   ```
   cluster ha modify -configured true
   ```

   Sie müssen diesen Schritt für jedes Cluster durchführen.

7. Halten Sie den Vorgang an, schalten Sie ihn aus und entfernen Sie die alten Controller-Module und Storage-Shelfs.

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen

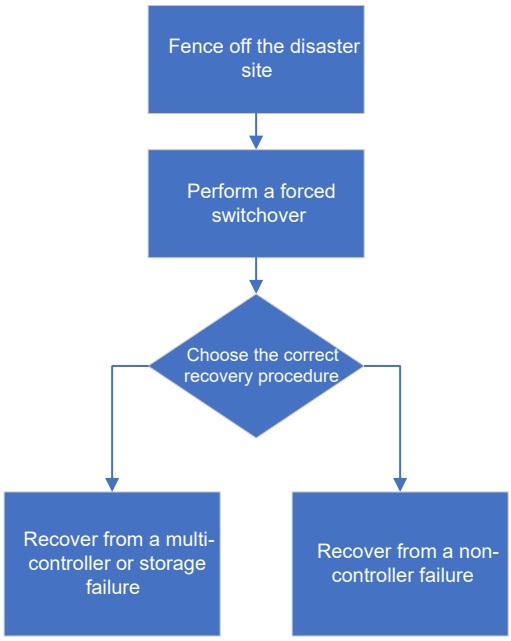
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management und Disaster Recovery"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln • Disaster Recovery
"Warten von MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes

"MetroCluster: Upgrade, Transition und Erweiterung"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"Installation und Konfiguration der MetroCluster Tiebreaker Software"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Dokumentation zu ONTAP Hardwaresystemen" In MetroCluster IP-Konfigurationen können Standardwartungsverfahren für Storage Shelves verwendet werden.	• Hot-Adding eines Festplatten-Shelfs • Hot-entfernen eines Festplatten-Shelfs
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate

Nach einem Ausfall wiederherstellen

Workflow für Disaster Recovery

Verwenden Sie den Workflow für die Durchführung der Disaster Recovery.



Durchführen einer erzwungenen Umschaltung nach einem Ausfall

Bei einem Ausfall müssen nach dem Switchover beide Schritte in Bezug auf das Disaster-Cluster und das noch funktionsfähige Cluster ausgeführt werden, um einen sicheren und kontinuierlichen Datenservice zu gewährleisten.

Ermitteln, ob ein Notfall aufgetreten ist, erfolgt durch:

- Einem Administrator
- Die MetroCluster Tiebreaker Software, wenn sie konfiguriert ist
- Die ONTAP Mediator-Software, sofern sie konfiguriert ist

Fechten vor dem Disaster-Standort

Falls die Disaster-Site-Nodes nach dem Ausfall ausgetauscht werden müssen, müssen diese unterbrochen werden, um einen Wiederaufnahme des Service am Standort zu verhindern. Andernfalls riskieren Sie die Gefahr einer Beschädigung von Daten, wenn Clients vor dem Abschluss des Austauschvorgangs auf die Nodes zugreifen.

Schritt

1. Beenden Sie die Nodes am Disaster Site, und halten Sie sie herunterfahren oder an der LOADER-

Eingabeaufforderung, bis das Boot ONTAP geleitet wird:

```
system node halt -node disaster-site-node-name
```

Wenn die Disaster-Site-Nodes zerstört wurden oder nicht angehalten werden können, schalten Sie den Strom an die Nodes aus, und starten Sie die Ersatz-Nodes erst, wenn Sie im Wiederherstellungsvorgang weitergeleitet werden.

Erzwungene Umschaltung durchführen

Neben dem unterbrechungsfreien Betrieb bei Test und Wartung ermöglicht die Umschaltung mit einem einzigen Befehl ein Recovery nach einem Standortausfall.

Bevor Sie beginnen

- Mindestens einer der verbleibenden Standortknoten muss vor dem Switchover betriebsbereit sein.
- Alle früheren Konfigurationsänderungen müssen abgeschlossen sein, bevor Sie einen Switchback-Vorgang durchführen.

  Damit wird der Wettbewerb mit dem ausgehandelten Switchover- oder Switchback-Betrieb vermieden.

> SnapMirror und SnapVault Konfigurationen werden automatisch gelöscht.

Über diese Aufgabe

Der `metrocluster switchover` Command Switches über die Nodes in allen DR-Gruppen in der MetroCluster Konfiguration. In einer MetroCluster Konfiguration mit acht Nodes wechselt sie beispielsweise über die Nodes in beiden DR-Gruppen.

Schritte

1. Führen Sie die Umschaltung durch, indem Sie den folgenden Befehl am verbleibenden Standort ausführen:

   ```
   metrocluster switchover -forced-on-disaster true
   ```

   > Der Vorgang kann einige Minuten dauern. Sie können den Fortschritt mithilfe des überprüfen `metrocluster operation show` Befehl.

2. Antwort `y` Wenn Sie dazu aufgefordert werden, mit der Umschaltung fortzufahren.
3. Überprüfen Sie, ob die Umschaltung erfolgreich abgeschlossen wurde, indem Sie den ausführen `metrocluster operation show` Befehl.

```
mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

Wenn die Umschaltung vetoed ist, haben Sie die Möglichkeit, die neu zu stellen `metrocluster switchover-forced-on-disaster true` Befehl mit dem `--override-vetoes` Option. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Umschaltung verhinderten.

Nachdem Sie fertig sind

SnapMirror Beziehungen müssen nach der Umschaltung neu hergestellt werden.

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 über das Root-Aggregat umgeschalteten Zustands unbestimmt und wird als fehlgeschlagen angezeigt. Während dieser Zeit wird die umschaltete Root nicht aktualisiert. Der tatsächliche Status dieses Plex kann nur nach der MetroCluster-Heilungsphase ermittelt werden.

Zugriff auf Volumes im Status „NV-Fehler“ nach einer Umschaltung

Nach einer Umschaltung müssen Sie den NV-Fehler-Status löschen, indem Sie den zurücksetzen `-in -nvfailed-state` Parameter von `volume modify` Befehl, um die Einschränkung von Clients für den Zugriff auf Daten zu entfernen.

Bevor Sie beginnen

Die Datenbank oder das Dateisystem dürfen nicht ausgeführt werden oder es darf versucht werden, auf das betroffene Volume zuzugreifen.

Über diese Aufgabe

Einstellen des `-in-nvfailed-state` Für Parameter ist die Berechtigung auf erweiterter Ebene erforderlich.

Schritt

1. Stellen Sie das Volume mithilfe von wieder her `volume modify` Befehl mit dem `-in-nvfailed-state` Parameter auf false gesetzt.

Nachdem Sie fertig sind

Anweisungen zur Überprüfung der Gültigkeit von Datenbankdateien finden Sie in der Dokumentation für Ihre spezifische Datenbanksoftware.

Wenn Ihre Datenbank LUNs verwendet, überprüfen Sie die Schritte, um nach einem NVRAM-Fehler den Host Zugriff auf die LUNs zu ermöglichen.

Verwandte Informationen

"Überwachung und Schutz der Datenbankgültigkeit mithilfe von NVFAIL"

Auswahl des richtigen Wiederherstellungsverfahrens

Nach einem Fehler in einer MetroCluster-Konfiguration müssen Sie das richtige Wiederherstellungsverfahren auswählen. Verwenden Sie die folgende Tabelle und Beispiele, um das entsprechende Wiederherstellungsverfahren auszuwählen.

Bei diesen Informationen in dieser Tabelle wird davon ausgegangen, dass die Installation oder der Übergang abgeschlossen ist, d. h., dass der `metrocluster configure` Befehl erfolgreich ausgeführt.

Umfang der Ausfälle am Disaster-Standort	Verfahren
• Kein Hardwarefehler (z. B. ein Stromausfall)	"Wiederherstellung nach einem Ausfall eines Controllers"
• Kein Controller-Modul-Fehler • Andere Hardware ist ausgefallen	"Wiederherstellung nach einem Ausfall eines Controllers"
• Ausfall eines einzelnen Controller-Moduls oder Ausfall von FRU-Komponenten innerhalb des Controller-Moduls • Laufwerke sind nicht ausgefallen	Wenn ein Fehler auf ein einzelnes Controller-Modul beschränkt ist, müssen Sie das FRU-Ersatzverfahren für das Controller-Modul für das Plattformmodell verwenden. In einer MetroCluster Konfiguration mit vier oder acht Nodes ist ein solcher Ausfall für das lokale HA-Paar isoliert. **Hinweis:** das FRU-Ersatzverfahren für das Controller-Modul kann in einer MetroCluster-Konfiguration mit zwei Knoten verwendet werden, wenn kein Laufwerk oder andere Hardware-Ausfälle auftreten. "Dokumentation zu ONTAP Hardwaresystemen"
• Ausfall eines einzelnen Controller-Moduls oder Ausfall von FRU-Komponenten innerhalb des Controller-Moduls • Laufwerke ausgefallen	"Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"

• Ausfall eines einzelnen Controller-Moduls oder Ausfall von FRU-Komponenten innerhalb des Controller-Moduls • Laufwerke sind nicht ausgefallen • Zusätzliche Hardware außerhalb des Controller-Moduls ist ausgefallen	"Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall" Sie sollten alle Schritte für die Antriebszuweisung überspringen.
• Ausfall mehrerer Controller-Module (mit oder ohne zusätzlichen Ausfall) innerhalb einer DR-Gruppe	"Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"

Ausfallszenarien für Controller-Module während der MetroCluster-Installation

Die Reaktion auf einen Ausfall eines Controller-Moduls während des MetroCluster-Konfigurationsverfahrens hängt davon ab, ob der `metrocluster configure` Befehl erfolgreich abgeschlossen.

- Wenn der `metrocluster configure` Der Befehl wurde noch nicht ausgeführt oder ist fehlgeschlagen. Sie müssen das Verfahren zur Konfiguration der MetroCluster Software von Anfang an mit einem Ersatz-Controller-Modul neu starten.

  Führen Sie die Schritte in aus "Systemeinstellungen auf einem Controller-Modul werden wiederhergestellt" Auf jedem Controller (einschließlich des Ersatz-Controllers) überprüfen, ob die vorherige Konfiguration entfernt wurde.

- Wenn der `metrocluster configure` Befehl erfolgreich abgeschlossen und wenn das Controller-Modul ausfällt, verwenden Sie die vorherige Tabelle, um das richtige Wiederherstellungsverfahren zu bestimmen.

Ausfallszenarien für Controller-Module bei der Umstellung von MetroCluster FC zu IP

Das Recovery-Verfahren kann angewendet werden, wenn während der Umstellung ein Standortausfall auftritt. Sie kann jedoch nur verwendet werden, wenn die Konfiguration eine stabile gemischte Konfiguration ist, bei der FC DR-Gruppe und der IP DR-Gruppe beide vollständig konfiguriert sind. Die Ausgabe des `metrocluster node show` Der Befehl sollte beide DR-Gruppen mit allen acht Nodes anzeigen.

Wenn während der Transition der Fehler aufgetreten ist, während die Nodes hinzugefügt oder entfernt werden, müssen Sie sich an den technischen Support wenden.

Szenarien für Controller-Module in MetroCluster Konfigurationen mit acht Nodes

Ausfallszenarien:

- Ausfall eines einzelnen Controller-Moduls in einer einzelnen DR-Gruppe
- Zwei Controller-Modulfehler in einer einzelnen DR-Gruppe
- Ausfall eines einzelnen Controller-Moduls in separaten DR-Gruppen
- Drei Controller-Ausfälle verteilen sich auf die DR-Gruppen

Ausfall eines einzelnen Controller-Moduls in einer einzelnen DR-Gruppe

In diesem Fall ist der Fehler auf ein HA-Paar beschränkt.

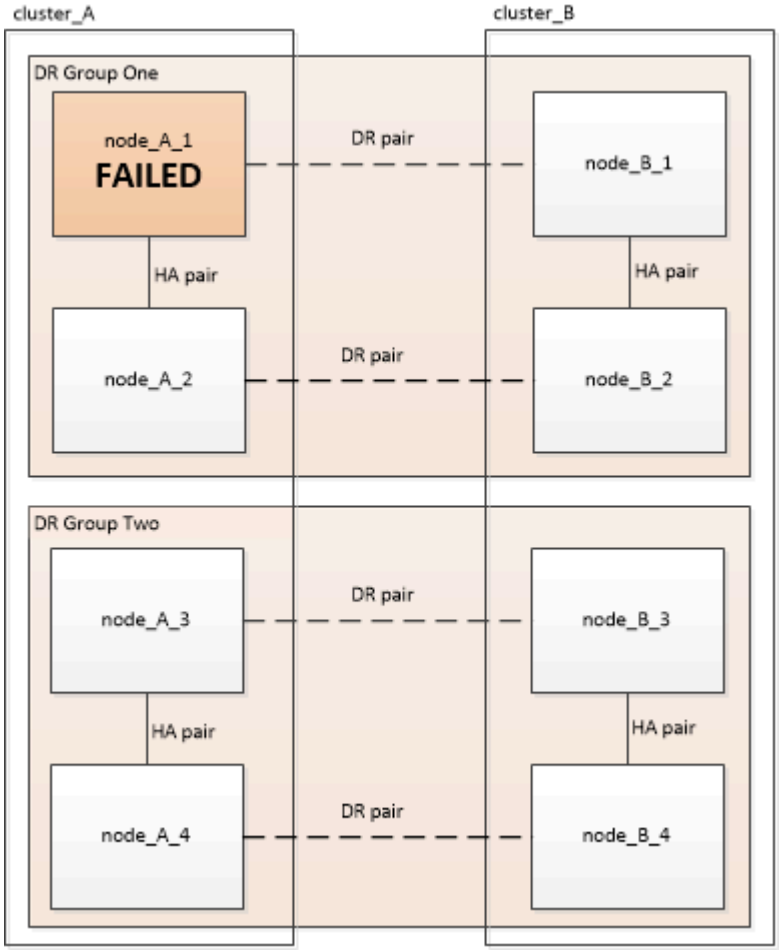
- Wenn kein Storage ausgetauscht werden muss, können Sie das FRU-Ersatzverfahren für das Plattformmodell verwenden.

  "Dokumentation zu ONTAP Hardwaresystemen"

- Wenn Speicher ausgetauscht werden muss, können Sie das Verfahren zur Wiederherstellung von Multi-Controller-Modulen verwenden.

  "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"

  Dieses Szenario gilt auch für MetroCluster-Konfigurationen mit vier Nodes.

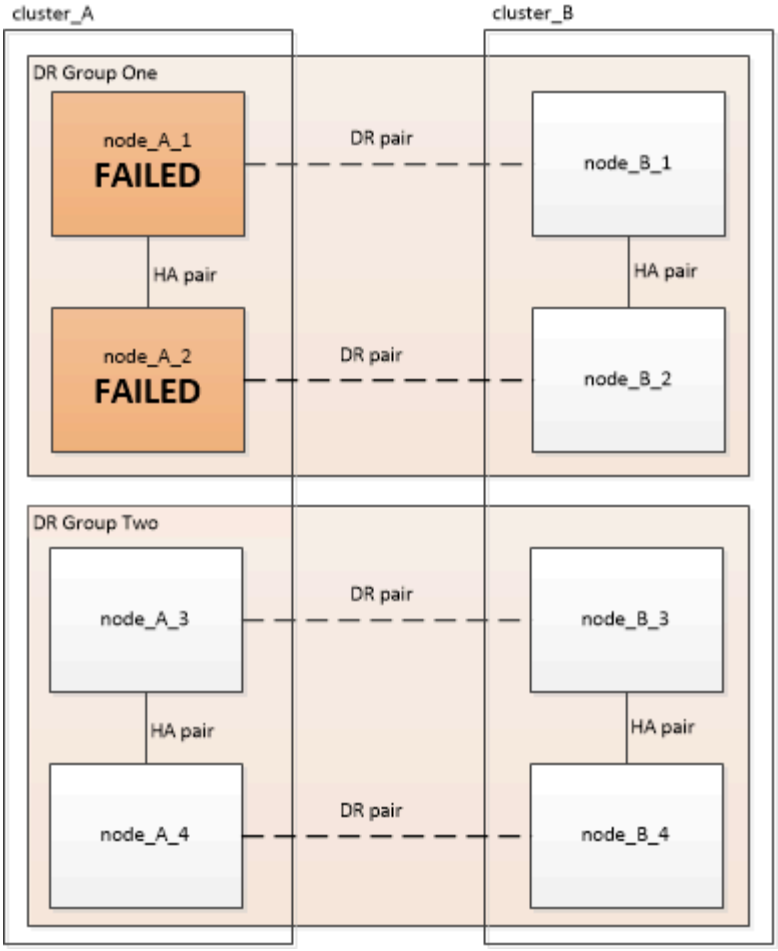


Zwei Controller-Modulfehler in einer einzelnen DR-Gruppe

In diesem Fall erfordert der Ausfall eine Umschaltung. Sie können das Wiederherstellungsverfahren für Fehler mit mehreren Controllern verwenden.

"Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"

Dieses Szenario gilt auch für MetroCluster-Konfigurationen mit vier Nodes.



Ausfall eines einzelnen Controller-Moduls in separaten DR-Gruppen

In diesem Fall ist der Fehler auf separate HA-Paare beschränkt.

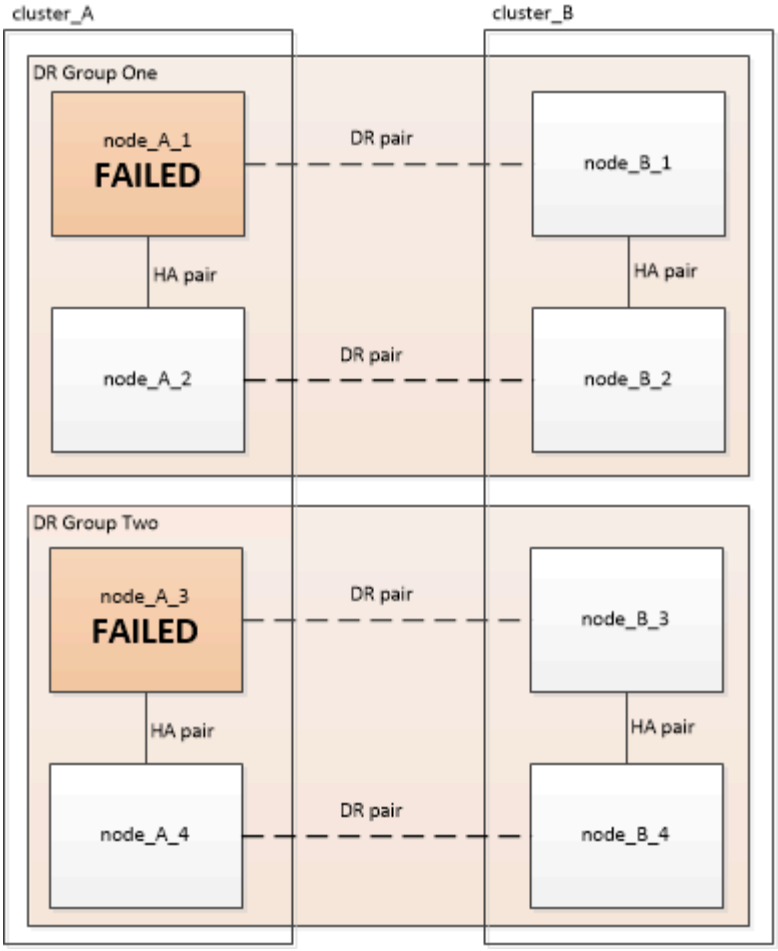
- Wenn kein Storage ausgetauscht werden muss, können Sie das FRU-Ersatzverfahren für das Plattformmodell verwenden.

  Der FRU-Austausch wird zweimal pro ausgefallenem Controller-Modul durchgeführt.

  "Dokumentation zu ONTAP Hardwaresystemen"

- Wenn Speicher ausgetauscht werden muss, können Sie das Verfahren zur Wiederherstellung von Multi-Controller-Modulen verwenden.

  "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"



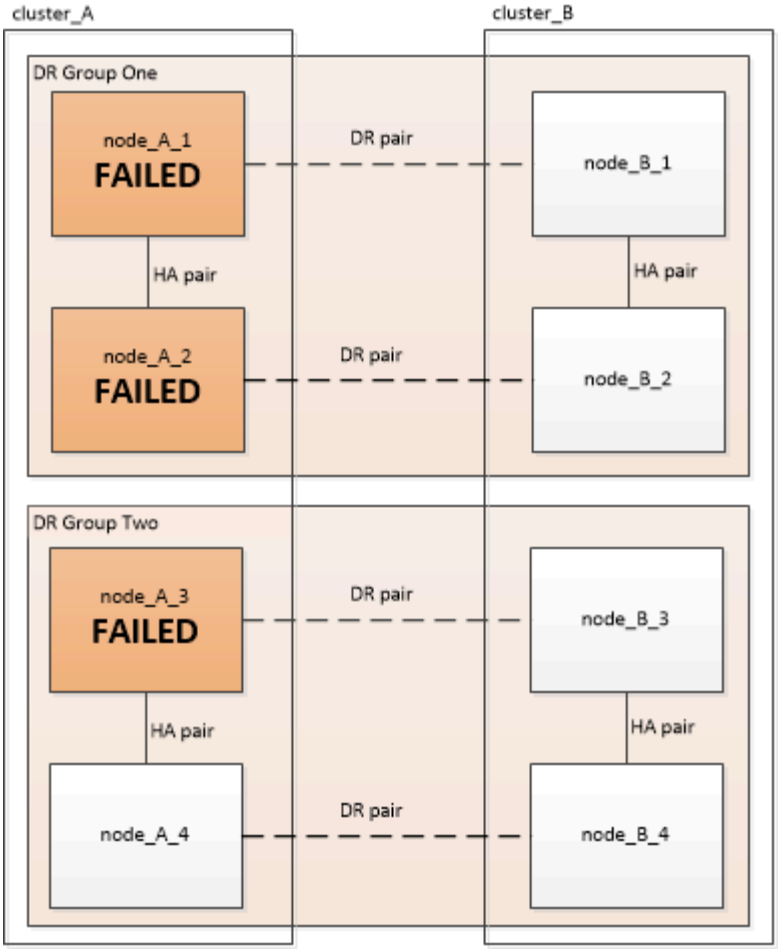
Drei Controller-Ausfälle verteilen sich auf die DR-Gruppen

In diesem Fall erfordert der Ausfall eine Umschaltung. Sie können das Wiederherstellungsverfahren für die Wiederherstellung von Multicontrollermodulen für DR-Gruppe 1 verwenden.

"Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"

Sie können das plattformspezifische FRU-Ersatzverfahren für das Controller-Modul für DR-Gruppe 2 verwenden.

"Dokumentation zu ONTAP Hardwaresystemen"



Szenarien für Fehler im Controller-Modul in MetroCluster-Konfigurationen mit zwei Nodes

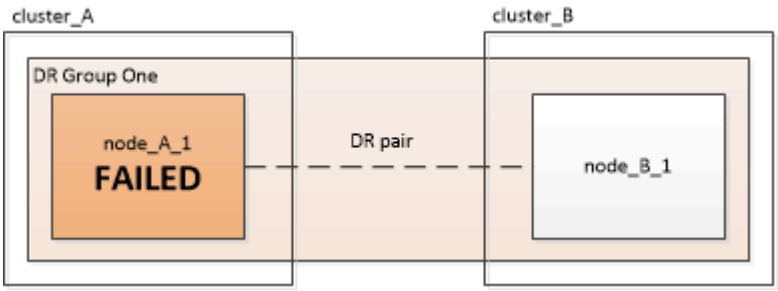
Das Verfahren, das Sie verwenden, hängt vom Umfang des Fehlers ab.

- Wenn kein Storage ausgetauscht werden muss, können Sie das FRU-Ersatzverfahren für das Plattformmodell verwenden.

  "Dokumentation zu ONTAP Hardwaresystemen"

- Wenn Speicher ausgetauscht werden muss, können Sie das Verfahren zur Wiederherstellung von Multi-Controller-Modulen verwenden.

  "Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall"



Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall

Wiederherstellung nach einem Multi-Controller- oder Storage-Ausfall

Wenn der Controller-Ausfall alle Controller-Module auf einer Seite einer DR-Gruppe in einer MetroCluster Konfiguration umfasst (einschließlich eines einzelnen Controllers in einer MetroCluster Konfiguration mit zwei Nodes), oder wenn der Storage ausgetauscht wurde, müssen die Geräte ersetzt und die Eigentumsrechte an Laufwerken neu zugewiesen werden, um bei einem Ausfall die Wiederherstellung zu ermöglichen.

Vergewissern Sie sich, dass Sie die folgenden Aufgaben überprüft und ausgeführt haben, bevor Sie dieses Verfahren verwenden:

- Überprüfen Sie die verfügbaren Wiederherstellungsverfahren, bevor Sie sich für die Verwendung dieses Verfahrens entscheiden.

  "Auswahl des richtigen Wiederherstellungsverfahrens"

- Vergewissern Sie sich, dass die Konsolenprotokollierung auf Ihren Geräten aktiviert ist.

  "Aktivieren Sie die Konsolenprotokollierung"

- Stellen Sie sicher, dass der Katastrophenort abgetrennt ist.

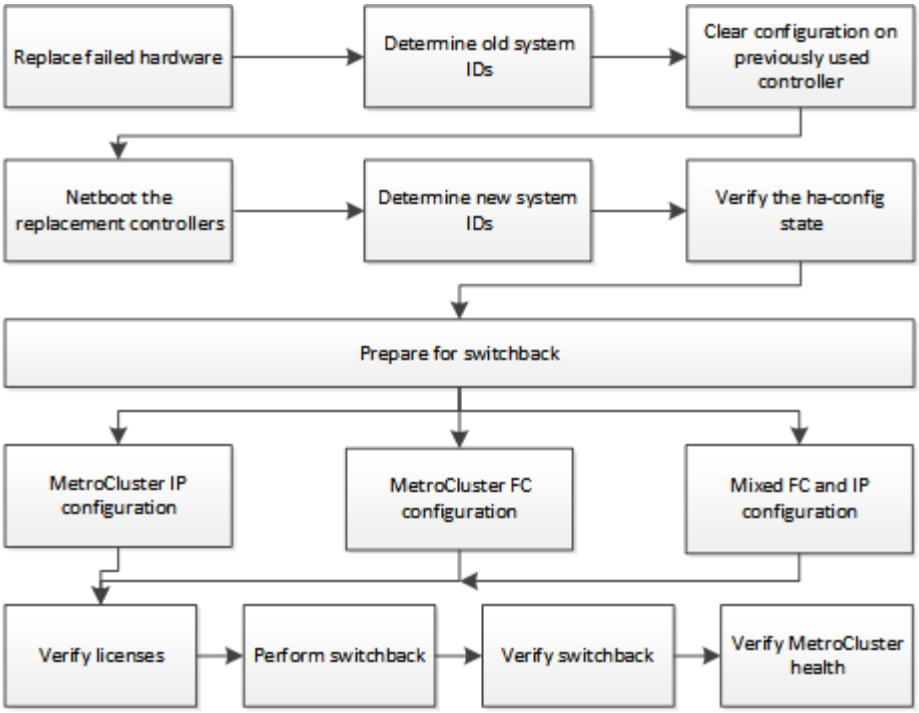
  "Fechten vor dem Disaster-Standort".

- Vergewissern Sie sich, dass die Umschaltung durchgeführt wurde.

  "Erzwungene Umschaltung durchführen".

- Stellen Sie sicher, dass die Ersatzlaufwerke und die Controller-Module neu sind und zuvor keine Eigentumsrechte zugewiesen wurden.
- Die Beispiele in diesem Verfahren zeigen Konfigurationen mit zwei oder vier Nodes. Wenn eine Konfiguration mit acht Nodes vorhanden ist (zwei DR-Gruppen), müssen Fehler berücksichtigt und die erforderliche Recovery-Aufgabe auf den zusätzlichen Controller-Modulen ausgeführt werden.

Bei diesem Verfahren wird folgender Workflow verwendet:



Dieses Verfahren kann bei der Wiederherstellung auf einem System verwendet werden, das sich während des Ausfalls in der Mitte des Übergangs befand. In diesem Fall müssen Sie die entsprechenden Schritte durchführen, wenn Sie sich für den Wechsel vorbereiten, wie in der Prozedur angegeben.

Aktivieren Sie die Konsolenprotokollierung

Aktivieren Sie Konsole-Protokollierung auf Ihren Geräten, bevor Sie Hardware ersetzen und neue Controller booten.

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Ersetzen Sie die Hardware und starten Sie neue Controller

Wenn Hardwarekomponenten ersetzt werden müssen, müssen Sie sie durch die einzelnen Hardware-Austauschrichtlinien und Installationshandbücher austauschen.

Austausch der Hardware am Notfallstandort

Bevor Sie beginnen

Die Storage-Controller müssen ausgeschaltet sein oder angehalten bleiben (zeigt die LOADER-Eingabeaufforderung an).

Schritte

1. Tauschen Sie die Komponenten bei Bedarf aus.

> In diesem Schritt ersetzen und verkabeln Sie die Komponenten genau so, wie sie vor der Katastrophe verkabelt waren. Sie dürfen die Komponenten nicht einschalten.

Wenn Sie ersetzen…	Führen Sie diese Schritte aus…	Verwenden Sie diese Leitfäden…
FC Switches in einer MetroCluster FC-Konfiguration	a. Installieren Sie die neuen Switches. b. ISL-Links verkabeln. Schalten Sie die FC-Switches derzeit nicht ein.	"Warten von MetroCluster-Komponenten"
IP-Switches in einer MetroCluster IP-Konfiguration	a. Installieren Sie die neuen Switches. b. ISL-Links verkabeln. Schalten Sie die IP-Schalter derzeit nicht ein.	"MetroCluster IP-Installation und -Konfiguration: Unterschiede zwischen den ONTAP MetroCluster-Konfigurationen"
Platten-Shelfs	a. Installieren Sie die Festplatten-Shelfs und Festplatten. ◦ Festplatten-Shelf-Stacks sollten die gleiche Konfiguration sein wie am verbleibenden Standort. ◦ Festplatten können dieselbe oder größer sein, müssen jedoch vom gleichen Typ (SAS oder SATA) sein. b. Verkabeln Sie die Festplatten-Shelfs mit angrenzenden Shelfs im Stack und mit der FC-to-SAS Bridge. Schalten Sie die Festplatten-Shelfs derzeit nicht ein.	"Dokumentation zu ONTAP Hardwaresystemen"
SAS-Kabel	a. Installieren Sie die neuen Kabel. Schalten Sie die Festplatten-Shelfs derzeit nicht ein.	"Dokumentation zu ONTAP Hardwaresystemen"

Bridges von FC-zu-SAS in einer MetroCluster FC-Konfiguration	a. Die FC-to-SAS-Bridges installieren. b. Verbinden Sie die FC-to-SAS-Bridges. Verkabeln Sie sie je nach Ihrem MetroCluster-Konfigurationstyp mit FC-Switches oder den Controller-Modulen. Schalten Sie die Bridges von FC-to-SAS derzeit nicht ein.	"Installation und Konfiguration von Fabric-Attached MetroCluster" "Installation und Konfiguration von Stretch MetroCluster"

Controller-Module	a. Installieren der neuen Controller-Module: ◦ Die Controller-Module müssen das gleiche Modell sein wie die zu ersetzenden. Beispiel: 8080 Controller-Module müssen durch 8080 Controller-Module ersetzt werden. ◦ Die Controller-Module dürfen bisher nicht zu einem der Cluster innerhalb der MetroCluster Konfiguration oder einer zuvor bestehenden Cluster-Konfiguration gehören. Wenn dies der Fall ist, müssen Sie Standardwerte festlegen und einen “wipeconfig”-Prozess durchführen. ◦ Stellen Sie sicher, dass sich alle Netzwerkkarten (wie Ethernet oder FC) in denselben Steckplätzen befinden, die in den alten Controller-Modulen verwendet werden. b. Die neuen Controller-Module genau wie die alten verkabeln. Die Ports, die das Controller-Modul mit dem Storage verbinden (entweder durch Verbindungen mit IP- oder FC-Switches, FC-to-SAS-Bridges oder direkt), sollten dieselben sein wie vor der Katastrophe. Schalten Sie die Controller-Module derzeit nicht ein.	"Dokumentation zu ONTAP Hardwaresystemen"

2. Stellen Sie sicher, dass alle Komponenten für Ihre Konfiguration korrekt verkabelt sind.

- "MetroCluster IP-Konfiguration"
- "MetroCluster Fabric-Attached-Konfiguration"

Ermitteln Sie die System-IDs und VLAN-IDs der alten Controller-Module

Nachdem Sie die gesamte Hardware am Disaster-Standort ausgetauscht haben, müssen Sie die System-IDs der ersetzten Controller-Module ermitteln. Sie benötigen die alten System-IDs, wenn Sie Festplatten den neuen Controller-Modulen neu zuweisen. Bei Systemen wie AFF A220, AFF A250, AFF A400, AFF A800, FAS2750 Modelle FAS500f, FAS8300 oder FAS8700 müssen auch die von den MetroCluster IP-Schnittstellen verwendeten VLAN-IDs ermittelt werden.

Bevor Sie beginnen

Alle Geräte am Disaster-Standort müssen ausgeschaltet sein.

Über diese Aufgabe

Diese Diskussion enthält Beispiele für Konfigurationen mit zwei und vier Nodes. Bei Konfigurationen mit acht Nodes müssen Ausfälle in den zusätzlichen Nodes der zweiten DR-Gruppe berücksichtigt werden.

Bei einer MetroCluster Konfiguration mit zwei Nodes können Sie Verweise auf das zweite Controller-Modul an jedem Standort ignorieren.

Die Beispiele in diesem Verfahren basieren auf folgenden Annahmen:

- Standort A ist der Notfallstandort.
- Node_A_1 ist ausgefallen und wird vollständig ersetzt.
- Node_A_2 ist ausgefallen und wird vollständig ersetzt.

  Node _A_2 ist nur in einer MetroCluster-Konfiguration mit vier Nodes vorhanden.

- Standort B ist der überlebende Standort.
- Node_B_1 ist in einem ordnungsgemäßen Zustand.
- Node_B_2 ist in einem ordnungsgemäßen Zustand.

  Node_B_2 ist nur in einer MetroCluster-Konfiguration mit vier Knoten vorhanden.

Die Controller-Module verfügen über die folgenden ursprünglichen System-IDs:

Anzahl der Knoten in der MetroCluster-Konfiguration	Knoten	Ursprüngliche System-ID
Vier	Node_A_1	4068741258
Node_A_2	4068741260	Knoten_B_1
4068741254	Knoten_B_2	4068741256
Zwei	Node_A_1	4068741258

Schritte

1. Zeigen Sie am verbleibenden Standort die System-IDs der Nodes in der MetroCluster-Konfiguration an.

Anzahl der Knoten in der MetroCluster-Konfiguration	Verwenden Sie diesen Befehl
Vier oder acht	`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`
Zwei	`metrocluster node show -fields node-systemid,dr-partner-systemid`

In diesem Beispiel für eine MetroCluster-Konfiguration mit vier Nodes werden die folgenden alten System-IDs abgerufen:

- Node_A_1: 4068741258
- Node_A_2: 4068741260

  Festplatten, die zu den alten Controller-Modulen gehören, sind immer noch im Besitz dieser System-IDs.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  4068741258    4068741260
4068741254          4068741256
1           Cluster_A  Node_A_2  4068741260    4068741258
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

  In diesem Beispiel für eine MetroCluster-Konfiguration mit zwei Nodes wird die folgende alte System-ID abgerufen:

- Node_A_1: 4068741258

  Festplatten, die dem alten Controller-Modul gehören, sind immer noch im Besitz dieser System-ID.

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1  4068741258    4068741254
1           Cluster_B  Node_B_1  -             -
2 entries were displayed.
```

2. Für MetroCluster-IP-Konfigurationen mit ONTAP Mediator erhalten Sie die IP-Adresse von ONTAP Mediator:

   ```
   storage iscsi-initiator show -node * -label mediator
   ```

3. Bei den Systemen handelt es sich um AFF A220, AFF A400, FAS2750, FAS8300 oder FAS8700. Ermitteln der VLAN-IDs:

   ```
   metrocluster interconnect show
   ```

   Die VLAN-IDs sind in den Adapternamen enthalten, der in der Spalte Adapter der Ausgabe angezeigt wird.

   In diesem Beispiel sind die VLAN-IDs 120 und 130:

```
metrocluster interconnect show
                          Mirror   Mirror
                  Partner Admin    Oper
Node Partner Name Type    Status   Status  Adapter Type   Status
---- ------------ ------- -------- ------- ------- ------ ------
Node_A_1 Node_A_2 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
Node_A_2 Node_A_1 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
12 entries were displayed.
```

Isolierung von Ersatzlaufwerken vom verbleibenden Standort (MetroCluster IP-Konfigurationen)

Sie müssen alle Ersatzlaufwerke isolieren, indem Sie die MetroCluster iSCSI-Initiator-Verbindungen von den noch intakten Nodes trennen.

Über diese Aufgabe

Dieses Verfahren ist nur bei MetroCluster IP-Konfigurationen erforderlich.

Schritte

1. Ändern Sie von der Eingabeaufforderung eines verbleibenden Node auf die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   Sie müssen mit reagieren `y` Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*) anzuzeigen.

2. Trennen Sie die iSCSI-Initiatoren auf beiden noch intakten Knoten der DR-Gruppe:

   ```
   storage iscsi-initiator disconnect -node surviving-node -label *
   ```

   Dieser Befehl muss zweimal pro den noch intakten Nodes ausgegeben werden.

   Im folgenden Beispiel werden die Befehle zum Trennen der Initiatoren auf Standort B angezeigt:

   ```
   site_B::*> storage iscsi-initiator disconnect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator disconnect -node node_B_2 -label *
   ```

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Löschen Sie die Konfiguration auf einem Controller-Modul

Bevor Sie in der MetroCluster-Konfiguration ein neues Controller-Modul verwenden, müssen Sie die vorhandene Konfiguration löschen.

Schritte

1. Halten Sie den Node gegebenenfalls an, um die Eingabeaufforderung anzuzeigen `LOADER`:

   ```
   halt
   ```

2. Legen Sie an der `LOADER` Eingabeaufforderung die Umgebungsvariablen auf die Standardwerte fest:

   ```
   set-defaults
   ```

3. Umgebung speichern:

   ```
   saveenv
   ```

4. Starten Sie an der `LOADER` Eingabeaufforderung das Startmenü:

```
boot_ontap menu
```

5. Löschen Sie an der Eingabeaufforderung des Startmenüs die Konfiguration:

   ```
   wipeconfig
   ```

   Antworten `yes` An die Bestätigungsaufforderung.

   Der Node wird neu gebootet, und das Startmenü wird erneut angezeigt.

6. Wählen Sie im Startmenü die Option **5**, um das System im Wartungsmodus zu booten.

   Antworten `yes` An die Bestätigungsaufforderung.

Booten Sie die neuen Controller-Module ein

Wenn die neuen Controller-Module eine andere Version von ONTAP als die Version der verbleibenden Controller-Module aufweisen, müssen Sie die neuen Controller-Module als Netzboot bereitstellen.

Bevor Sie beginnen

- Sie müssen Zugriff auf einen HTTP-Server haben.
- Sie müssen auf die NetApp Support-Website zugreifen können, um die erforderlichen Systemdateien für Ihre Plattform und die Version der darauf ausgeführten ONTAP Software herunterzuladen.

  "NetApp Support"

Schritte

1. Auf das zugreifen "NetApp Support Website" Zum Herunterladen der Dateien zum Ausführen des Netzboots des Systems.
2. Laden Sie die entsprechende ONTAP Software aus dem Abschnitt zum Software-Download der NetApp Support-Website herunter und speichern Sie die Datei ontap-Version_image.tgz in einem über Web zugänglichen Verzeichnis.
3. Rufen Sie das Verzeichnis mit Webzugriff auf, und stellen Sie sicher, dass die benötigten Dateien verfügbar sind.

Wenn das Plattformmodell…	Dann…
Systeme der FAS/AFF8000 Serie	Extrahieren Sie den Inhalt der ontap-Version_image.tgzfile in das Zielverzeichnis: Tar -zxvf ontap-Version_image.tgz HINWEIS: Wenn Sie den Inhalt auf Windows extrahieren, verwenden Sie 7-Zip oder WinRAR, um das Netzboot Image zu extrahieren. Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei:Netzboot/Kernel enthalten
Alle anderen Systeme	Ihre Verzeichnisliste sollte einen Netzboot-Ordner mit einer Kernel-Datei enthalten: ontap-Version_image.tgz Sie müssen nicht die ontap-Version_image.tgz-Datei extrahieren.

4. Konfigurieren Sie an der Eingabeaufforderung DES LOADERS die Netzboot-Verbindung für eine

Management-LIF:

- Wenn die IP-Adresse DHCP ist, konfigurieren Sie die automatische Verbindung:

  ```
  ifconfig e0M -auto
  ```

- Wenn die IP-Adresse statisch ist, konfigurieren Sie die manuelle Verbindung:

  ```
  ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
  ```

5. Führen Sie den Netzboot aus.
   - Wenn es sich bei der Plattform um ein System der 80xx-Serie handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Wenn es sich bei der Plattform um ein anderes System handelt, verwenden Sie den folgenden Befehl:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Wählen Sie im Startmenü die Option **(7) Neue Software zuerst installieren** aus, um das neue Software-Image auf das Boot-Gerät herunterzuladen und zu installieren.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein
   `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie
   die URL der Bilddatei ein: `\http://web_server_ip/path_to_web-
   accessible_directory/ontap-version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Seien Sie dabei `n` So überspringen Sie die Backup-Recovery, wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Starten Sie den Neustart durch Eingabe `y` Wenn eine Eingabeaufforderung wie die folgende angezeigt wird:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

9. Wählen Sie im Startmenü die Option **Option 5**, um in den Wartungsmodus zu wechseln.

10. Wenn Sie über eine MetroCluster-Konfiguration mit vier Nodes verfügen, wiederholen Sie diesen Vorgang auf dem anderen neuen Controller-Modul.

Ermitteln Sie die System-IDs der Ersatz-Controller-Module

Nachdem Sie die gesamte Hardware am Notfallstandort ausgetauscht haben, müssen Sie die System-ID des neu installierten Storage Controller-Moduls oder -Moduls bestimmen.

Über diese Aufgabe

Sie müssen dieses Verfahren mit den Ersatz-Controller-Modulen im Wartungsmodus durchführen.

Dieser Abschnitt enthält Beispiele für Konfigurationen mit zwei und vier Nodes. Bei Konfigurationen mit zwei Nodes können Sie Verweise auf den zweiten Node an jedem Standort ignorieren. Bei Konfigurationen mit acht Nodes müssen die zusätzlichen Nodes in der zweiten DR-Gruppe berücksichtigt werden. Die Beispiele machen folgende Annahmen:

- Standort A ist der Notfallstandort.
- Node_A_1 wurde ersetzt.
- Node_A_2 wurde ersetzt.

  Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.

- Standort B ist der überlebende Standort.
- Node_B_1 ist in einem ordnungsgemäßen Zustand.
- Node_B_2 ist in einem ordnungsgemäßen Zustand.

  Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Anzahl der Knoten in der MetroCluster-Konfiguration	Knoten	Ursprüngliche System-ID	Neue System-ID	Wird mit diesem Knoten als DR-Partner gekoppelt
Vier	Node_A_1	4068741258	1574774970	Knoten_B_1
Node_A_2	4068741260	1574774991	Knoten_B_2	Knoten_B_1
4068741254	Unverändert	Node_A_1	Knoten_B_2	4068741256
Unverändert	Node_A_2	Zwei	Node_A_1	4068741258
1574774970	Knoten_B_1	Knoten_B_1	4068741254	Unverändert

In einer MetroCluster Konfiguration mit vier Nodes bestimmt das System DR-Partnerschaften, indem es den Node mit der niedrigsten System-ID bei Site_A und den Node mit der niedrigsten System-ID am Standort_B verbindet Da sich die System-IDs ändern, können sich die DR-Paare nach dem Austausch des Controllers unterscheiden, als es vor dem Ausfall der Fall war.

Im vorhergehenden Beispiel:

- Node_A_1 (1574774970) wird mit Node_B_1 (4068741254) gekoppelt
- Node_A_2 (1574774991) wird mit Node_B_2 (4068741256) gekoppelt

Schritte

1. Zeigen Sie bei dem Node im Wartungsmodus von jedem Node die lokale System-ID des Node an: `disk show`

   Im folgenden Beispiel ist die neue lokale System-ID 1574774970:

   ```
   *> disk show
    Local System ID: 1574774970
    ...
   ```

2. Wiederholen Sie auf dem zweiten Knoten den vorherigen Schritt.

   Dieser Schritt ist für eine MetroCluster Konfiguration mit zwei Nodes nicht erforderlich.

   Im folgenden Beispiel ist die neue lokale System-ID 1574774991:

   ```
   *> disk show
    Local System ID: 1574774991
    ...
   ```

Überprüfen Sie den Status der HA-Konfiguration der Komponenten

In einer MetroCluster Konfiguration muss der HA-Konfigurationszustand des Controller-Moduls und der Gehäusekomponenten auf „mcc“ oder „mcc-2n“ gesetzt werden, damit sie ordnungsgemäß hochfahren.

Bevor Sie beginnen

Das System muss sich im Wartungsmodus befinden.

Über diese Aufgabe

Diese Aufgabe muss an jedem neuen Controller-Modul ausgeführt werden.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   ```
   ha-config show
   ```

   Der richtige HA-Status hängt von Ihrer MetroCluster-Konfiguration ab.

Anzahl der Controller in der MetroCluster-Konfiguration	DER HA-Status für alle Komponenten sollte…

MetroCluster FC-Konfiguration mit acht oder vier Nodes	mcc
MetroCluster FC-Konfiguration mit zwei Nodes	mcc-2n
MetroCluster IP-Konfiguration	Mccip

2. Wenn der angezeigte Systemzustand des Controllers nicht korrekt ist, setzen Sie den HA-Status für das Controller-Modul ein:

Anzahl der Controller in der MetroCluster-Konfiguration	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify controller mcc-2n`
MetroCluster IP-Konfiguration	`ha-config modify controller mccip`

3. Wenn der angezeigte Systemzustand des Chassis nicht korrekt ist, setzen Sie den HA-Status für das Chassis ein:

Anzahl der Controller in der MetroCluster-Konfiguration	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify chassis mcc-2n`
MetroCluster IP-Konfiguration	`ha-config modify chassis mccip`

4. Wiederholen Sie diese Schritte auf dem anderen Ersatzknoten.

Stellen Sie fest, ob die End-to-End-Verschlüsselung auf den ursprünglichen Systemen aktiviert war

Sie sollten überprüfen, ob die ursprünglichen Systeme für die End-to-End-Verschlüsselung konfiguriert wurden.

Schritt

1. Führen Sie den folgenden Befehl vom verbleibenden Standort aus:

   ```
   metrocluster node show -fields is-encryption-enabled
   ```

   Wenn die Verschlüsselung aktiviert ist, wird die folgende Ausgabe angezeigt:

```
1 cluster_A node_A_1 true
1 cluster_A node_A_2 true
1 cluster_B node_B_1 true
1 cluster_B node_B_2 true
4 entries were displayed.
```

Siehe "Konfigurieren Sie die End-to-End-Verschlüsselung" Für unterstützte Systeme.

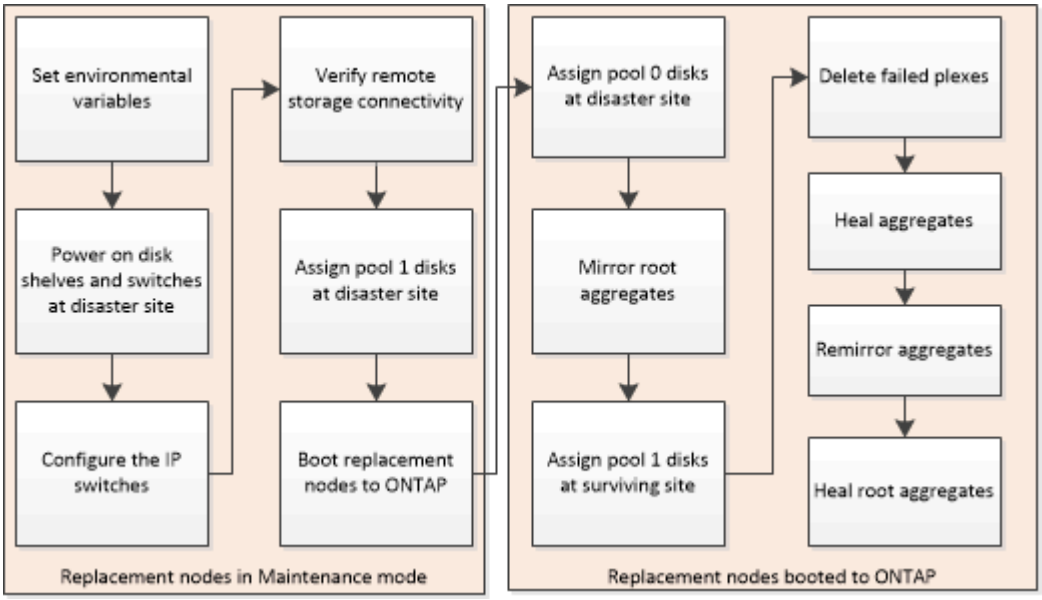
Bereiten Sie den Wechsel zurück in einer MetroCluster IP-Konfiguration vor

Bereiten Sie den Wechsel zurück in einer MetroCluster IP-Konfiguration vor

Sie müssen bestimmte Aufgaben ausführen, um die MetroCluster IP-Konfiguration für den Switchback-Betrieb vorzubereiten.

Über diese Aufgabe

Nbsp;



Festlegen der erforderlichen Umgebungsvariablen in MetroCluster IP-Konfigurationen

In MetroCluster IP-Konfigurationen müssen Sie die IP-Adresse der MetroCluster-Schnittstellen auf den Ethernet-Ports abrufen und sie dann zum Konfigurieren der Schnittstellen auf den Ersatz-Controller-Modulen verwenden.

Über diese Aufgabe

- Dieser Vorgang ist nur in MetroCluster IP-Konfigurationen erforderlich.
- Befehle in dieser Aufgabe werden über die Cluster-Eingabeaufforderung des noch intakten Standorts und über die LOADER-Eingabeaufforderung der Nodes am DR-Standort ausgeführt.
- Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig

verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

Falls unterstützt, können Sie mit dem Parameter auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben `vlan-id` .

Die folgenden Plattformen unterstützen **Not** den `vlan-id` Parameter:

- FAS8200 UND AFF A300
- AFF A320
- FAS9000 und AFF A700
- AFF C800, ASA C800, AFF A800 und ASA A800

  Alle anderen Plattformen unterstützen den `vlan-id` Parameter.

- Die Nodes in diesen Beispielen weisen die folgenden IP-Adressen für ihre MetroCluster IP-Verbindungen auf:

> Diese Beispiele gelten für ein AFF A700 oder FAS9000 System. Die Schnittstellen variieren je nach Plattformmodell.

Knoten	Port	IP-Adresse
Node_A_1	e5a	172.17.26.10
E5b	172.17.27.10	Node_A_2
e5a	172.17.26.11	E5b
172.17.27.11	Knoten_B_1	e5a
172.17.26.13	E5b	172.17.27.13
Knoten_B_2	e5a	172.17.26.12

In der folgenden Tabelle sind die Beziehungen zwischen den Nodes und den MetroCluster-IP-Adressen der einzelnen Nodes zusammengefasst.

Knoten	HA-Partner	DR-Partner	DR-Hilfspartner
Node_A_1 • e5a: 172.17.26.10 • E5b: 172.17.27.10	Node_A_2 • e5a: 172.17.26.11 • E5b: 172.17.27.11	Knoten_B_1 • e5a: 172.17.26.13 • E5b: 172.17.27.13	Knoten_B_2 • e5a: 172.17.26.12 • E5b: 172.17.27.12
Node_A_2 • e5a: 172.17.26.11 • E5b: 172.17.27.11	Node_A_1 • e5a: 172.17.26.10 • E5b: 172.17.27.10	Knoten_B_2 • e5a: 172.17.26.12 • E5b: 172.17.27.12	Knoten_B_1 • e5a: 172.17.26.13 • E5b: 172.17.27.13

Knoten_B_1 • e5a: 172.17.26.13 • E5b: 172.17.27.13	Knoten_B_2 • e5a: 172.17.26.12 • E5b: 172.17.27.12	Node_A_1 • e5a: 172.17.26.10 • E5b: 172.17.27.10	Node_A_2 • e5a: 172.17.26.11 • E5b: 172.17.27.11
Knoten_B_2 • e5a: 172.17.26.12 • E5b: 172.17.27.12	Knoten_B_1 • e5a: 172.17.26.13 • E5b: 172.17.27.13	Node_A_2 • e5a: 172.17.26.11 • E5b: 172.17.27.11	Node_A_1 • e5a: 172.17.26.10 • E5b: 172.17.27.10

- Die von Ihnen festgelegten MetroCluster Bootarg-Werte hängen davon ab, ob Ihr neues System gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet. Verwenden Sie die folgenden Informationen, um die Ports für Ihr System zu bestimmen.

Shared-Cluster-/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte Cluster-/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A20 • AFF A30 • AFF C30 • AFF A50 • AFF C60 • AFF C80 • AFF A70 • AFF A90 • AFF A1K	• FAS50 • FAS70 • FAS90

Shared-MetroCluster/HA-Ports

Die in der folgenden Tabelle aufgeführten Systeme verwenden gemeinsam genutzte MetroCluster/HA-Ports:

AFF und ASA Systeme	FAS Systeme
• AFF A150, ASA A150 • AFF A220 • AFF C250, ASA C250 • AFF A250, ASA A250 • AFF A300 • AFF A320 • AFF C400, ASA C400 • AFF A400, ASA A400 • AFF A700 • AFF C800, ASA C800 • AFF A800, ASA A800 • AFF A900, ASA A900	• FAS2750 • FAS500f • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500

Schritte

1. Holen Sie sich vom verbleibenden Standort die IP-Adressen der MetroCluster-Schnittstellen auf dem DR-Standort:

   ```
   metrocluster configuration-settings connection show
   ```

Die erforderlichen Adressen sind die DR-Partneradressen, die in der Spalte **Zielnetzwerkadresse** angezeigt werden.

Die Befehlsausgabe hängt davon ab, ob Ihr Plattformmodell gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet.

Systeme mit gemeinsam genutzten Cluster/HA-Ports

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

Systeme mit gemeinsam genutzten MetroCluster/HA-Ports

Die folgende Ausgabe zeigt die IP-Adressen für eine Konfiguration mit AFF A700 und FAS9000 Systemen mit MetroCluster IP-Schnittstellen an den Ports e5a und e5b. Die Schnittstellen können je nach Plattformtyp variieren.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
```

```
DR                      Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

2. Wenn Sie die VLAN-ID oder Gateway-Adresse für die Schnittstelle ermitteln müssen, bestimmen Sie die VLAN-IDs vom verbleibenden Standort:

   `metrocluster configuration-settings interface show`

   - Sie müssen die VLAN-ID ermitteln, wenn die Plattformmodelle VLAN-IDs unterstützen (siehe Liste oben) und wenn Sie nicht die Standard-VLAN-IDs verwenden.
   - Sie benötigen die Gateway-Adresse, wenn Sie verwenden "Layer-3-Wide-Area-Netzwerke".

     Die VLAN-IDs sind in der Spalte **Netzwerkadresse** der Ausgabe enthalten. Die Spalte **Gateway** zeigt die Gateway-IP-Adresse an.

     In diesem Beispiel sind die Schnittstellen e0a mit der VLAN-ID 120 und e0b mit der VLAN-ID 130:

```
Cluster-A::*> metrocluster configuration-settings interface show
DR
Config
Group Cluster Node     Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1
      cluster_A
              node_A_1
                  Home Port: e0a-120
                          172.17.26.10  255.255.255.0  -
completed
                  Home Port: e0b-130
                          172.17.27.10  255.255.255.0  -
completed
```

3. Legen Sie an der `LOADER` Eingabeaufforderung für jeden Disaster-Standort-Node den Bootarg-Wert fest, je nachdem, ob Ihr Plattformmodell gemeinsam genutzte Cluster/HA-Ports oder gemeinsam genutzte MetroCluster/HA-Ports verwendet:

   - Wenn die Schnittstellen die Standard-VLANs verwenden oder das Plattformmodell keine VLAN-ID verwendet (siehe Liste oben), ist die *vlan-id* nicht erforderlich.
   - Wenn die Konfiguration nicht verwendet wird "Layer3 Wide Area Networks"Der Wert für *Gateway-IP-Adresse* ist **0** (Null).

Systeme mit gemeinsam genutzten Cluster/HA-Ports

Legen Sie den folgenden Bootarg fest:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,0,0,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```

Mit den folgenden Befehlen werden die Werte für Node_A_1 unter Verwendung von VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12,130
```

Im folgenden Beispiel werden die Befehle für Node_A_1 ohne VLAN-ID angezeigt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,0,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,0,172.17.27.13,172.17.27.12
```

Systeme mit gemeinsam genutzten MetroCluster/HA-Ports

Legen Sie den folgenden Bootarg fest:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-
address,vlan-id
```

Mit den folgenden Befehlen werden die Werte für Node_A_1 unter Verwendung von VLAN 120 für das erste Netzwerk und VLAN 130 für das zweite Netzwerk festgelegt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

Im folgenden Beispiel werden die Befehle für Node_A_1 ohne VLAN-ID angezeigt:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

4. Erfassen Sie vom verbleibenden Standort aus die UUUIDs für den Katastrophenstandort:

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid

  (metrocluster node show)
dr-group-id cluster     node     node-uuid
node-cluster-uuid
----------- ----------- -------- ------------------------------------
------------------------------
1           cluster_A   node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_A   node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_B   node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098

c9e55d
1           cluster_B   node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098

c9e55d
4 entries were displayed.
cluster_A::*>
```

Knoten	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Knoten_B_1	F37b240b-9ac1-11e7-9b42-00a098c9e55d
Knoten_B_2	Bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A	E7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	F03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	Aa9a7a7a-9a81-11e7-a4e9-00a098908c35

5. Setzen Sie an DER LOADER-Eingabeaufforderung der Ersatz-Nodes die UUUIDs ein:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID`
```

a. Legen Sie die UUIDs auf Node_A_1 fest.

   Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_A_1 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f

setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Legen Sie die UUIDs auf Node_A_2 fest:

   Im folgenden Beispiel werden die Befehle zum Einstellen der UUIDs auf Node_A_2 angezeigt:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f

setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d

setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

6. Wenn die Originalsysteme für ADP konfiguriert wurden, aktivieren Sie an der LOADER-

Eingabeaufforderung der Ersatz-Nodes ADP:

```
setenv bootarg.mcc.adp_enabled true
```

7. Wenn ONTAP 9.5, 9.6 oder 9.7 an DER LOADER-Eingabeaufforderung der Ersatz-Nodes ausgeführt wird, aktivieren Sie die folgende Variable:

   ```
   setenv bootarg.mcc.lun_part true
   ```

   a. Legen Sie die Variablen auf Node_A_1 fest.

      Das folgende Beispiel zeigt die Befehle zum Einstellen der Werte auf Node_A_1, wenn ONTAP 9.6 ausgeführt wird:

      ```
      setenv bootarg.mcc.lun_part true
      ```

   b. Legen Sie die Variablen auf Node_A_2 fest.

      Das folgende Beispiel zeigt die Befehle zum Einstellen der Werte auf Node_A_2, wenn ONTAP 9.6 ausgeführt wird:

   ```
   setenv bootarg.mcc.lun_part true
   ```

8. Wenn die ursprünglichen Systeme für die End-to-End-Verschlüsselung konfiguriert waren, legen Sie an jeder LOADER-Eingabeaufforderung des Ersatz-Nodes den folgenden Bootarg fest:

   ```
   setenv bootarg.mccip.encryption_enabled 1
   ```

9. Wenn die Originalsysteme für ADP konfiguriert wurden, legen Sie an jeder LOADER-Eingabeaufforderung der Ersatzknoten die ursprüngliche System-ID (**nicht** die System-ID des Ersatzcontrollermoduls) und die System-ID des DR-Partners des Knotens fest:

   ```
   setenv bootarg.mcc.local_config_id original-sysID
   ```

   ```
   setenv bootarg.mcc.dr_partner dr_partner-sysID
   ```

   "Ermitteln Sie die System-IDs der alten Controller-Module"

   a. Legen Sie die Variablen auf Node_A_1 fest.

      Im folgenden Beispiel werden die Befehle zum Einstellen der System-IDs auf Node_A_1 angezeigt:

      - Die alte System-ID von Node_A_1 ist 4068741258.
      - Die System-ID von Node_B_1 lautet 4068741254.

      ```
      setenv bootarg.mcc.local_config_id 4068741258
      setenv bootarg.mcc.dr_partner 4068741254
      ```

   b. Legen Sie die Variablen auf Node_A_2 fest.

Im folgenden Beispiel werden die Befehle zum Einstellen der System-IDs auf Node_A_2 angezeigt:

- Die alte System-ID von Node_A_1 ist 4068741260.
- Die System-ID von Node_B_1 lautet 4068741256.

```
setenv bootarg.mcc.local_config_id 4068741260
setenv bootarg.mcc.dr_partner 4068741256
```

Einschalten des Systems am Disaster-Standort (MetroCluster IP-Konfigurationen)

Die Festplatten-Shelfs und MetroCluster IP-Switches müssen am DR-Standort eingeschaltet werden. Die Controller-Module am Disaster-Standort bleiben an der LOADER-Eingabeaufforderung.

Über diese Aufgabe

Die Beispiele in diesem Verfahren gehen davon aus, dass:

- Standort A ist der Notfallstandort.
- Standort B ist der überlebende Standort.

Schritte

1. Schalten Sie die Platten-Shelfs am Disaster Standort ein und stellen Sie sicher, dass alle Festplatten ausgeführt werden.
2. Schalten Sie die MetroCluster-IP-Switches ein, wenn sie nicht bereits aktiviert sind.

Konfiguration der IP-Switches (MetroCluster IP-Konfigurationen)

Sie müssen alle ersetzten IP-Switches konfigurieren.

Über diese Aufgabe

Diese Aufgabe bezieht sich ausschließlich auf MetroCluster IP-Konfigurationen.

Dies muss an beiden Schaltern erfolgen. Überprüfen Sie nach der Konfiguration des ersten Switches, ob der Speicherzugriff am verbleibenden Standort nicht beeinträchtigt ist.

> Sie dürfen den zweiten Switch nicht fortsetzen, wenn der Speicherzugriff auf dem noch intakten Standort beeinträchtigt ist.

Schritte

1. Siehe "MetroCluster IP Installation und Konfiguration: : Unterschiede zwischen den ONTAP MetroCluster-Konfigurationen" Für Verfahren zur Verkabelung und Konfiguration eines Ersatzschalters.

   Sie können die Verfahren in den folgenden Abschnitten verwenden:

   - Verkabeln der IP-Switches
   - Konfigurieren der IP-Switches
2. Wenn die ISLs am verbleibenden Standort deaktiviert waren, aktivieren Sie die ISLs und überprüfen Sie, ob die ISLs online sind.

a. Aktivierung der ISL-Schnittstellen am ersten Switch:

```
no shutdown
```

Die folgenden Beispiele zeigen die Befehle für einen Broadcom IP-Switch oder einen Cisco IP-Switch.

Switch-Anbieter	Befehle

Broadcom	`(IP_Switch_A_1)> enable`
	`(IP_switch_A_1)# configure`
	`(IP_switch_A_1)(Config)# interface 0/13-0/16`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# no shutdown`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# exit`
	`(IP_switch_A_1)(Config)# exit`

Cisco	`IP_switch_A_1# conf t`
	`IP_switch_A_1(config)# int eth1/15-eth1/20`
	`IP_switch_A_1(config)# no shutdown`
	`IP_switch_A_1(config)# copy running startup`
	`IP_switch_A_1(config)# show interface brief`

b. Aktivierung der ISL-Schnittstellen am Partner-Switch:

```
no shutdown
```

Die folgenden Beispiele zeigen die Befehle für einen Broadcom IP-Switch oder einen Cisco IP-Switch.

Switch-Anbieter	Befehle

Broadcom	`(IP_Switch_A_2)> enable`
	`(IP_switch_A_2)# configure`
	`(IP_switch_A_2)(Config)# interface 0/13-0/16`
	`(IP_switch_A_2)(Interface 0/13-0/16 )# no shutdown`
	`(IP_switch_A_2)(Interface 0/13-0/16 )# exit`
	`(IP_switch_A_2)(Config)# exit`

Cisco	`IP_switch_A_2# conf t`
	`IP_switch_A_2(config)# int eth1/15-eth1/20`
	`IP_switch_A_2(config)# no shutdown`
	`IP_switch_A_2(config)# copy running startup`
	`IP_switch_A_2(config)# show interface brief`

c. Vergewissern Sie sich, dass die Schnittstellen aktiviert sind:

   `show interface brief`

   Das folgende Beispiel zeigt die Ausgabe für einen Cisco Switch.

```
IP_switch_A_2(config)# show interface brief

--------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------
mt0 -- up 10.10.99.10 100 1500
--------------------------------------------------------
Ethernet    VLAN Type Mode    Status Reason Speed   Port
Interface                                           Ch
#
--------------------------------------------------------
.
.
.
Eth1/15    10   eth   access  up     none   40G(D)  --
Eth1/16    10   eth   access  up     none   40G(D)  --
Eth1/17    10   eth   access  down   none   auto(D) --
Eth1/18    10   eth   access  down   none   auto(D) --
Eth1/19    10   eth   access  down   none   auto(D) --
Eth1/20    10   eth   access  down   none   auto(D) --
.
.
.
IP_switch_A_2#
```

Überprüfen der Storage-Konnektivität zum Remote Standort (MetroCluster IP-Konfigurationen)

Sie müssen sicherstellen, dass die ersetzten Nodes mit den Festplatten-Shelfs am verbleibenden Standort verbunden sind.

Über diese Aufgabe

Diese Aufgabe wird auf den Ersatz-Nodes am Disaster-Standort ausgeführt.

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Schritte

1. Zeigt die Festplatten an, die der ursprünglichen System-ID gehören.

   ```
   disk show -s old-system-ID
   ```

   Die Remote-Datenträger können vom 0m-Gerät erkannt werden. 0m zeigt an, dass die Festplatte über die MetroCluster-iSCSI-Verbindung verbunden ist. Diese Festplatten müssen später im Wiederherstellungsverfahren neu zugewiesen werden.

```
*> disk show -s 4068741256
Local System ID: 1574774970

  DISK     OWNER                 POOL  SERIAL NUMBER   HOME
DR HOME
---------- --------------------- ----- -------------
--------------------- ----------------------
0m.i0.0L11 node_A_2 (4068741256) Pool1 S396NA0HA02128  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.1L38 node_A_2 (4068741256) Pool1 S396NA0J148778  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.0L52 node_A_2 (4068741256) Pool1 S396NA0J148777  node_A_2
(4068741256) node_A_2  (4068741256)
...
...
NOTE: Currently 49 disks are unowned. Use 'disk show -n' for additional
information.
*>
```

2. Wiederholen Sie diesen Schritt auf den anderen Ersatzknoten

Neuzuordnen der Eigentumsrechte an Pool-1-Festplatten am Disaster-Standort (MetroCluster IP-Konfigurationen)

Wenn am Disaster-Standort ein oder beide Controller-Module oder NVRAM-Karten ausgetauscht wurden, hat sich die System-ID geändert, und Sie müssen Festplatten, die zu den Root-Aggregaten gehören, den Ersatz-Controller-Modulen neu zuweisen.

Über diese Aufgabe

Da sich die Nodes im Switchover-Modus befinden, werden bei dieser Aufgabe nur die Festplatten mit den Root-Aggregaten von Pool1 des Disaster-Standorts neu zugewiesen. Sie sind derzeit die einzigen Festplatten, die noch zur alten System-ID gehören.

Diese Aufgabe wird auf den Ersatz-Nodes am Disaster-Standort ausgeführt.

Diese Aufgabe wird im Wartungsmodus ausgeführt.

Die Beispiele machen folgende Annahmen:

- Standort A ist der Notfallstandort.
- Node_A_1 wurde ersetzt.
- Node_A_2 wurde ersetzt.
- Standort B ist der überlebende Standort.
- Node_B_1 ist in einem ordnungsgemäßen Zustand.
- Node_B_2 ist in einem ordnungsgemäßen Zustand.

Die alten und neuen System-IDs wurden in identifiziert "Ersetzen Sie die Hardware und starten Sie neue

Controller".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Knoten	Ursprüngliche System-ID	Neue System-ID
Node_A_1	4068741258	1574774970
Node_A_2	4068741260	1574774991
Knoten_B_1	4068741254	Unverändert
Knoten_B_2	4068741256	Unverändert

Schritte

1. Weisen Sie beim Austausch-Node im Wartungsmodus die Root-Aggregat-Festplatten neu zu. Verwenden Sie dabei den richtigen Befehl, je nachdem, ob Ihr System mit ADP und Ihrer ONTAP-Version konfiguriert ist.

   Sie können mit der Umverteilung fortfahren, wenn Sie dazu aufgefordert werden.

Wenn das System ADP verwendet…	Verwenden Sie diesen Befehl zur Umverteilung der Festplatte…
Ja (ONTAP 9.8)	`disk reassign -s old-system-ID -d new-system-ID -r dr-partner-system-ID`
Ja (ONTAP 9.7.x und früher)	`disk reassign -s old-system-ID -d new-system-ID -p old-partner-system-ID`
Nein	`disk reassign -s old-system-ID -d new-system-ID`

   Das folgende Beispiel zeigt die Neuzuweisung von Laufwerken auf einem nicht-ADP-System:

```
*> disk reassign -s 4068741256 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537037643.
Do you want to continue (y/n)? y
disk reassign parameters: new_home_owner_id 537070473 ,
new_home_owner_name
Disk 0m.i0.3L14 will be reassigned.
Disk 0m.i0.1L6 will be reassigned.
Disk 0m.i0.1L8 will be reassigned.
Number of disks to be reassigned: 3
```

2. Löschen Sie den Inhalt der Mailbox-Platten:

   ```
   mailbox destroy local
   ```

   Sie können den Vorgang zum Zerstören fortsetzen, wenn Sie dazu aufgefordert werden.

   Im folgenden Beispiel wird die Ausgabe des Befehls „Mailbox zerstören“ für den lokalen Befehl angezeigt:

   ```
   *> mailbox destroy local
   Destroying mailboxes forces a node to create new empty mailboxes,
   which clears any takeover state, removes all knowledge
   of out-of-date plexes of mirrored volumes, and will prevent
   management services from going online in 2-node cluster
   HA configurations.
   Are you sure you want to destroy the local mailboxes? y
   ...............Mailboxes destroyed.
   *>
   ```

3. Wenn die Datenträger ausgetauscht wurden, sind lokale Plexe ausgefallen, die gelöscht werden müssen.

   a. Zeigt den Aggregatstatus an:

      ```
      aggr status
      ```

      Im folgenden Beispiel ist der Plex Node_A_1_aggr0/plex0 fehlgeschlagen.

```
*> aggr status
Aug 18 15:00:07 [node_B_1:raid.vol.mirror.degraded:ALERT]: Aggregate
node_A_1_aggr0 is
   mirrored and one plex has failed. It is no longer protected by
mirroring.
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex0
   clean(-1), online(0)
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex2
   clean(0), online(1)
Aug 18 15:00:07 [node_B_1:raid.mirror.vote.noRecord1Plex:error]:
WARNING: Only one plex
   in aggregate node_A_1_aggr0 is available. Aggregate might contain
stale data.
Aug 18 15:00:07 [node_B_1:raid.debug:info]:
volobj_mark_sb_recovery_aggrs: tree:
   node_A_1_aggr0 vol_state:1 mcc_dr_opstate: unknown
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (VOL):
   raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (MIRROR):
   raid state change UNINITD -> DEGRADED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex0
   (PLEX): raid state change UNINITD -> FAILED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2
   (PLEX): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2/rg0
   (GROUP): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Topology updated for
aggregate node_A_1_aggr0
   to plex plex2
*>
```

b. Löschen Sie den fehlgeschlagenen Plex:

```
aggr destroy plex-id
```

```
*> aggr destroy node_A_1_aggr0/plex0
```

4. Halten Sie den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   `halt`

5. Wiederholen Sie diese Schritte auf dem anderen Node am Disaster-Standort.

Booten von ONTAP bei Ersatz-Controller-Modulen in MetroCluster IP-Konfigurationen

Sie müssen die Ersatzknoten am Disaster-Standort zum Betriebssystem ONTAP booten.

Über diese Aufgabe

Dieser Task beginnt mit den Nodes am Disaster-Standort im Wartungsmodus.

Schritte

1. Beenden Sie bei einem der Ersatz-Nodes die LOADER-Eingabeaufforderung: `halt`
2. Anzeigen des Startmenüs: `boot_ontap menu`
3. Wählen Sie im Startmenü Option 6, **Flash aus Backup config aktualisieren**.

   Das System bootet zweimal. Sie sollten antworten `yes` Wenn Sie dazu aufgefordert werden, fortzufahren. Nach dem zweiten Start sollten Sie antworten `y` Wenn Sie dazu aufgefordert werden, dass die System-ID nicht stimmt.

   > Wenn Sie den NVRAM-Inhalt eines verwendeten Ersatz-Controller-Moduls nicht gelöscht haben, wird möglicherweise die folgende Panikmeldung angezeigt: `PANIC: NVRAM contents are invalid…`. Wenn dieser Fall eintritt, booten Sie das System erneut zur ONTAP-Eingabeaufforderung (`boot_ontap menu`). Dann müssen Sie es Setzen Sie die Boot_Recovery und rdb_Corrupt Bootargs zurück

   - Bestätigung zur Fortsetzung der Eingabeaufforderung:

     ```
     Selection (1-9)? 6

     This will replace all flash-based configuration with the last backup
     to
     disks. Are you sure you want to continue?: yes
     ```

   - Eingabeaufforderung für nicht übereinstimmende System-ID:

     ```
     WARNING: System ID mismatch. This usually occurs when replacing a
     boot device or NVRAM cards!
     Override system ID? {y|n} y
     ```

4. Vergewissern Sie sich vom verbleibenden Standort, dass die korrekten Partner-System-IDs auf die Nodes angewendet wurden:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

In diesem Beispiel sollten die folgenden neuen System-IDs in der Ausgabe angezeigt werden:

- Node_A_1: 1574774970
- Node_A_2: 1574774991

In der Spalte „ha-Partner-System“ sollten die neuen System-IDs angezeigt werden.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  1574774970    1574774991
4068741254         4068741256
1           Cluster_A  Node_A_2  1574774991    1574774970
4068741256         4068741254
1           Cluster_B  Node_B_1  -             -                  -
-
1           Cluster_B  Node_B_2  -             -                  -
-
4 entries were displayed.
```

5. Wenn die Partner-System-IDs nicht korrekt festgelegt wurden, müssen Sie manuell den korrekten Wert festlegen:
   a. Halten Sie die LOADER-Eingabeaufforderung am Node gedrückt und zeigen Sie sie an.
   b. Überprüfen Sie den aktuellen Wert des Partner-SYSID Bootarg:

      ```
      printenv
      ```

   c. Setzen Sie den Wert auf die richtige Partner-System-ID:

      ```
      setenv partner-sysid partner-sysID
      ```

   d. Booten des Node:

      ```
      boot_ontap
      ```

   e. Wiederholen Sie diese Unterschritte ggf. auf dem anderen Knoten.
6. Bestätigen Sie, dass die Ersatz-Nodes am Disaster-Standort für den Wechsel bereit sind:

   ```
   metrocluster node show
   ```

   Auf den Recovery-Modus für den Wechsel zum Recovery-Modus sollten die Ersatz-Nodes warten. Wenn sie sich stattdessen im normalen Modus befinden, können Sie die Ersatz-Nodes neu booten. Nach diesem Booten sollten die Nodes auf den Recovery-Modus wechseln warten.

Das folgende Beispiel zeigt, dass die Ersatz-Nodes für den Wechsel zum Rückseite bereit sind:

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

7. Überprüfen Sie die Konfigurationseinstellungen der MetroCluster-Verbindung:

   `metrocluster configuration-settings connection show`

   Der Konfigurationsstatus sollte als abgeschlossen angegeben werden.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
```

```
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_1
                 Home Port: e5a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
      cluster_A
              node_A_2
                 Home Port: e5a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e5a
                      172.17.26.11    172.17.26.12    DR Partner
completed
                 Home Port: e5a
                      172.17.26.11    172.17.26.13    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.12    DR Partner
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.13    DR Auxiliary
completed
```

```
               node_A_1
                  Home Port: e5a
                       172.17.26.10    172.17.26.11    HA Partner
completed
                  Home Port: e5a
                       172.17.26.10    172.17.26.13    DR Partner
completed
                  Home Port: e5a
                       172.17.26.10    172.17.26.12    DR Auxiliary
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.11    HA Partner
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.13    DR Partner
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.12    DR Auxiliary
completed
24 entries were displayed.

cluster_B::*>
```

8. Wiederholen Sie die vorherigen Schritte auf dem anderen Knoten am Disaster-Standort.

Reset the Boot_Recovery and rdb_corrupte Bootargs

Falls erforderlich, können Sie die Boot_Recovery und rdb_Corrupt_bootargs zurücksetzen

Schritte

1. Halten Sie den Node wieder an die LOADER-Eingabeaufforderung an:

```
node_A_1::*> halt -node _node-name_
```

2. Überprüfen Sie, ob die folgenden Bootargs eingestellt sind:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Wenn eine der Bootarg auf einen Wert gesetzt wurde, heben Sie die Einstellung auf und starten Sie die ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Wiederherstellen der Konnektivität von den noch intakten Nodes zum Disaster-Standort (MetroCluster IP-Konfigurationen)

Sie müssen die MetroCluster-iSCSI-Initiator-Verbindungen von den noch intakten Nodes wiederherstellen.

Über diese Aufgabe

Dieses Verfahren ist nur bei MetroCluster IP-Konfigurationen erforderlich.

Schritte

1. Ändern Sie von der Eingabeaufforderung eines verbleibenden Node auf die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

   Sie müssen mit reagieren `y` Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*) anzuzeigen.

2. Verbinden Sie die iSCSI-Initiatoren auf beiden noch intakten Nodes in der DR-Gruppe:

   ```
   storage iscsi-initiator connect -node surviving-node -label *
   ```

   Im folgenden Beispiel werden die Befehle zum Verbinden der Initiatoren auf Standort B angezeigt:

   ```
   site_B::*> storage iscsi-initiator connect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator connect -node node_B_2 -label *
   ```

3. Zurück zur Administratorberechtigungsebene:

   ```
   set -privilege admin
   ```

Überprüfen der automatischen Zuweisung oder manuelles Zuweisen von Pool 0-Laufwerken

Bei Systemen, die für ADP konfiguriert sind, müssen Sie überprüfen, ob Pool-0-Laufwerke automatisch zugewiesen wurden. Bei Systemen, die nicht für ADP konfiguriert sind, müssen Sie die Laufwerke Pool 0 manuell zuweisen.

Überprüfen der Laufwerkszuweisung von Pool 0-Laufwerken auf ADP-Systemen am DR-Standort (MetroCluster IP-Systeme)

Wenn Laufwerke am Disaster-Standort ausgetauscht wurden und das System für ADP konfiguriert ist, müssen Sie überprüfen, ob die Remote-Laufwerke für die Nodes sichtbar und korrekt zugewiesen wurden.

Schritt

1. Vergewissern Sie sich, dass Pool-0-Laufwerke automatisch zugewiesen werden:

   ```
   disk show
   ```

   Im folgenden Beispiel für ein AFF A800 System ohne externe Shelfs wurde ein Quartal (8 Laufwerke) automatisch Node_A_1 zugewiesen, und ein Quartal wurde Node_A_2 automatisch zugewiesen. Die verbleibenden Laufwerke sind Remote-Laufwerke (Pool1) für Node_B_1 und Node_B_2.

   ```
   cluster_A::*> disk show
                   Usable     Disk      Container           Container
   Disk            Size       Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
   node_A_2
   ```

```
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Zuweisen von Pool-0-Laufwerken an nicht-ADP-Systemen am Disaster-Standort (MetroCluster-IP-Konfigurationen)

Wenn Laufwerke am Disaster-Standort ausgetauscht wurden und das System nicht für ADP konfiguriert ist, müssen Sie dem Pool 0 manuell neue Laufwerke zuweisen.

Über diese Aufgabe

Bei ADP-Systemen werden die Laufwerke automatisch zugewiesen.

Schritte

1. Weisen Sie bei einem der Ersatz-Nodes am Disaster-Standort den Pool 0-Laufwerken des Node neu zu:

   ```
   storage disk assign -n number-of-replacement disks -p 0
   ```

   Dieser Befehl weist die neu hinzugefügten (und nicht im Besitz befindlichen) Laufwerke am Disaster-Standort zu. Sie sollten dieselbe Anzahl und Größe (oder größer) von Laufwerken zuweisen, die der Node vor dem Notfall hatte. Der `storage disk assign` Die man-Page enthält weitere Informationen zum Durchführen einer granulareren Laufwerkszuweisung.

2. Wiederholen Sie den Schritt auf dem anderen Ersatz-Node am Disaster-Standort.

Zuweisen von Pool 1-Laufwerken am verbleibenden Standort (MetroCluster-IP-Konfigurationen)

Wenn Laufwerke am Disaster-Standort ausgetauscht wurden und das System nicht für ADP konfiguriert ist, müssen am verbleibenden Standort manuell Remote-Laufwerke am DR-Standort dem Pool 1 des verbleibenden Nodes zugewiesen werden. Sie müssen die Anzahl der zuzuordnenden Laufwerke angeben.

Über diese Aufgabe

Bei ADP-Systemen werden die Laufwerke automatisch zugewiesen.

Schritt

1. Weisen Sie am verbleibenden Standort dem Pool 1-Laufwerk (Remote-Laufwerke) des ersten Node zu:
   `storage disk assign -n number-of-replacement disks -p 1 0m*`

   Dieser Befehl weist die neu hinzugefügten und nicht im Besitz befindlichen Laufwerke am Disaster-Standort zu.

   Mit dem folgenden Befehl werden 22 Laufwerke zugewiesen:

   ```
   cluster_B::> storage disk assign -n 22 -p 1 0m*
   ```

Löschen ausgefallener Plexe, die sich im Eigentum des noch intakten Standorts befinden (MetroCluster IP-Konfigurationen)

Nachdem die Hardware ersetzt und Festplatten zugewiesen wurden, müssen ausgefallene Remote-Plexe gelöscht werden, die sich im Eigentum der noch verbleibenden Site befinden, sich jedoch am DR-Standort.

Über diese Aufgabe

Diese Schritte werden auf dem noch intakten Cluster durchgeführt.

Schritte

1. Ermitteln Sie die lokalen Aggregate:
   `storage aggregate show -is-home true`

   ```
   cluster_B::> storage aggregate show -is-home true

   cluster_B Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_B_1_aggr0 1.49TB  74.12GB 95% online       1 node_B_1
   raid4,

   mirror

   degraded
   node_B_2_aggr0 1.49TB  74.12GB 95% online       1 node_B_2
   raid4,

   mirror

   degraded
   node_B_1_aggr1 2.99TB  2.88TB   3% online      15 node_B_1
   raid_dp,
   ```

```
mirror

degraded
node_B_1_aggr2 2.99TB  2.91TB   3% online      14 node_B_1
raid_tec,

mirror

degraded
node_B_2_aggr1 2.95TB  2.80TB   5% online      37 node_B_2
raid_dp,

mirror

degraded
node_B_2_aggr2 2.99TB  2.87TB   4% online      35 node_B_2
raid_tec,

mirror

degraded
6 entries were displayed.

cluster_B::>
```

2. Identifizieren der fehlerhaften Remote-Plexe:

   ```
   storage aggregate plex show
   ```

   Im folgenden Beispiel werden die Plexe aufruft, die Remote sind (nicht plex0) und den Status „Fehlgeschlagen“ aufweisen:

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_1_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr2 plex0 normal,active true     0
node_B_1_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr2 plex0 normal,active true     0
node_B_2_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
20 entries were displayed.

cluster_B::>
```

3. Versetzen Sie jede der ausgefallenen Plexe in den Offline-Modus und löschen Sie sie anschließend:

   a. Versetzen Sie die ausgefallenen Plexe in den Offline-Modus:

      `storage aggregate plex offline -aggregate aggregate-name -plex plex-id`

      Das folgende Beispiel zeigt, dass das Aggregat „Node_B_2_aggr1/plex1“ offline geschaltet wird:

      ```
      cluster_B::> storage aggregate plex offline -aggregate node_B_1_aggr0
      -plex plex4

      Plex offline successful on plex: node_B_1_aggr0/plex4
      ```

   b. Löschen Sie den fehlgeschlagenen Plex:

      `storage aggregate plex delete -aggregate aggregate-name -plex plex-id`

      Sie können den Plex zerstören, wenn Sie dazu aufgefordert werden.

Das folgende Beispiel zeigt, dass der Plex Node_B_2_aggr1/plex1 gelöscht wird.

```
cluster_B::> storage aggregate plex delete -aggregate  node_B_1_aggr0
-plex plex4

Warning: Aggregate "node_B_1_aggr0" is being used for the local
management root
         volume or HA partner management root volume, or has been
marked as
         the aggregate to be used for the management root volume
after a
         reboot operation. Deleting plex "plex4" for this aggregate
could lead
         to unavailability of the root volume after a disaster
recovery
         procedure. Use the "storage aggregate show -fields
         has-mroot,has-partner-mroot,root" command to view such
aggregates.

Warning: Deleting plex "plex4" of mirrored aggregate "node_B_1_aggr0"
on node
         "node_B_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you
want to
         destroy this plex? {y|n}: y
[Job 633] Job succeeded: DONE

cluster_B::>
```

Sie müssen diese Schritte für jede der fehlgeschlagenen Plexe wiederholen.

4. Überprüfen Sie, ob die Plexe entfernt wurden:

   ```
   storage aggregate plex show -fields aggregate,status,is-online,plex,pool
   ```

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

5. Ermitteln Sie die Switched-over-Aggregate:

   `storage aggregate show -is-home false`

   Sie können auch die verwenden `storage aggregate plex show -fields aggregate,status,is-online,plex,pool` Befehl zur Identifizierung von Plex 0 Switched-over-Aggregaten. Sie haben den Status „Fehlgeschlagen, inaktiv“.

   Die folgenden Befehle zeigen vier Umschaltaggregate:

   - Node_A_1_aggr1
   - Node_A_1_aggr2
   - Node_A_2_aggr1
   - Node_A_2_aggr2

```
cluster_B::> storage aggregate show -is-home false

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.12TB  1.88TB   11% online      91 node_B_1
raid_dp,

mirror

degraded
node_A_1_aggr2 2.89TB  2.64TB    9% online      90 node_B_1
raid_tec,

mirror

degraded
node_A_2_aggr1 2.12TB  1.86TB   12% online      91 node_B_2
raid_dp,

mirror

degraded
node_A_2_aggr2 2.89TB  2.64TB    9% online      90 node_B_2
raid_tec,

mirror

degraded
4 entries were displayed.

cluster_B::>
```

6. Identifizierung vermittelter Plexe:

   `storage aggregate plex show -fields aggregate,status,is-online,Plex,pool`

   Sie möchten die Plexe mit dem Status „Fehlgeschlagen, inaktiv“ identifizieren.

   Die folgenden Befehle zeigen vier Umschaltaggregate:

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

7. Löschen Sie den fehlgeschlagenen Plex:

   ```
   storage aggregate plex delete -aggregate node_A_1_aggr1 -plex plex0
   ```

   Sie können den Plex zerstören, wenn Sie dazu aufgefordert werden.

   Das folgende Beispiel zeigt, dass der Plex Node_A_1_aggr1/plex0 gelöscht wird:

```
cluster_B::> storage aggregate plex delete -aggregate node_A_1_aggr1
-plex plex0

Warning: Aggregate "node_A_1_aggr1" hosts MetroCluster metadata volume
         "MDV_CRS_e8457659b8a711e78b3b00a0988fe74b_A". Deleting plex
"plex0"
         for this aggregate can lead to the failure of configuration
         replication across the two DR sites. Use the "volume show
-vserver
         <admin-vserver> -volume MDV_CRS*" command to verify the
location of
         such volumes.

Warning: Deleting plex "plex0" of mirrored aggregate "node_A_1_aggr1" on
node
         "node_A_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you want
to
         destroy this plex? {y|n}: y
[Job 639] Job succeeded: DONE

cluster_B::>
```

Sie müssen diese Schritte für jeden der ausgefallenen Aggregate wiederholen.

8. Vergewissern Sie sich, dass keine fehlerhaften Plexe auf dem verbleibenden Standort vorhanden sind.

   Die folgende Ausgabe zeigt, dass alle Plexe normal, aktiv und online sind.

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex1 normal,active true     1
10 entries were displayed.

cluster_B::>
```

Durchführen der Aggregatheilung und Wiederherstellung von Spiegelungen (MetroCluster IP Konfigurationen)

Nach dem Austausch der Hardware und der Zuweisung von Festplatten können Sie in Systemen mit ONTAP 9.5 oder einer älteren Version die MetroCluster-Heilvorgänge durchführen. In allen Versionen von ONTAP müssen Sie überprüfen, ob die Aggregate gespiegelt wurden und, falls erforderlich, die Spiegelung neu starten.

Über diese Aufgabe

Ab ONTAP 9.6 werden die Heilungsvorgänge automatisch ausgeführt, wenn die Disaster-Site-Nodes gestartet werden. Die Heilbefehle sind nicht erforderlich.

Diese Schritte werden auf dem noch intakten Cluster durchgeführt.

Schritte

1. Wenn Sie ONTAP 9.6 oder höher verwenden, müssen Sie überprüfen, ob die automatische Heilung erfolgreich abgeschlossen wurde:

   a. Bestätigen Sie, dass die Vorgänge „Heal-aggr-Auto“ und „Heal-root-aggr-Auto“ abgeschlossen sind:

      ```
      metrocluster operation history show
      ```

      In der folgenden Ausgabe wird gezeigt, dass die Vorgänge auf „Cluster_A“ erfolgreich abgeschlossen wurden

```
cluster_B::*> metrocluster operation history show
Operation                     State          Start Time       End
Time
----------------------------- -------------- ----------------
----------------
heal-root-aggr-auto           successful      2/25/2019 06:45:58

2/25/2019 06:46:02
heal-aggr-auto                successful     2/25/2019 06:45:48

2/25/2019 06:45:52
.
.
.
```

b. Bestätigen Sie, dass der Notfallstandort für den Wechsel bereit ist:

```
metrocluster node show
```

In der folgenden Ausgabe wird gezeigt, dass die Vorgänge auf „Cluster_A“ erfolgreich abgeschlossen wurden

```
cluster_B::*> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- ------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1      configured     enabled   heal roots
completed
              node_A_2      configured     enabled   heal roots
completed
      cluster_B
              node_B_1      configured     enabled   waiting for
switchback recovery
              node_B_2      configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Wenn Sie ONTAP 9.5 oder früher verwenden, müssen Sie die Aggregatheilung durchführen:

a. Überprüfen Sie den Status der Nodes:

```
metrocluster node show
```

Die folgende Ausgabe zeigt, dass die Umschaltung abgeschlossen wurde, sodass eine Heilung

durchgeführt werden kann.

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

b. Durchführen der Aggregationskorrektur:

```
metrocluster heal -phase aggregates
```

Die folgende Ausgabe zeigt einen typischen Heilungsvorgang für Aggregate.

```
cluster_B::*> metrocluster heal -phase aggregates
[Job 647] Job succeeded: Heal Aggregates is successful.

cluster_B::*> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 10/26/2017 12:01:15
   End Time: 10/26/2017 12:01:17
     Errors: -

cluster_B::*>
```

c. Vergewissern Sie sich, dass die Aggregatheilung abgeschlossen und der Notfallstandort bereit für den Wechsel ist:

```
metrocluster node show
```

Die folgende Ausgabe zeigt, dass die Phase „Heal Aggregates“ auf „Cluster_A“ abgeschlossen ist

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1          configured     enabled   heal
aggregates completed
              node_A_2          configured     enabled   heal
aggregates completed
      cluster_B
              node_B_1          configured     enabled   waiting for
switchback recovery
              node_B_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

3. Wenn Festplatten ausgetauscht wurden, müssen die lokalen und Switched-over-Aggregate gespiegelt werden:

   a. Anzeigen der Aggregate:

      `storage aggregate show`

```
cluster_B::> storage aggregate show
cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

normal
node_B_1_aggr1 3.14TB  3.04TB    3% online     15 node_B_1
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.06TB    3% online     14 node_B_1
```

```
raid_tec,

normal
node_B_1_aggr1 3.14TB  2.99TB    5% online     37 node_B_2
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.02TB    4% online     35 node_B_2
raid_tec,

normal

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.36TB  2.12TB   10% online     91 node_B_1
raid_dp,

normal
node_A_1_aggr2 3.14TB  2.90TB    8% online     90 node_B_1
raid_tec,

normal
node_A_2_aggr1 2.36TB  2.10TB   11% online     91 node_B_2
raid_dp,

normal
node_A_2_aggr2 3.14TB  2.89TB    8% online     90 node_B_2
raid_tec,

normal
12 entries were displayed.

cluster_B::>
```

b. Spiegelung des Aggregats:

```
storage aggregate mirror -aggregate aggregate-name
```

Die folgende Ausgabe zeigt einen typischen Spiegelungsvorgang.

```
cluster_B::> storage aggregate mirror -aggregate node_B_1_aggr1

Info: Disks would be added to aggregate "node_B_1_aggr1" on node
"node_B_1" in
      the following manner:

      Second Plex

        RAID Group rg0, 6 disks (block checksum, raid_dp)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          dparity    5.20.6                    SSD
-
          parity     5.20.14                   SSD
-
          data       5.21.1                    SSD
894.0GB
          data       5.21.3                    SSD
894.0GB
          data       5.22.3                    SSD
894.0GB
          data       5.21.13                   SSD
894.0GB

      Aggregate capacity available for volume use would be 2.99TB.

Do you want to continue? {y|n}: y
```

c. Wiederholen Sie den vorherigen Schritt für jedes Aggregat vom verbleibenden Standort.
d. Warten Sie, bis die Aggregate sich neu synchronisiert haben, Sie können den Status mit dem überprüfen `storage aggregate show` Befehl.

   Die folgende Ausgabe zeigt, dass sich mehrere Aggregate neu synchronisieren.

```
cluster_B::> storage aggregate show

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,
```

```
mirrored,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

mirrored,

normal
node_B_1_aggr1 2.86TB  2.76TB    4% online     15 node_B_1
raid_dp,

resyncing
node_B_1_aggr2 2.89TB  2.81TB    3% online     14 node_B_1
raid_tec,

resyncing
node_B_2_aggr1 2.73TB  2.58TB    6% online     37 node_B_2
raid_dp,

resyncing
node_B-2_aggr2 2.83TB  2.71TB    4% online     35 node_B_2
raid_tec,

resyncing

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 1.86TB  1.62TB   13% online     91 node_B_1
raid_dp,

resyncing
node_A_1_aggr2 2.58TB  2.33TB   10% online     90 node_B_1
raid_tec,

resyncing
node_A_2_aggr1 1.79TB  1.53TB   14% online     91 node_B_2
raid_dp,

resyncing
node_A_2_aggr2 2.64TB  2.39TB    9% online     90 node_B_2
raid_tec,
```

```
resyncing
12 entries were displayed.
```

e. Vergewissern Sie sich, dass alle Aggregate online sind und erneut synchronisiert wurden:

```
storage aggregate plex show
```

Die folgende Ausgabe zeigt, dass alle Aggregate erneut synchronisiert wurden.

```
cluster_A::> storage aggregate plex show
  ()
                    Is      Is         Resyncing
Aggregate Plex      Online  Resyncing    Percent Status
--------- --------- ------- ---------- --------- ---------------
node_B_1_aggr0 plex0 true    false              - normal,active
node_B_1_aggr0 plex8 true    false              - normal,active
node_B_2_aggr0 plex0 true    false              - normal,active
node_B_2_aggr0 plex8 true    false              - normal,active
node_B_1_aggr1 plex0 true    false              - normal,active
node_B_1_aggr1 plex9 true    false              - normal,active
node_B_1_aggr2 plex0 true    false              - normal,active
node_B_1_aggr2 plex5 true    false              - normal,active
node_B_2_aggr1 plex0 true    false              - normal,active
node_B_2_aggr1 plex9 true    false              - normal,active
node_B_2_aggr2 plex0 true    false              - normal,active
node_B_2_aggr2 plex5 true    false              - normal,active
node_A_1_aggr1 plex4 true    false              - normal,active
node_A_1_aggr1 plex8 true    false              - normal,active
node_A_1_aggr2 plex1 true    false              - normal,active
node_A_1_aggr2 plex5 true    false              - normal,active
node_A_2_aggr1 plex4 true    false              - normal,active
node_A_2_aggr1 plex8 true    false              - normal,active
node_A_2_aggr2 plex1 true    false              - normal,active
node_A_2_aggr2 plex5 true    false              - normal,active
20 entries were displayed.
```

4. Führen Sie auf Systemen mit ONTAP 9.5 und früheren Versionen die Phase der Heilung von Root-Aggregaten durch:

```
metrocluster heal -phase root-aggregates
```

```
cluster_B::> metrocluster heal -phase root-aggregates
[Job 651] Job is queued: MetroCluster Heal Root Aggregates Job.Oct 26
13:05:00
[Job 651] Job succeeded: Heal Root Aggregates is successful.
```

5. Vergewissern Sie sich, dass die Phase „Wurzeln heilen“ abgeschlossen ist und der Notfallstandort für den Wechsel bereit ist:

   Die folgende Ausgabe zeigt, dass die Phase „Heal Roots“ auf Cluster_A abgeschlossen ist

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal roots
completed
              node_A_2           configured     enabled   heal roots
completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

Fahren Sie fort, um die Lizenzen auf den ersetzten Nodes zu überprüfen.

"Überprüfung der Lizenzen auf den ersetzten Nodes"

Bereiten Sie sich auf den Wechsel zurück in einer MetroCluster FC-Konfiguration vor

Überprüfen der Portkonfiguration (nur MetroCluster FC-Konfigurationen)

Sie müssen die Umgebungsvariablen auf dem Node festlegen und dann deaktivieren, um die MetroCluster Konfiguration vorzubereiten.

Über diese Aufgabe

Dieses Verfahren wird bei den Ersatz-Controller-Modulen im Wartungsmodus durchgeführt.

Die Schritte zum Prüfen der Konfiguration der Ports sind nur auf Systemen erforderlich, auf denen FC- oder CNA-Ports im Initiator-Modus verwendet werden.

Schritte

1. Stellen Sie im Wartungsmodus die FC-Port-Konfiguration wieder her:

   ```
   ucadmin modify -m fc -t initiatoradapter_name
   ```

   Wenn Sie in der Initiator-Konfiguration nur eines der Portpaare verwenden möchten, geben Sie einen genauen Adapternamen ein.

2. Führen Sie je nach Konfiguration eine der folgenden Aktionen durch:

Wenn die Konfiguration des FC-Ports…	Dann…
Das gleiche für beide Ports	Beantworten Sie „`y`“, wenn Sie vom System dazu aufgefordert werden, da durch das Ändern eines Ports in einem Portpaar auch der andere Port geändert wird.
Anders	a. Beantworten Sie „`n`“, wenn Sie vom System dazu aufgefordert werden. b. Wiederherstellen der Konfiguration des FC-Ports: `ucadmin modify -m fc -t initiator

3. Beenden des Wartungsmodus:

   ```
   halt
   ```

   Nachdem Sie den Befehl ausgegeben haben, warten Sie, bis das System an der LOADER-Eingabeaufforderung angehalten wird.

4. Starten Sie den Node wieder in den Wartungsmodus, damit die Konfigurationsänderungen wirksam werden:

   ```
   boot_ontap maint
   ```

5. Überprüfen Sie die Werte der Variablen:

   ```
   ucadmin show
   ```

6. Beenden Sie den Wartungsmodus und zeigen Sie die LOADER-Eingabeaufforderung an:

   ```
   halt
   ```

Konfiguration der FC-to-SAS-Bridges (nur MetroCluster FC-Konfigurationen)

Wenn Sie die Bridges für FC-to-SAS ersetzt haben, müssen Sie sie beim Wiederherstellen der MetroCluster-Konfiguration konfigurieren. Das Verfahren entspricht der Erstkonfiguration einer FC-to-SAS-Bridge.

Schritte

1. Schalten Sie die FC-to-SAS-Bridges ein.
2. Legen Sie die IP-Adresse an den Ethernet-Ports mithilfe des fest `set IPAddress port ipaddress` Befehl.
   - `port` Kann entweder „MP1“ oder „MP2“ sein.
   - `ipaddress` Kann eine IP-Adresse im Format xxx.xxx.xxx.xxx sein.

     Im folgenden Beispiel ist die IP-Adresse 10.10.10.55 am Ethernet-Port 1:

```
Ready.
set IPAddress MP1 10.10.10.55

Ready. *
```

3. Stellen Sie die IP-Subnetzmaske an den Ethernet-Ports mithilfe des ein `set IPSubnetMask port mask` Befehl.
   - `port` Kann „MP1“ oder „MP2“ sein.
   - `mask` Kann eine Subnetzmaske im Format xxx.xxx.xxx.xxx.xxx sein.

     Im folgenden Beispiel ist die IP-Subnetzmaske 255.255.255.0 auf Ethernet-Port 1:

```
Ready.
set IPSubnetMask MP1 255.255.255.0

Ready. *
```

4. Stellen Sie die Geschwindigkeit an den Ethernet-Ports mithilfe des ein `set EthernetSpeed port speed` Befehl.
   - `port` Kann „MP1“ oder „MP2“ sein.
   - `speed` Kann „100“ oder „1000“ lauten.

     Im folgenden Beispiel ist die Ethernet-Geschwindigkeit auf 1000 am Ethernet-Port 1 eingestellt.

```
Ready.
set EthernetSpeed MP1 1000

Ready. *
```

5. Speichern Sie die Konfiguration mit dem `saveConfiguration` Führen Sie einen Befehl aus, und starten Sie die Bridge neu, wenn Sie dazu aufgefordert werden.

   Wenn Sie die Konfiguration nach der Konfiguration der Ethernet-Ports speichern, können Sie mit der Bridge-Konfiguration über Telnet fortfahren und über FTP auf die Bridge zugreifen, um Firmware-Updates

durchzuführen.

Das folgende Beispiel zeigt die `saveConfiguration` Befehl und Eingabeaufforderung zum Neustart der Bridge.

```
Ready.
SaveConfiguration
  Restart is necessary....
  Do you wish to restart (y/n) ?
Confirm with 'y'. The bridge will save and restart with the new
settings.
```

6. Nachdem die FC-to-SAS-Bridge neu gebootet wurde, melden Sie sich erneut an.
7. Legen Sie die Geschwindigkeit auf den FC-Ports mit dem fest `set fcdatarate port speed` Befehl.
   - `port` Kann „1“ oder „2“ sein.
   - `speed` Je nach Modellbrücke können Sie entweder „2 GB“, „4 GB“, „8 GB“ oder „16 GB“ wählen.

     Im folgenden Beispiel wird die Port-FC1-Geschwindigkeit auf „8 GB“ eingestellt.

```
Ready.
set fcdatarate 1 8Gb

Ready. *
```

8. Legen Sie die Topologie auf den FC-Ports mit dem fest `set FCConnMode port mode` Befehl.
   - `port` Kann „1“ oder „2“ sein.
   - `mode` Kann „ptp“, „Loop“, „ptp-Loop“ oder „Auto“ sein.

     Im folgenden Beispiel wird die Port-FC1-Topologie auf „ptp“ gesetzt.

```
Ready.
set FCConnMode 1 ptp

Ready. *
```

9. Speichern Sie die Konfiguration mit dem `saveConfiguration` Führen Sie einen Befehl aus, und starten Sie die Bridge neu, wenn Sie dazu aufgefordert werden.

   Das folgende Beispiel zeigt die `saveConfiguration` Befehl und Eingabeaufforderung zum Neustart der Bridge.

```
 Ready.
 SaveConfiguration
    Restart is necessary....
    Do you wish to restart (y/n) ?
 Confirm with 'y'. The bridge will save and restart with the new
settings.
```

10. Nachdem die FC-to-SAS-Bridge neu gebootet wurde, melden Sie sich erneut an.
11. Wenn auf der FC-to-SAS-Bridge Firmware 1.60 oder höher ausgeführt wird, aktivieren Sie SNMP.

```
Ready.
set snmp enabled

Ready. *
saveconfiguration

Restart is necessary....
Do you wish to restart (y/n) ?

Verify with 'y' to restart the FibreBridge.
```

12. Schalten Sie die FC-to-SAS-Bridges aus.

Konfiguration der FC-Switches (nur MetroCluster FC-Konfigurationen)

Wenn Sie die FC-Switches am Disaster-Standort ersetzt haben, müssen Sie diese anhand anbieterspezifischer Verfahren konfigurieren. Sie müssen einen Switch konfigurieren, überprüfen, ob der Speicherzugriff am verbleibenden Standort nicht beeinträchtigt ist, und dann den zweiten Switch konfigurieren.

Verwandte Aufgaben

"Portzuweisungen für FC-Switches"

Konfigurieren eines Brocade FC-Switch nach dem Standortausfall

Verwenden Sie dieses Brocade spezifische Verfahren, um den Ersatz-Switch zu konfigurieren und die ISL-Ports zu aktivieren.

Über diese Aufgabe

Die Beispiele in diesem Verfahren basieren auf folgenden Annahmen:

- Standort A ist der Notfallstandort.
- FC_Switch_A_1 wurde ersetzt.
- FC_Switch_A_2 wurde ersetzt.
- Standort B ist der überlebende Standort.

- FC_Switch_B_1 ist in einem ordnungsgemäßen Zustand.
- FC_Switch_B_2 ist in einem ordnungsgemäßen Zustand.

Sie müssen überprüfen, ob Sie die angegebenen Portzuweisungen verwenden, wenn Sie die FC-Switches verkabeln:

- "Portzuweisungen für FC-Switches"

Die Beispiele zeigen zwei FC-to-SAS-Bridges. Wenn Sie mehr Brücken haben, müssen Sie die zusätzlichen Ports deaktivieren und anschließend aktivieren.

Schritte

1. Starten und Vorkonfigurieren des neuen Switch:

   a. Schalten Sie den neuen Schalter ein, und lassen Sie ihn starten.

   b. Überprüfen Sie die Firmware-Version auf dem Switch, um sicherzustellen, dass sie mit der Version der anderen FC-Switches übereinstimmt:

   `firmwareShow`

   c. Konfigurieren Sie den neuen Switch, wie in den folgenden Themen beschrieben, und überspringen Sie die Schritte zur Konfiguration des Zoning auf dem Switch.

   "Installation und Konfiguration von Fabric-Attached MetroCluster"

   "Installation und Konfiguration von Stretch MetroCluster"

   d. Deaktivieren Sie den Switch dauerhaft:

   `switchcfgpersistentdisable`

   Der Schalter bleibt nach einem Neustart oder Fastboot deaktiviert. Wenn dieser Befehl nicht verfügbar ist, sollten Sie den verwenden `switchdisable` Befehl.

   Im folgenden Beispiel wird der Befehl auf BrocadeSwitchA angezeigt:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   Im folgenden Beispiel wird der Befehl auf BrocadeSwitchB angezeigt:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

2. Vollständige Konfiguration des neuen Switch:

   a. Aktivieren Sie die ISLs auf dem verbleibenden Standort:

   `portcfgpersistentenable port-number`

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

b. Aktivieren Sie die ISLs auf den Ersatz-Switches:

   `portcfgpersistentenable port-number`

```
FC_switch_A_1:admin> portcfgpersistentenable 10
FC_switch_A_1:admin> portcfgpersistentenable 11
```

c. Stellen Sie auf dem Ersatzschalter (in diesem Beispiel FC_Switch_A_1) sicher, dass die ISL-Server online sind:

   `switchshow`

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1" (downstream)
...
```

3. Dauerhaft aktivieren Sie den Switch:

   `switchcfgpersistentenable`

4. Vergewissern Sie sich, dass die Ports online sind:

   `switchshow`

Konfiguration eines Cisco FC Switch nach Standortausfall

Zur Konfiguration des Ersatz-Switches und zur Aktivierung der ISL-Ports muss das Cisco spezifische Verfahren verwendet werden.

Über diese Aufgabe

Die Beispiele in diesem Verfahren basieren auf folgenden Annahmen:

- Standort A ist der Notfallstandort.
- FC_Switch_A_1 wurde ersetzt.
- FC_Switch_A_2 wurde ersetzt.
- Standort B ist der überlebende Standort.
- FC_Switch_B_1 ist in einem ordnungsgemäßen Zustand.
- FC_Switch_B_2 ist in einem ordnungsgemäßen Zustand.

Schritte

1. Konfigurieren des Switches:
   a. Siehe "Installation und Konfiguration von Fabric-Attached MetroCluster"
   b. Befolgen Sie die Schritte zur Konfiguration des Switch in "Konfigurieren von Cisco FC-Switches" Abschnitt „ *außer*“ für den Abschnitt „Zoning auf einem Cisco FC Switch konfigurieren“:

      Das Zoning wird später in diesem Verfahren konfiguriert.

2. Aktivieren Sie auf dem gesunden Switch (in diesem Beispiel FC_Switch_B_1) die ISL-Ports.

   Im folgenden Beispiel werden die Befehle zur Aktivierung der Ports angezeigt:

   ```
   FC_switch_B_1# conf t
   FC_switch_B_1(config)# int fc1/14-15
   FC_switch_B_1(config)# no shut
   FC_switch_B_1(config)# end
   FC_switch_B_1# copy running-config startup-config
   FC_switch_B_1#
   ```

3. Vergewissern Sie sich, dass die ISL-Ports mit dem Befehl show Interface Brief verfügbar sind.
4. Rufen Sie die Zoning-Informationen von der Fabric ab.

   Im folgenden Beispiel werden die Befehle zur Verteilung der Zoning-Konfiguration angezeigt:

   ```
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 10
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 20
   FC_switch_B_1(config-zone)# end
   ```

   FC_Switch_B_1 wird auf alle anderen Switches im Fabric für „vsan 10“ und „vsan 20“ verteilt, und die Zoning-Informationen werden von FC_Switch_A_1 abgerufen.

5. Überprüfen Sie beim ordnungsgemäßen Switch, ob die Zoning-Informationen vom Partner-Switch abgerufen werden:

   `show zone`

   ```
   FC_switch_B_1# show zone
   zone name FC-VI_Zone_1_10 vsan 10
     interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

   zone name STOR_Zone_1_20_25A vsan 20
     interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

   zone name STOR_Zone_1_20_25B vsan 20
     interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
     interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
     interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
   FC_switch_B_1#
   ```

6. Ermitteln Sie die weltweiten Namen (WWNs) der Switches in der Switch Fabric.

   In diesem Beispiel sind die beiden Switch-WWNs:

   - FC_Switch_A_1: 20:00:54:7f:ee:b8:24:c0
   - FC_Switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

7. Konfigurationsmodus für die Zone eingeben und Zonenmitglieder entfernen, die nicht zu den Switch-WWNs der beiden Switches gehören:

   `no member interface interface-ide swwn wwn`

   In diesem Beispiel sind die folgenden Mitglieder nicht mit dem WWN eines der Switches in der Fabric verknüpft und müssen entfernt werden:

   - Zonenname FC-VI_Zone_1_10 vsan 10
     - Schnittstelle fc1/1, gestreut 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/2 geschwibelt 20:00:54:7f:ee:e3:86:50

     > AFF Systeme A700 und FAS9000 unterstützen vier FC-VI-Ports. Sie müssen alle vier Ports aus der FC-VI-Zone entfernen.

   - Zonenname STOR_Zone_1_20_25A vsan 20
     - Schnittstelle fc1/5 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/8 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/9 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/10 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/11 geschwibelt 20:00:54:7f:ee:e3:86:50
   - Zonenname STOR_Zone_1_20_25B vsan 20
     - Schnittstelle fc1/8 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/9 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/10 geschwibelt 20:00:54:7f:ee:e3:86:50
     - Schnittstelle fc1/11 geschwibelt 20:00:54:7f:ee:e3:86:50

   Das folgende Beispiel zeigt das Entfernen dieser Schnittstellen:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

8. Fügen Sie die Ports des neuen Schalters zu den Zonen hinzu.

   Im folgenden Beispiel wird vorausgesetzt, dass die Verkabelung am Ersatzschalter mit dem alten Switch identisch ist:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

9. Überprüfen Sie, ob das Zoning ordnungsgemäß konfiguriert ist: `show zone`

   Die Ausgabe des folgenden Beispiels zeigt die drei Zonen:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

Überprüfen der Speicherkonfiguration

Es muss sichergestellt werden, dass der gesamte Storage von den verbleibenden Nodes aus sichtbar ist.

Schritte

1. Vergewissern Sie sich, dass alle Storage-Komponenten am Notfallstandort gleich sind in Menge und Typ am verbleibenden Standort.

   Am verbleibenden Standort und am DR-Standort sollte die gleiche Anzahl an Festplatten-Shelf-Stacks, Platten-Shelfs und Festplatten verwendet werden. In einer MetroCluster-Konfiguration mit Bridge- oder Fabric-Attached Storage sollten die Standorte über die gleiche Anzahl von FC-to-SAS-Bridges verfügen.

2. Vergewissern Sie sich, dass alle Festplatten, die am Disaster-Standort ausgetauscht wurden, im Besitz sind:

```
run local disk show-n
```

Festplatten sollten als nicht-Eigentümer angezeigt werden.

3. Wenn keine Festplatten ausgetauscht wurden, vergewissern Sie sich, dass alle Festplatten vorhanden sind:

```
disk show
```

Einschalten des Systems am Disaster-Standort

Wenn die Vorbereitung auf den Wechsel zum Back bereit ist, müssen die MetroCluster Komponenten am Disaster-Standort eingeschaltet werden. Zusätzlich müssen Sie die SAS-Storage-Verbindungen auch in Direct-Attached MetroCluster-Konfigurationen reaktivieren und in Fabric-Attached MetroCluster-Konfigurationen-Ports unterstützen, die nicht zwischen Switches liegen.

Bevor Sie beginnen

Sie müssen die MetroCluster-Komponenten bereits genau wie die alten ersetzt und verkabelt haben.

"Installation und Konfiguration von Fabric-Attached MetroCluster"

"Installation und Konfiguration von Stretch MetroCluster"

Über diese Aufgabe

Die Beispiele in diesem Verfahren gehen davon aus, dass:

- Standort A ist der Notfallstandort.
  - FC_Switch_A_1 wurde ersetzt.
  - FC_Switch_A_2 wurde ersetzt.
- Standort B ist der überlebende Standort.
  - FC_Switch_B_1 ist in einem ordnungsgemäßen Zustand.
  - FC_Switch_B_2 ist in einem ordnungsgemäßen Zustand.

Die FC-Switches sind nur in Fabric-Attached MetroCluster-Konfigurationen verfügbar.

Schritte

1. Bei Stretch-MetroCluster-Konfiguration über SAS-Verkabelung (und keine FC Switch Fabric- oder FC-to-SAS-Bridges) verbinden Sie den gesamten Storage einschließlich des Remote-Storage über beide Standorte hinweg.

   Der Controller am Disaster-Standort muss ausgeschaltet bleiben oder an DER LOADER-Eingabeaufforderung angezeigt werden.

2. Deaktivieren Sie auf dem verbleibenden Standort die automatische Festplattenzuordnung:

```
storage disk option modify -autoassign off *
```

```
cluster_B::> storage disk option modify -autoassign off *
2 entries were modified.
```

3. Vergewissern Sie sich am verbleibenden Standort, dass die automatische Festplattenzuordnung aus ist:

   `storage disk option show`

```
cluster_B::> storage disk option show
Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          off             default
node_B_2       on            on          off             default
2 entries were displayed.

 cluster_B::>
```

4. Schalten Sie die Platten-Shelfs am Disaster Standort ein und stellen Sie sicher, dass alle Festplatten ausgeführt werden.
5. Aktivieren Sie in einer MetroCluster Konfiguration mit Bridge- oder Fabric-Attached Storage alle FC-to-SAS-Bridges am DR-Standort.
6. Wenn Festplatten ausgetauscht wurden, lassen Sie die Controller ausgeschaltet oder an DER LOADER-Eingabeaufforderung.
7. Aktivieren Sie in einer Fabric-Attached MetroCluster-Konfiguration die nicht-ISL-Ports auf den FC-Switches.

Wenn der Switch-Anbieter…	Verwenden Sie anschließend diese Schritte, um die Ports zu aktivieren…

Brocade	a. Dauerhaft die Ports aktivieren, die mit den FC-to-SAS-Bridges verbunden sind: `portpersistentenable port-number`
	
	Im folgenden Beispiel sind die Ports 6 und 7 aktiviert:
	
	`FC_switch_A_1:admin> portpersistentenable 6`
	`FC_switch_A_1:admin> portpersistentenable 7`
	
	`FC_switch_A_1:admin>`
	
	b. Dauerhaft aktivieren Sie die Ports, die mit den HBAs und FC-VI-Adaptern verbunden sind: `portpersistentenable port-number`
	
	Im folgenden Beispiel sind die Ports 6 und 7 aktiviert:
	
	`FC_switch_A_1:admin> portpersistentenable 1`
	`FC_switch_A_1:admin> portpersistentenable 2`
	`FC_switch_A_1:admin> portpersistentenable 4`
	`FC_switch_A_1:admin> portpersistentenable 5`
	`FC_switch_A_1:admin>`
	
	Bei AFF A700 und FAS9000 Systemen müssen Sie alle vier FC-VI-Ports mithilfe des Befehls switchcfgpersistent enable dauerhaft aktivieren.
	
	c. Wiederholen Sie die Teilschritte A und b für den zweiten FC-Switch am noch verbleibenden Standort.

Cisco	a. Wechseln Sie in den Konfigurationsmodus für die Schnittstelle, und aktivieren Sie dann die Ports mit dem Befehl „no shut“.
	
	Im folgenden Beispiel ist Port fc1/36 deaktiviert:
	
	`FC_switch_A_1# conf t`
	`FC_switch_A_1(config)#`
	`interface fc1/36`
	`FC_switch_A_1(config)# no shut`
	`FC_switch_A_1(config-if)# end`
	`FC_switch_A_1# copy running-`
	`config startup-config`
	
	b. Vergewissern Sie sich, dass der Switch-Port aktiviert ist: `show interface brief`
	
	c. Wiederholen Sie die Subschritte A und b auf den anderen Ports, die mit den FC-to-SAS-Bridges, HBAs und FC-VI-Adaptern verbunden sind.
	
	d. Wiederholen Sie die Teilschritte A, b und c für den zweiten FC-Switch am verbleibenden Standort.

Eigentümerschaft für ausgetauschte Laufwerke zuweisen

Wenn Laufwerke beim Wiederherstellen von Hardware am Disaster-Standort ausgetauscht oder Laufwerke gar nicht benötigt werden, müssen die betroffenen Laufwerke Eigentum zugewiesen werden.

Bevor Sie beginnen

Der Disaster-Standort muss über mindestens so viele Laufwerke verfügen wie vor der Katastrophe.

Die Anordnung der Platten-Shelves und Laufwerke muss die Anforderungen in erfüllen "Erforderliche MetroCluster IP-Komponente und Namenskonventionen" Des Abschnitts "Installation und Konfiguration von MetroCluster IP".

Über diese Aufgabe

Diese Schritte werden für das Cluster am Disaster-Standort durchgeführt.

Dieses Verfahren zeigt die Neuzuweisung aller Laufwerke und die Erstellung neuer Plexe am Disaster-Standort. Die neuen Plexe sind Remote-Plexe des verbleibenden Standorts und der lokalen Plexe eines Notfallstandorts.

Dieser Abschnitt enthält Beispiele für Konfigurationen mit zwei und vier Nodes. Bei Konfigurationen mit zwei Nodes können Sie Verweise auf den zweiten Node an jedem Standort ignorieren. Bei Konfigurationen mit acht Nodes müssen die zusätzlichen Nodes in der zweiten DR-Gruppe berücksichtigt werden. Die Beispiele machen folgende Annahmen:

- Standort A ist der Notfallstandort.
  - Node_A_1 wurde ersetzt.
  - Node_A_2 wurde ersetzt.

    Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.
- Standort B ist der überlebende Standort.
  - Node_B_1 ist in einem ordnungsgemäßen Zustand.
  - Node_B_2 ist in einem ordnungsgemäßen Zustand.

    Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.

Die Controller-Module verfügen über die folgenden ursprünglichen System-IDs:

Anzahl der Knoten in der MetroCluster-Konfiguration	Knoten	Ursprüngliche System-ID
Vier	Node_A_1	4068741258
Node_A_2	4068741260	Knoten_B_1
4068741254	Knoten_B_2	4068741256
Zwei	Node_A_1	4068741258

Beim Zuweisen der Laufwerke sollten Sie folgende Punkte beachten:

- Die Anzahl der alten Festplatten muss für jeden Node mindestens die gleiche Anzahl an Festplatten aufweisen, die vor dem Ausfall vorhanden waren.

  Wenn eine niedrigere Anzahl von Festplatten angegeben oder vorhanden ist, werden die Heilungsvorgänge aufgrund des unzureichenden Speicherplatzes möglicherweise nicht abgeschlossen.
- Die zu erstellenden neuen Plexe sind Remote-Plexe, die zum verbleibenden Standort (Node_B_x Pool1) und lokale Plexe gehören, die zum Notfallstandort (Node_B_x Pool0) gehören.
- Die Gesamtzahl der benötigten Laufwerke sollte nicht die Root-Aggr-Festplatten enthalten.

  Wenn n Disketten Pool1 der überlebenden Seite zugewiesen werden, dann sollten n-3 Disketten der Disaster Site zugewiesen werden mit der Annahme, dass das Root-Aggregat drei Festplatten verwendet.
- Keine der Festplatten kann einem Pool zugewiesen werden, der sich von dem der unterscheidet, dem alle anderen Festplatten im selben Stapel zugewiesen sind.
- Festplatten, die zum verbleibenden Standort gehören, werden Pool 1 zugewiesen, Festplatten, die zum Disaster-Standort gehören, werden Pool 0 zugewiesen.

Schritte

1. Weisen Sie die neuen Laufwerke ohne Besitzer zu, unabhängig davon, ob Sie über eine MetroCluster Konfiguration mit vier oder zwei Nodes verfügen:

- Weisen Sie bei MetroCluster-Konfigurationen mit vier Nodes den entsprechenden Festplatten-Pools die neuen, nicht im Besitz befindlichen Festplatten zu, indem Sie die folgenden Befehle auf den Ersatz-Nodes verwenden:

  i. Weisen Sie die ersetzten Festplatten für jeden Knoten systematisch ihren jeweiligen Disk-Pools zu:

     ```
     disk assign -s sysid -n old-count-of-disks -p pool
     ```

     Sie geben am verbleibenden Standort einen Befehl zur Festplattenzuordnung für jeden Node aus:

     ```
     cluster_B::> disk assign -s node_B_1-sysid -n old-count-of-disks
     -p 1 **\(remote pool of surviving site\)**
     cluster_B::> disk assign -s node_B_2-sysid -n old-count-of-disks
     -p 1 **\(remote pool of surviving site\)**
     cluster_B::> disk assign -s node_A_1-old-sysid -n old-count-of-
     disks -p 0 **\(local pool of disaster site\)**
     cluster_B::> disk assign -s node_A_2-old-sysid -n old-count-of-
     disks -p 0 **\(local pool of disaster site\)**
     ```

     Im folgenden Beispiel werden die Befehle mit den System-IDs angezeigt:

```
cluster_B::> disk assign -s 4068741254 -n 21 -p 1
cluster_B::> disk assign -s 4068741256 -n 21 -p 1
cluster_B::> disk assign -s 4068741258 -n 21 -p 0
cluster_B::> disk assign -s 4068741260 -n 21 -p 0
```

  i. Bestätigen Sie den Besitz der Festplatten:

     ```
     storage disk show -fields owner, pool
     ```

```
storage disk show -fields owner, pool
cluster_A::> storage disk show -fields owner, pool
disk     owner          pool
-------- ------------- -----
0c.00.1  node_A_1      Pool0
0c.00.2  node_A_1      Pool0
.
.
.
0c.00.8  node_A_1      Pool1
0c.00.9  node_A_1      Pool1
.
.
.
0c.00.15 node_A_2      Pool0
0c.00.16 node_A_2      Pool0
.
.
.
0c.00.22 node_A_2      Pool1
0c.00.23 node_A_2      Pool1
.
.
.
```

- Weisen Sie bei MetroCluster-Konfigurationen mit zwei Nodes den entsprechenden Festplatten-Pools die neuen, nicht im Besitz befindlichen Festplatten zu. Verwenden Sie dazu die folgenden Befehle auf dem Ersatzknoten:
  i. Zeigen Sie die lokalen Shelf-IDs an:

     ```
     run local storage show shelf
     ```

  ii. Weisen Sie die ersetzten Festplatten für den gesunden Node Pool 1 zu:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 1 -s
     node_B_1-sysid -f
     ```

  iii. Weisen Sie die ersetzten Festplatten für den Ersatzknoten Pool 0 zu:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 0 -s
     node_A_1-sysid -f
     ```

2. Schalten Sie am verbleibenden Standort die automatische Festplattenzuordnung erneut ein:

   ```
   storage disk option modify -autoassign on *
   ```

```
cluster_B::> storage disk option modify -autoassign on *
2 entries were modified.
```

3. Bestätigen Sie am verbleibenden Standort, dass die automatische Festplattenzuordnung auf ist:

   `storage disk option show`

```
 cluster_B::> storage disk option show
 Node      BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          on              default
node_B_2       on            on          on              default
2 entries were displayed.

 cluster_B::>
```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

"MetroCluster-Konfigurationen nutzen SyncMirror zur Bereitstellung von Datenredundanz"

Durchführen der Aggregatheilung und Wiederherstellung von Spiegelungen (MetroCluster FC-Konfigurationen)

Nach dem Ersetzen der Hardware und dem Zuweisen von Festplatten können Sie die MetroCluster-Heilvorgänge durchführen. Es muss bestätigt werden, dass die Aggregate gespiegelt wurden und, falls erforderlich, die Spiegelung neu starten.

Schritte

1. Führen Sie die beiden Heilungsphasen (Aggregatheilung und Wurzelheilung) am Notfallstandort durch:

```
cluster_B::> metrocluster heal -phase aggregates

cluster_B::> metrocluster heal -phase root-aggregates
```

2. Überwachen Sie die Reparatur und überprüfen Sie, ob sich die Aggregate entweder im resynchronisiert oder gespiegelten Status befinden:

   `storage aggregate show -node local`

Wenn das Aggregat diesen Status zeigt…	Dann…
Resynchronisierung	Es ist keine Aktion erforderlich. Lassen Sie das Aggregat die Resynchronisierung abschließen.

Spiegelung beeinträchtigt	Fahren Sie mit fort Wenn ein oder mehrere Plexe offline bleiben, sind zum Rebuild des Spiegels zusätzliche Schritte erforderlich.
Gespiegelt, normal	Es ist keine Aktion erforderlich.
Unbekannt, offline	Das Root-Aggregat zeigt diesen Status an, wenn alle Festplatten der Disaster-Sites ersetzt wurden.

```
cluster_B::> storage aggregate show -node local

 Aggregate     Size Available Used% State   #Vols  Nodes      RAID
Status
 --------- -------- --------- ----- ------- ------ ----------
------------
 node_B_1_aggr1
           227.1GB   11.00GB   95% online       1 node_B_1   raid_dp,
                                                              resyncing
 NodeA_1_aggr2
           430.3GB   28.02GB   93% online       2 node_B_1   raid_dp,
                                                              mirror
                                                              degraded
 node_B_1_aggr3
           812.8GB   85.37GB   89% online       5 node_B_1   raid_dp,
                                                              mirrored,
                                                              normal
 3 entries were displayed.

cluster_B::>
```

In den folgenden Beispielen besitzen die drei Aggregate einen anderen Status:

Knoten	Status
Node_B_1_aggr1	Resynchronisierung
Node_B_1_aggr2	Spiegelung beeinträchtigt
Node_B_1_aggr3	Gespiegelt, normal

3. Wenn ein oder mehrere Plexe offline bleiben, sind zusätzliche Schritte erforderlich, um die Spiegelung wiederherzustellen.

   In der vorherigen Tabelle muss die Spiegelung für Node_B_1_aggr2 neu erstellt werden.

a. Zeigen Sie Details zum Aggregat an, um fehlerhafte Plexe zu identifizieren:

```
storage aggregate show -r -aggregate node_B_1_aggr2
```

Im folgenden Beispiel befindet sich Plex /Node_B_1_aggr2/plex0 in einem fehlgeschlagenen Zustand:

```
cluster_B::> storage aggregate show -r -aggregate node_B_1_aggr2

 Owner Node: node_B_1
  Aggregate: node_B_1_aggr2 (online, raid_dp, mirror degraded) (block
checksums)
   Plex: /node_B_1_aggr2/plex0 (offline, failed, inactive, pool0)
    RAID Group /node_B_1_aggr2/plex0/rg0 (partial)
                                                                    Usable
Physical
      Position Disk                      Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------

   Plex: /node_B_1_aggr2/plex1 (online, normal, active, pool1)
    RAID Group /node_B_1_aggr2/plex1/rg0 (normal, block checksums)
                                                                    Usable
Physical
      Position Disk                      Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------
      dparity  1.44.8                     1   SAS    15000  265.6GB
273.5GB (normal)
      parity   1.41.11                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.42.8                     1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.11                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.44.9                     1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.18                    1   SAS    15000  265.6GB
273.5GB (normal)
 6 entries were displayed.

 cluster_B::>
```

a. Löschen Sie den fehlgeschlagenen Plex:

```
storage aggregate plex delete -aggregate aggregate-name -plex plex
```

b. Wiederherstellung der Spiegelung:

```
storage aggregate mirror -aggregate aggregate-name
```

c. Überwachen Sie die Resynchronisierung und den Spiegelungsstatus der Plex, bis alle Spiegel wiederhergestellt sind und alle Aggregate den gespiegelten, normalen Status anzeigen:

```
storage aggregate show
```

Neuzuweisung der Eigentumsrechte an den Root-Aggregaten an Ersatz-Controller-Modulen (MetroCluster FC-Konfigurationen)

Wenn am Disaster-Standort ein oder beide Controller-Module oder NVRAM-Karten ausgetauscht wurden, hat sich die System-ID geändert, und Sie müssen Festplatten, die zu den Root-Aggregaten gehören, den Ersatz-Controller-Modulen neu zuweisen.

Über diese Aufgabe

Da sich die Nodes im Umschaltmodus befinden und die Reparatur durchgeführt wurde, werden in diesem Abschnitt nur die Festplatten mit den Root-Aggregaten von Pool 1 des Disaster Site neu zugewiesen. Sie sind derzeit die einzigen Festplatten, die noch zur alten System-ID gehören.

Dieser Abschnitt enthält Beispiele für Konfigurationen mit zwei und vier Nodes. Bei Konfigurationen mit zwei Nodes können Sie Verweise auf den zweiten Node an jedem Standort ignorieren. Bei Konfigurationen mit acht Nodes müssen die zusätzlichen Nodes in der zweiten DR-Gruppe berücksichtigt werden. Die Beispiele machen folgende Annahmen:

- Standort A ist der Notfallstandort.
  - Node_A_1 wurde ersetzt.
  - Node_A_2 wurde ersetzt.

    Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.
- Standort B ist der überlebende Standort.
  - Node_B_1 ist in einem ordnungsgemäßen Zustand.
  - Node_B_2 ist in einem ordnungsgemäßen Zustand.

    Nur in MetroCluster Konfigurationen mit vier Nodes vorhanden.

Die alten und neuen System-IDs wurden in identifiziert "Ersetzen Sie die Hardware und starten Sie neue Controller".

Die Beispiele in diesem Verfahren verwenden Controller mit den folgenden System-IDs:

Anzahl der Nodes	Knoten	Ursprüngliche System-ID	Neue System-ID

Vier	Node_A_1	4068741258	1574774970
	Node_A_2	4068741260	1574774991
	Knoten_B_1	4068741254	Unverändert
	Knoten_B_2	4068741256	Unverändert
Zwei	Node_A_1	4068741258	1574774970

Schritte

1. Weisen Sie beim Ersatzknoten im Wartungsmodus die Root-Aggregat-Festplatten neu zu:

   ```
   disk reassign -s old-system-ID -d new-system-ID
   ```

   ```
   *> disk reassign -s 4068741258 -d 1574774970
   ```

2. Sehen Sie sich die Festplatten an, um die Eigentümeränderung der Pool1 Root-Aggr-Festplatten der Disaster Site zum Ersatzknoten zu bestätigen:

   ```
   disk show
   ```

   Die Ausgabe kann mehr oder weniger Festplatten anzeigen, je nachdem, wie viele Festplatten sich im Root-Aggregat befinden und ob eine dieser Festplatten ausgefallen ist und ersetzt wurde. Wenn die Festplatten ausgetauscht wurden, werden Pool0-Laufwerke nicht in der Ausgabe angezeigt.

   Die Pool1 Root-Aggregat-Platten des Disaster-Standortes sollten nun dem Ersatz-Node zugewiesen werden.

```
*> disk show
Local System ID: 1574774970

  DISK             OWNER                POOL   SERIAL NUMBER   HOME
DR HOME
------------       -------------        -----  -------------
-------------       -------------
sw_A_1:6.126L19    node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L3     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L7     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_B_1:6.126L8     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L24    node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L2     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)

*> aggr status
         Aggr State           Status
 node_A_1_root online          raid_dp, aggr
                               mirror degraded
                               64-bit
*>
```

3. Aggregatstatus anzeigen:

   ```
   aggr status
   ```

   Die Ausgabe kann mehr oder weniger Festplatten anzeigen, je nachdem, wie viele Festplatten sich im Root-Aggregat befinden und ob eine dieser Festplatten ausgefallen ist und ersetzt wurde. Wenn Disketten ersetzt wurden, werden Pool0-Platten nicht in der Ausgabe angezeigt.

   ```
   *> aggr status
            Aggr State           Status
     node_A_1_root online          raid_dp, aggr
                                   mirror degraded
                                   64-bit
   *>
   ```

4. Löschen Sie den Inhalt der Mailbox-Platten:

   ```
   mailbox destroy local
   ```

5. Wenn das Aggregat nicht online ist, bringen Sie es online:

   ```
   aggr online aggr_name
   ```

6. Halten Sie den Node an, um die LOADER-Eingabeaufforderung anzuzeigen:

   ```
   halt
   ```

Booten der neuen Controller-Module (MetroCluster FC-Konfigurationen)

Nachdem die Aggregatreparatur sowohl für die Daten als auch die Root-Aggregate abgeschlossen wurde, müssen Sie den Node oder die Nodes am Disaster-Standort booten.

Über diese Aufgabe

Diese Aufgabe beginnt mit den Nodes, in denen die LOADER-Eingabeaufforderung angezeigt wird.

Schritte

1. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

2. [[Step 2,Schritt 2]] im Startmenü Option 6 auswählen **Flash von Backup config aktualisieren**.
3. Antworten `y` An die folgende Eingabeaufforderung:

   ```
   This will replace all flash-based configuration with the last backup to disks.
   Are you sure you want to continue?: y
   ```

   Das System startet zweimal, das zweite Mal, um die neue Konfiguration zu laden.

   > Wenn Sie den NVRAM-Inhalt eines verwendeten Ersatz-Controllers nicht gelöscht haben, wird möglicherweise ein Panikzustand mit der folgenden Meldung angezeigt: `PANIC: NVRAM contents are invalid…`Wenn dies der Fall ist, wiederholen Wählen Sie im Startmenü Option 6, **Flash aus Backup config aktualisieren**. Um das System an der ONTAP-Eingabeaufforderung zu booten. Dann müssen Sie es Setzen Sie die Boot Recovery und rdb_Corrupt Bootargs zurück

4. Root-Aggregat auf Plex 0 spiegeln:
   a. Weisen Sie dem neuen Controller-Modul drei Pool0 Disks zu.
   b. Root-Aggregat-Pool1 Plex spiegeln:

      ```
      aggr mirror root-aggr-name
      ```

   c. Weisen Sie Pool0 auf dem lokalen Knoten nicht eigene Festplatten zu
5. Wenn Sie eine Konfiguration mit vier Nodes haben, wiederholen Sie die vorherigen Schritte auf dem anderen Node am Disaster-Standort.
6. Aktualisieren Sie die MetroCluster-Konfiguration:
   a. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

b. Aktualisieren Sie die Konfiguration:

```
metrocluster configure -refresh true
```

c. Zurück zum Admin-Berechtigungsmodus:

```
set -privilege admin
```

7. Bestätigen Sie, dass die Ersatz-Nodes am Disaster-Standort für den Wechsel bereit sind:

```
metrocluster node show
```

Die Ersatz-Nodes sollten sich im Modus „`Warten auf Wiederherstellung beim Wechsel`“ befinden. Wenn sich diese im Modus „`Normal`“ befinden, können Sie die Ersatz-Nodes neu booten. Nach diesem Booten sollten sich die Nodes im Modus „`Warten auf zurückwechseln Recovery`“ befinden.

Das folgende Beispiel zeigt, dass die Ersatz-Nodes für den Wechsel zum Rückseite bereit sind:

```
cluster_B::> metrocluster node show
DR                    Configuration  DR
Grp Cluster Node      State          Mirroring Mode
--- ------- --------- -------------- --------- --------------------
1   cluster_B
            node_B_1  configured     enabled   switchover completed
            node_B_2  configured     enabled   switchover completed
    cluster_A
            node_A_1  configured     enabled   waiting for switchback
recovery
            node_A_2  configured     enabled   waiting for switchback
recovery
4 entries were displayed.

cluster_B::>
```

Nächste Schritte

Fahren Sie mit fort "Den Disaster Recovery-Prozess abschließen".

Reset the Boot_Recovery and rdb_corrupte Bootargs

Falls erforderlich, können Sie die Boot_Recovery und rdb_Corrupt_bootargs zurücksetzen

Schritte

1. Halten Sie den Node wieder an die LOADER-Eingabeaufforderung an:

```
node_A_1::*> halt -node _node-name_
```

2. Überprüfen Sie, ob die folgenden Bootargs eingestellt sind:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Wenn eine der Bootarg auf einen Wert gesetzt wurde, heben Sie die Einstellung auf und starten Sie die ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Vorbereitung auf den Wechsel zurück in einer heterogenen Konfiguration (Recovery während des Übergangs)

Sie müssen bestimmte Aufgaben durchführen, um die gemischte MetroCluster IP- und FC-Konfiguration für den Switchback-Betrieb vorzubereiten. Dieses Verfahren gilt nur für Konfigurationen, bei denen während der Migration von MetroCluster FC zu IP ein Fehler aufgetreten ist.

Über diese Aufgabe

Dieses Verfahren sollte nur verwendet werden, wenn eine Wiederherstellung auf einem System durchgeführt wird, das sich während des Ausfalls Mitte des Übergangs befand.

In diesem Szenario ist die MetroCluster eine gemischte Konfiguration:

- Eine DR-Gruppe besteht aus Fabric-Attached MetroCluster-FC-Knoten.

  Auf diesen Nodes müssen Sie die MetroCluster-FC-Recovery-Schritte durchführen.

- Eine DR-Gruppe besteht aus MetroCluster IP Knoten.

  Auf diesen Knoten müssen Sie die MetroCluster IP-Recovery-Schritte durchführen.

Schritte

Führen Sie die Schritte in der folgenden Reihenfolge aus.

1. Bereiten Sie die FC-Nodes auf den Wechsel vor, indem Sie die folgenden Aufgaben in der Reihenfolge durchführen:
   a. "Überprüfen der Portkonfiguration (nur MetroCluster FC-Konfigurationen)"
   b. "Konfiguration der FC-to-SAS-Bridges (nur MetroCluster FC-Konfigurationen)"

c. "Konfiguration der FC-Switches (nur MetroCluster FC-Konfigurationen)"

d. "Überprüfen der Speicherkonfiguration" (Führen Sie nur diese Schritte auf ersetzten Laufwerken auf den MetroCluster FC Nodes durch.)

e. "Einschalten des Systems am Disaster-Standort" (Führen Sie nur diese Schritte auf ersetzten Laufwerken auf den MetroCluster FC Nodes durch.)

f. "Eigentümerschaft für ausgetauschte Laufwerke zuweisen" (Führen Sie nur diese Schritte auf ersetzten Laufwerken auf den MetroCluster FC Nodes durch.)

g. Führen Sie die Schritte unter aus "Neuzuweisung der Eigentumsrechte an den Root-Aggregaten an Ersatz-Controller-Modulen (MetroCluster FC-Konfigurationen)", Bis und einschließlich des Schritts, um den Befehl zum Löschen der Mailbox auszulösen.

h. Zerstören Sie den lokalen Plex (Plex 0) des Root-Aggregats:

```
aggr destroy plex-id
```

i. Wenn das Root-Aggregat nicht online ist, bringen Sie es online.

2. Booten der MetroCluster FC-Knoten

Sie müssen diese Schritte auf beiden MetroCluster FC Nodes durchführen.

a. Anzeigen des Startmenüs:

```
boot_ontap menu
```

b. Wählen Sie im Startmenü Option 6, **Flash aus Backup config aktualisieren**.

c. Antworten `y` An die folgende Eingabeaufforderung:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?: y
```

Das System startet zweimal, das zweite Mal, um die neue Konfiguration zu laden.

> Wenn Sie den NVRAM-Inhalt eines verwendeten Ersatz-Controllers nicht gelöscht haben, wird möglicherweise ein Panikzustand mit der folgenden Meldung angezeigt: `PANIC: NVRAM contents are invalid…` Wenn dies der Fall ist, wiederholen Sie diese Teilschritte, um das System an der ONTAP-Eingabeaufforderung zu booten. Dann müssen Sie es Setzen Sie die Boot Recovery und rdb_Corrupt Bootargs zurück

3. Root-Aggregat auf Plex 0 spiegeln:

Sie müssen diese Schritte auf beiden MetroCluster FC Nodes durchführen.

a. Weisen Sie dem neuen Controller-Modul drei Pool0 Disks zu.

b. Root-Aggregat-Pool1 Plex spiegeln:

```
aggr mirror root-aggr-name
```

c. Weisen Sie Pool0 auf dem lokalen Knoten nicht eigene Festplatten zu

4. Zurück zum Wartungsmodus.

Sie müssen diese Schritte auf beiden MetroCluster FC Nodes durchführen.

a. Stoppen Sie den Knoten:

```
halt
```

b. Booten des Node zu Maintenance:

```
mode:boot_ontap maint
```

5. Löschen Sie den Inhalt der Mailbox-Platten:

```
mailbox destroy local
```

Sie müssen diese Schritte auf beiden MetroCluster FC Nodes durchführen.

6. Stoppen Sie die Knoten:
```
halt
```
7. Überprüfen Sie nach dem Booten der Nodes den Status des Node:

```
metrocluster node show
```

```
siteA::*> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     siteA
              wmc66-a1          configured     enabled   waiting for
switchback recovery
              wmc66-a2          configured     enabled   waiting for
switchback recovery
      siteB
              wmc66-b1          configured     enabled   switchover
completed
              wmc66-b2          configured     enabled   switchover
completed
2     siteA
              wmc55-a1          -              -         -
              wmc55-a2          unreachable    -         -
      siteB
              wmc55-b1          configured     enabled   switchover
completed
              wmc55-b2          configured
```

8. Bereiten Sie die MetroCluster-IP-Nodes für den Wechsel vor, indem Sie die Aufgaben in ausführen "Vorbereitung für den Wechsel zurück in einer MetroCluster IP-Konfiguration" Bis einschließlich "Löschen ausgefallener Plexe, die sich im Eigentum des noch intakten Standorts befinden (MetroCluster IP-Konfigurationen)".

9. Führen Sie auf den MetroCluster FC-Knoten die Schritte unter aus "Durchführen der Aggregatheilung und Wiederherstellung von Spiegelungen (MetroCluster FC-Konfigurationen)".
10. Führen Sie auf den MetroCluster IP-Knoten die Schritte unter aus "Durchführen der Aggregatheilung und Wiederherstellung von Spiegelungen (MetroCluster IP Konfigurationen)".
11. Führen Sie die restlichen Aufgaben des Wiederherstellungsprozesses ab "Wiederherstellung von Objektspeichern für FabricPool-Konfigurationen".

Reset the Boot_Recovery and rdb_corrupte Bootargs

Falls erforderlich, können Sie die Boot_Recovery und rdb_Corrupt_bootargs zurücksetzen

Schritte

1. Halten Sie den Node wieder an die LOADER-Eingabeaufforderung an:

```
node_A_1::*> halt -node _node-name_
```

2. Überprüfen Sie, ob die folgenden Bootargs eingestellt sind:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Wenn eine der Bootarg auf einen Wert gesetzt wurde, heben Sie die Einstellung auf und starten Sie die ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Wiederherstellung abgeschlossen

Führen Sie die erforderlichen Aufgaben aus, um die Wiederherstellung nach einem Ausfall mehrerer Controller oder Speicher abzuschließen.

Wiederherstellung von Objektspeichern für FabricPool-Konfigurationen

Wenn einer der Objektspeicher in einer FabricPool Spiegelung sich gemeinsam mit dem Disaster-Standort MetroCluster befand und zerstört wurde, müssen Sie den Objektspeicher und die FabricPool Spiegelung wiederherstellen.

Über diese Aufgabe

- Wenn die Objektspeicher über einen Remote-Standort und ein MetroCluster Standort zerstört werden, müssen Sie den Objektspeicher nicht neu erstellen, die ursprünglichen Objektspeicherkonfigurationen sowie die Cold-Daten-Inhalte werden aufbewahrt.

- Weitere Informationen zu FabricPool-Konfigurationen finden Sie im "Festplatten- und Aggregatmanagement".

Schritt

1. Folgen Sie dem Verfahren „Ersetzen einer FabricPool-Spiegelung auf einer MetroCluster-Konfiguration“ in "Festplatten- und Aggregatmanagement".

Überprüfung der Lizenzen auf den ersetzten Nodes

Sie müssen neue Lizenzen für die Ersatzknoten installieren, wenn die beeinträchtigten Knoten ONTAP-Funktionen verwenden, die eine Standard-Lizenz (Node-locked) erfordern. Bei Standardlizenzen sollte jeder Node im Cluster über seinen eigenen Schlüssel für die Funktion verfügen.

Über diese Aufgabe

Bis zum Installieren von Lizenzschlüssel sind Funktionen, für die Standardlizenzen erforderlich sind, weiterhin für den Ersatz-Node verfügbar. Wenn der beeinträchtigte Knoten jedoch der einzige Node im Cluster war, der eine Lizenz für die Funktion besitzt, sind keine Konfigurationsänderungen an der Funktion zulässig. Durch die Verwendung nicht lizenzierter Funktionen auf dem Node können Sie Ihre Lizenzvereinbarung möglicherweise nicht mehr erfüllen, sodass Sie den Ersatzlizenzschlüssel oder die Schlüssel so schnell wie möglich auf dem Ersatzknoten installieren sollten.

Die Lizenzschlüssel müssen im 28-stelligen Format vorliegen.

Sie haben eine 90-Tage-Nachfrist zur Installation der Lizenzschlüssel. Nach Ablauf der Frist werden alle alten Lizenzen ungültig. Nachdem ein gültiger Lizenzschlüssel installiert wurde, haben Sie 24 Stunden Zeit, um alle Schlüssel zu installieren, bevor die Kulanzzeit endet.

> Wenn alle Nodes an einem Standort ausgetauscht wurden (ein einzelner Node bei einer MetroCluster Konfiguration mit zwei Nodes), müssen vor dem Wechsel die Lizenzschlüssel auf dem Ersatz-Node oder auf den Nodes installiert werden.

Schritte

1. Identifizieren Sie die Lizenzen auf dem Knoten:

   ```
   license show
   ```

   Im folgenden Beispiel werden Informationen zu Lizenzen im System angezeigt:

```
cluster_B::>  license show
         (system license show)

Serial Number: 1-80-00050
Owner: site1-01
Package           Type       Description             Expiration
-------          -------     -------------           -----------
Base             license     Cluster Base License        -
NFS              site        NFS License                 -
CIFS             site        CIFS License                -
iSCSI            site        iSCSI License               -
FCP              site        FCP License                 -
FlexClone        site        FlexClone License           -

6 entries were displayed.
```

2. Vergewissern Sie sich nach dem Wechsel zurück, dass die Lizenzen für den Node gut sind:

   ```
   metrocluster check license show
   ```

   Im folgenden Beispiel werden die Lizenzen angezeigt, die für den Knoten gut sind:

   ```
   cluster_B::> metrocluster check license show

   Cluster           Check                             Result
   -------           -------                           -------------
   Cluster_B         negotiated-switchover-ready       not-applicable
   NFS               switchback-ready                  not-applicable
   CIFS              job-schedules                     ok
   iSCSI             licenses                          ok
   FCP               periodic-check-enabled            ok
   ```

3. Wenn Sie neue Lizenzschlüssel benötigen, rufen Sie die Ersatz-Lizenzschlüssel auf der NetApp Support Site im Abschnitt „My Support“ unter „Software-Lizenzen“ auf.

   > Die neuen Lizenzschlüssel, die Sie benötigen, werden automatisch generiert und an die E-Mail-Adresse in der Datei gesendet. Wenn Sie die E-Mail mit den Lizenzschlüssel nicht innerhalb von 30 Tagen erhalten, lesen Sie den Abschnitt _ „Kontakt aufnehmen, wenn ich Probleme mit meinen Lizenzen habe?“_ im Knowledge Base-Artikel "Verfahren zum Austausch der Hauptplatine zur Aktualisierung der Lizenzierung auf einem All Flash FAS/FAS System"

4. Installieren Sie jeden Lizenzschlüssel:

   ```
   system license add -license-code license-key, license-key…+
   ```

5. Entfernen Sie ggf. die alten Lizenzen:
   a. Suchen Sie nach nicht verwendeten Lizenzen:

      ```
      license clean-up -unused -simulate
      ```

   b. Wenn die Liste korrekt aussieht, entfernen Sie die nicht verwendeten Lizenzen:

      ```
      license clean-up -unused
      ```

Wiederherstellung von Verschlüsselungsmanagement

Sind die Daten-Volumes verschlüsselt, müssen Sie das Verschlüsselungsmanagement wiederherstellen. Ist das Root-Volume verschlüsselt, müssen Sie das Verschlüsselungsmanagement wiederherstellen.

Schritte

1. Wenn Daten-Volumes verschlüsselt sind, stellen Sie die Schlüssel mithilfe des richtigen Befehls für Ihre Schlüsselverwaltungskonfiguration wieder her.

Sie verwenden…	Befehl
• Onboard-Verschlüsselungsmanagement*	`security key-manager onboard sync` Weitere Informationen finden Sie unter "Wiederherstellung der integrierten Schlüssel für das Verschlüsselungsmanagement".
Externes Schlüsselmanagement	`security key-manager key query -node node-name` Weitere Informationen finden Sie unter "Wiederherstellen der externen Schlüssel für das Verschlüsselungsmanagement".

2. Wenn das Root-Volume verschlüsselt ist, verwenden Sie das Verfahren unter "Wiederherstellung des Verschlüsselungsmanagements bei Verschlüsselung des Root-Volumes".

Zurückwechseln

Nachdem Sie die MetroCluster-Konfiguration repariert haben, können Sie den MetroCluster-Switchback-Vorgang ausführen. Der MetroCluster Switchback-Vorgang gibt die Konfiguration wieder in den normalen Betriebsstatus zurück, wobei die Virtual Machines (SVMs) am Disaster-Standort aktiv sind und die Daten aus den lokalen Festplattenpools bereitstellen.

Bevor Sie beginnen

- Der Disaster Cluster muss erfolgreich auf den verbleibenden Cluster umgeschaltet sein.
- Mit den Daten und den Root-Aggregaten muss eine Reparatur durchgeführt worden sein.
- Die verbleibenden Cluster-Nodes dürfen sich nicht im HA-Failover-Status befinden (alle Nodes müssen für jedes HA-Paar in Betrieb sein).
- Die Controller-Module des Disaster-Site-Standorts müssen vollständig gebootet werden und nicht im HA-Übernahmemodus.
- Das Root-Aggregat muss gespiegelt werden.
- Die Inter-Switch Links (ISLs) müssen online sein.

- Alle erforderlichen Lizenzen müssen auf dem System installiert sein.

Schritte

1. Vergewissern Sie sich, dass sich alle Nodes im Status aktiviert befinden:

   ```
   metrocluster node show
   ```

   Im folgenden Beispiel werden die Nodes angezeigt, die den Status aktiviert haben:

   ```
   cluster_B::>  metrocluster node show

   DR                        Configuration  DR
   Group Cluster Node        State          Mirroring Mode
   ----- ------- ----------- -------------- --------- --------------------
   1     cluster_A
                 node_A_1    configured     enabled   heal roots completed
                 node_A_2    configured     enabled   heal roots completed
         cluster_B
                 node_B_1    configured     enabled   waiting for
   switchback recovery
                 node_B_2    configured     enabled   waiting for
   switchback recovery
   4 entries were displayed.
   ```

2. Bestätigen Sie, dass die Neusynchronisierung auf allen SVMs abgeschlossen ist:

   ```
   metrocluster vserver show
   ```

3. Überprüfen Sie, ob alle automatischen LIF-Migrationen, die durch die heilenden Vorgänge durchgeführt werden, erfolgreich abgeschlossen sind:

   ```
   metrocluster check lif show
   ```

4. Führen Sie den Wechsel zurück durch, indem Sie den ausführen `metrocluster switchback` Befehl von einem beliebigen Node im verbleibenden Cluster
5. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe „Warten auf Umkehren“ anzeigt:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang „Normal“ anzeigt:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Wenn ein Wechsel zurückkehrt lange dauert, können Sie den Status der Basispläne in Bearbeitung überprüfen, indem Sie den folgenden Befehl auf der erweiterten Berechtigungsebene verwenden:

```
metrocluster config-replication resync-status show
```

6. Wiederherstellung beliebiger SnapMirror oder SnapVault Konfigurationen

   In ONTAP 8.3 müssen Sie nach dem Wechsel zum MetroCluster eine verlorene SnapMirror Konfiguration manuell wiederherstellen. In ONTAP 9.0 und höher wird die Beziehung automatisch wiederhergestellt.

Überprüfen eines erfolgreichen Umschalttasches

Nach dem Wechsel zurück möchten Sie sicherstellen, dass alle Aggregate und Storage Virtual Machines (SVMs) zurück und wieder online geschaltet werden.

Schritte

1. Vergewissern Sie sich, dass die Switched-Data-Aggregate zurückgeschaltet sind:

   ```
   storage aggregate show
   ```

   Im folgenden Beispiel ist aggr_b2 an Knoten B2 zurückgeschaltet:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Wenn am Disaster Site nicht gespiegelte Aggregate und nicht gespiegelte Aggregate nicht mehr vorhanden sind, dann zeigt das Aggregat in der Ausgabe des Befehls show des Storage aggregate möglicherweise den Status „`unknown`“ an. Wenden Sie sich an den technischen Support, um veraltete Einträge für nicht gespiegelte Aggregate zu entfernen, verweisen Sie im Knowledge Base-Artikel "Wie entfernt man veraltete, nicht gespiegelte Aggregate Einträge in einer MetroCluster nach dem Zwischenfall, bei dem Speicher verloren ging."

2. Vergewissern Sie sich, dass alle SVMs mit synchronen Zielen im verbleibenden Cluster inaktiv sind (mit dem Betriebsstatus „`stopped`“):

   `vserver show -subtype sync-destination`

```
node_B_1::> vserver show -subtype sync-destination
                                Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                              running    stopped    vs1a_vol   aggr_b2
```

   Für Sync-Ziel-Aggregate in der MetroCluster-Konfiguration wurde das Suffix „`-mc`“ automatisch an ihren Namen angehängt, um sie zu identifizieren.

3. Überprüfen Sie, ob die SVMs im Disaster-Cluster mit synchronisierten Quellen betriebsbereit sind:

```
vserver show -subtype sync-source
```

```
node_A_1::> vserver show -subtype sync-source
                                   Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                   running  running    vs1a_vol  aggr_b2
```

4. Vergewissern Sie sich, dass die Umkehrvorgänge mit dem erfolgreich waren `metrocluster operation show` Befehl.

Wenn die Befehlsausgabe angezeigt wird…	Dann…
Dass der Betriebszustand zurückwechseln erfolgreich ist.	Der Switch-Back-Vorgang ist abgeschlossen, und Sie können den Betrieb des Systems fortsetzen.
Dass der Betrieb des zurückkehrenden oder zurückkehrenden Agenten teilweise erfolgreich ist.	Führen Sie den vorgeschlagenen Fix aus, der in der Ausgabe des Befehls MetroCluster Operation show angegeben ist.

Nachdem Sie fertig sind

Sie müssen die vorherigen Abschnitte wiederholen, um den Umschalter in die entgegengesetzte Richtung auszuführen. Wenn Site_A die Umschaltung von Site_B durchgeführt hat, muss Site_B die Umschaltung von Site_A durchführen

Spiegelung der Root-Aggregate der Ersatz-Nodes

Falls Festplatten ausgetauscht wurden, müssen die Root-Aggregate der neuen Nodes am Disaster Site gespiegelt werden.

Schritte

1. Geben Sie am Notfallstandort die Aggregate an, die nicht gespiegelt wurden:

```
storage aggregate show
```

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1
raid4,

normal
node_A_2_aggr0
            1.49TB   74.12GB   95% online       1 node_A_2
raid4,

normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1         raid
4, normal

mirrored
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2         raid
4, normal

mirrored
4 entries were displayed.

cluster_A::>
```

2. Eines der Root-Aggregate spiegeln:

   ```
   storage aggregate mirror -aggregate root-aggregate
   ```

   Das folgende Beispiel zeigt, wie der Befehl Festplatten auswählt und wie Sie beim Spiegeln des Aggregats eine Bestätigung erhalten.

```
cluster_A::> storage aggregate mirror -aggregate node_A_2_aggr0

Info: Disks would be added to aggregate "node_A_2_aggr0" on node
"node_A_2" in
      the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid4)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          parity     2.10.0                    SSD
-
          data       1.11.19                   SSD
894.0GB
          data       2.10.2                    SSD
894.0GB

      Aggregate capacity available for volume use would be 1.49TB.

Do you want to continue? {y|n}: y

cluster_A::>
```

3. Überprüfen Sie, ob die Spiegelung des Root-Aggregats abgeschlossen ist:

   `storage aggregate show`

   Das folgende Beispiel zeigt, dass die Root-Aggregate gespiegelt werden.

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr0
            2.24TB   838.5GB   63% online       1 node_A_2    raid4,
                                                               mirrored,
                                                               normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2    raid4
                                                               mirrored,
                                                               normal
4 entries were displayed.

cluster_A::>
```

4. Wiederholen Sie diese Schritte für die anderen Root-Aggregate.

   Jedes Root-Aggregat, das keinen Status der Spiegelung hat, muss gespiegelt werden.

Neukonfiguration des ONTAP-Mediators (MetroCluster-IP-Konfigurationen)

Wenn Sie eine MetroCluster-IP-Konfiguration haben, die mit ONTAP Mediator konfiguriert wurde, müssen Sie die Zuordnung mit ONTAP Mediator entfernen und neu konfigurieren.

Bevor Sie beginnen

- Sie müssen über die IP-Adresse sowie den Benutzernamen und das Passwort für ONTAP Mediator verfügen.
- ONTAP Mediator muss auf dem Linux-Host konfiguriert und ausgeführt werden.

Schritte

1. Entfernen Sie die vorhandene ONTAP Mediator-Konfiguration:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Konfigurieren des ONTAP Mediators neu konfigurieren:

```
metrocluster configuration-settings mediator add -mediator-address mediator-
IP-address
```

Überprüfen des Systemzustands der MetroCluster-Konfiguration

Sie sollten den Systemzustand der MetroCluster-Konfiguration überprüfen, um einen ordnungsgemäßen Betrieb zu gewährleisten.

Schritte

1. Vergewissern Sie sich, dass die MetroCluster für jedes Cluster im normalen Modus konfiguriert ist:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Vergewissern Sie sich, dass die Spiegelung auf jedem Knoten aktiviert ist:

   ```
   metrocluster node show
   ```

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Prüfen Sie, ob die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the `metrocluster check show -instance` command
or sub-commands in `metrocluster check` directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run `metrocluster switchover -simulate` or `metrocluster
switchback -simulate`, respectively.
```

4. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

   `system health alert show`

5. Simulation eines Switchover-Vorgangs:

   a. Ändern Sie von der Eingabeaufforderung eines beliebigen Node auf die erweiterte Berechtigungsebene:

      `set -privilege advanced`

   Sie müssen mit reagieren `y` Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*) anzuzeigen.

   a. Führen Sie den Switchover mit durch `-simulate` Parameter:

      `metrocluster switchover -simulate`

   b. Zurück zur Administratorberechtigungsebene:

      `set -privilege admin`

6. Bestätigen Sie bei MetroCluster-IP-Konfigurationen mit ONTAP Mediator, dass ONTAP Mediator aktiv und betriebsbereit ist.

   a. Überprüfen Sie, ob die Mediator-Festplatten für das System sichtbar sind:

      `storage failover mailbox-disk show`

      Das folgende Beispiel zeigt, dass die Mailbox-Platten erkannt wurden.

```
node_A_1::*> storage failover mailbox-disk show
                 Mailbox
Node             Owner     Disk    Name        Disk UUID
-------------     ------   -----   -----        ----------------
sti113-vsim-ucs626g
.
.
     local     0m.i2.3L26
7BBA77C9:AD702D14:831B3E7E:0B0730EE:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i2.3L27
928F79AE:631EA9F9:4DCB5DE6:3402AC48:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i1.0L60
B7BCDB3C:297A4459:318C2748:181565A3:00000000:00000000:00000000:000000
00:00000000:00000000
.
.
.
     partner   0m.i1.0L14
EA71F260:D4DD5F22:E3422387:61D475B2:00000000:00000000:00000000:000000
00:00000000:00000000
     partner   0m.i2.3L64
4460F436:AAE5AB9E:D1ED414E:ABF811F7:00000000:00000000:00000000:000000
00:00000000:00000000
28 entries were displayed.
```

b. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

c. Überprüfen Sie, ob die Mailbox-LUNs für das System sichtbar sind:

```
storage iscsi-initiator show
```

In der Ausgabe wird das Vorhandensein der Mailbox-LUNs angezeigt:

```
Node    Type       Label      Target Portal     Target Name
Admin/Op
----    ----       --------   ---------    ---------
--------------------------------       --------
.
.
.
.node_A_1
               mailbox
                     mediator 172.16.254.1    iqn.2012-
05.local:mailbox.target.db5f02d6-e3d3    up/up
.
.
.
17 entries were displayed.
```

a. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

Wiederherstellung nach einem Ausfall eines Controllers

Nachdem die Systeme am Disaster-Standort Wartungsarbeiten oder Ersatz durchgeführt wurden, jedoch keine Controller ausgetauscht wurden, können Sie mit dem Prozess beginnen, die MetroCluster Konfiguration in einen vollständig redundanten Zustand zurückzusetzen. Dazu gehört auch die Reparatur der Konfiguration (zunächst die Daten-Aggregate und dann die Root-Aggregate) und das Durchführen des Switchback-Vorgangs.

Bevor Sie beginnen

- Alle MetroCluster-Hardware im Disaster-Cluster muss funktionsfähig sein.
- Die MetroCluster-Gesamtkonfiguration muss umschalten.
- In einer Fabric-Attached MetroCluster-Konfiguration muss die ISL zwischen den MetroCluster-Standorten verfügbar sein und betrieben werden.

Aktivieren Sie die Konsolenprotokollierung

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den von Ihnen verwendeten Geräten zu aktivieren und folgende Aktionen durchzuführen:

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung eine Wartungs-AutoSupport-Meldung aus, um die Case-Erstellung für die Dauer der Wartungsaktivität zu deaktivieren.

  Siehe Knowledge Base-Artikel "Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden".

- Aktivieren Sie die Sitzungsprotokollierung für jede CLI-Sitzung. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ im Knowledge Base-Artikel "So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen".

Reparatur der Konfiguration in einer MetroCluster-Konfiguration

In MetroCluster FC-Konfigurationen führen Sie die Heilungsvorgänge in einer bestimmten Reihenfolge aus, um die MetroCluster-Funktion nach einer Umschaltung wiederherzustellen.

In MetroCluster IP-Konfigurationen sollten die Heilungsvorgänge nach einer Umschaltung automatisch gestartet werden. Wenn dies nicht der Fall ist, können Sie die Heilungsoperationen manuell durchführen.

Bevor Sie beginnen

- Eine Umschaltung muss durchgeführt worden sein und der überlebende Standort muss Daten bereitstellen.
- Nodes am Disaster-Standort müssen angehalten oder deaktiviert werden.

  Sie dürfen während des Heilungsprozesses nicht vollständig gestartet werden.

- Storage am Disaster-Standort muss zugänglich sein (Shelfs werden hochgefahren, funktionieren und sind zugänglich).
- In Fabric-Attached MetroCluster-Konfigurationen müssen Inter-Switch-Links (ISLs) in Betrieb sein.
- In MetroCluster-Konfigurationen mit vier Nodes dürfen sich Nodes im verbleibenden Standort nicht im HA-Failover-Zustand befinden (alle Nodes müssen für jedes HA-Paar in Betrieb sein).

Über diese Aufgabe

Die Reparatur muss zunächst auf den Datenaggregaten und anschließend auf den Root-Aggregaten durchgeführt werden.

Reparieren der Datenaggregate

Die Datenaggregate müssen nach der Reparatur und dem Austausch beliebiger Hardware am Disaster-Standort repariert und ausgetauscht werden. In diesem Prozess werden die Datenaggregate neu synchronisiert und der (jetzt reparierte) Disaster-Standort wird auf den normalen Betrieb vorbereitet. Die Datenaggregate müssen vor dem Healing der Root-Aggregate repariert werden.

Über diese Aufgabe

Das folgende Beispiel zeigt eine erzwungene Umschaltung, um das Switchover-Aggregat online zu schalten. Alle Konfigurationsaktualisierungen im Remote-Cluster konnten erfolgreich auf das lokale Cluster repliziert werden. Im Rahmen dieses Verfahrens schalten Sie den Storage am Disaster Standort ein, jedoch nicht und dürfen die Controller-Module am DR-Standort nicht hochfahren.

Schritte

1. Überprüfen Sie, ob die Umschaltung abgeschlossen wurde:

   ```
   metrocluster operation show
   ```

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. Synchronisieren Sie die Datenaggregate neu, indem Sie den folgenden Befehl vom verbleibenden Cluster ausführen:

   `metrocluster heal -phase aggregates`

   ```
   controller_A_1::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.
   ```

   Wenn die Heilung ein Vetorecht ist, haben Sie die Möglichkeit, das zurückzugeben `metrocluster heal` Befehl mit dem `--override-vetoes` Parameter. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

3. Vergewissern Sie sich, dass der Vorgang abgeschlossen ist:

   `metrocluster operation show`

   ```
   controller_A_1::> metrocluster operation show
       Operation: heal-aggregates
         State: successful
   Start Time: 7/25/2014 18:45:55
      End Time: 7/25/2014 18:45:56
        Errors: -
   ```

4. Überprüfen Sie den Status der Aggregate:

   `storage aggregate show` Befehl.

   ```
   controller_A_1::> storage aggregate show
   Aggregate Size     Available Used% State   #Vols  Nodes        RAID
   Status
   --------- -------- --------- ----- ------- ------ ------------
   ------------
   ...
   aggr_b2   227.1GB  227.1GB   0%    online  0      mcc1-a2      raid_dp,
   mirrored, normal...
   ```

5. Wenn Storage am Disaster Standort ausgetauscht wurde, müssen eventuell die Aggregate neu gespiegelt werden.

Reparatur der Root-Aggregate nach einem Ausfall

Nachdem die Datenaggregate geheilt wurden, müssen Sie die Root-Aggregate heilen, um den Switchback-Betrieb zu ermöglichen.

Bevor Sie beginnen

Die Datenaggregationsphase des MetroCluster-Heilungsprozesses muss erfolgreich abgeschlossen sein.

Schritte

1. Wechseln Sie die gespiegelten Aggregate zurück:

   `metrocluster heal -phase root-aggregates`

   ```
   mcc1A::> metrocluster heal -phase root-aggregates
   [Job 137] Job succeeded: Heal Root Aggregates is successful
   ```

   Wenn die Heilung ein Vetorecht ist, haben Sie die Möglichkeit, das zurückzugeben `metrocluster heal` Befehl mit dem `--override-vetoes` Parameter. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

2. Stellen Sie sicher, dass der Heal-Vorgang abgeschlossen ist, indem Sie den folgenden Befehl auf dem Ziel-Cluster ausführen:

   `metrocluster operation show`

   ```
   mcc1A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

Überprüfen, ob das System für einen Wechsel bereit ist

Wenn sich Ihr System bereits im Umschaltzustand befindet, können Sie das verwenden `-simulate` Option, um eine Vorschau der Ergebnisse eines zurückkehrenden Vorgangs anzuzeigen.

Schritte

1. Schalten Sie jedes Controller-Modul am Disaster-Standort ein.

Wenn die Nodes ausgeschaltet sind:

Schalten Sie die Nodes ein.

Wenn die Eingabeaufforderung des LOADERS für DIE Nodes angezeigt wird:

Führen Sie den Befehl aus: `boot_ontap`

2. Überprüfen Sie nach dem Booten des Node, ob die Root-Aggregate gespiegelt sind.

Wenn ein Plex fehlschlägt:

a. Zerstöre den ausgefallenen Plex:

```
storage aggregate plex delete -aggregate <aggregate_name> -plex
<plex_name>
```

b. Stellen Sie die Spiegelbeziehung wieder her, indem Sie den Spiegel neu erstellen:

```
storage aggregate mirror -aggregate <aggregate-name>
```

Wenn ein Plex offline ist:

Online der Plex:

```
storage aggregate plex online -aggregate <aggregate_name> -plex <plex_name>
```

Wenn beide Plexus vorhanden sind:

Die Neusynchronisierung wird automatisch gestartet.

3. Simulieren Sie den Switchback-Betrieb:

a. Ändern Sie von der Eingabeaufforderung eines verbleibenden Node auf die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

Sie müssen mit reagieren `y` Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*) anzuzeigen.

a. Führen Sie den Umschalttavorgang mit dem aus `-simulate` Parameter:

```
metrocluster switchback -simulate
```

b. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

4. Überprüfen Sie die zurückgegebene Ausgabe.

Die Ausgabe zeigt an, ob der Switchback-Betrieb zu Fehlern führen würde.

Beispiel für Überprüfungsergebnisse

Das folgende Beispiel zeigt die erfolgreiche Überprüfung eines Switchback-Vorgangs:

```
cluster4::*> metrocluster switchback -simulate
  (metrocluster switchback)
[Job 130] Setting up the nodes and cluster components for the switchback
operation...DBG:backup_api.c:327:backup_nso_sb_vetocheck : MetroCluster
Switch Back
[Job 130] Job succeeded: Switchback simulation is successful.

cluster4::*> metrocluster op show
  (metrocluster operation show)
  Operation: switchback-simulate
      State: successful
 Start Time: 5/15/2014 16:14:34
   End Time: 5/15/2014 16:15:04
     Errors: -

cluster4::*> job show -name Me*
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
130    MetroCluster Switchback
                            cluster4
                                       cluster4-01
                                                      Success
       Description: MetroCluster Switchback Job - Simulation
```

Zurückwechseln

Nachdem Sie die MetroCluster-Konfiguration repariert haben, können Sie den MetroCluster-Switchback-Vorgang ausführen. Der MetroCluster Switchback-Vorgang gibt die Konfiguration wieder in den normalen Betriebsstatus zurück, wobei die Virtual Machines (SVMs) am Disaster-Standort aktiv sind und die Daten aus den lokalen Festplattenpools bereitstellen.

Bevor Sie beginnen

- Der Disaster Cluster muss erfolgreich auf den verbleibenden Cluster umgeschaltet sein.
- Mit den Daten und den Root-Aggregaten muss eine Reparatur durchgeführt worden sein.
- Die verbleibenden Cluster-Nodes dürfen sich nicht im HA-Failover-Status befinden (alle Nodes müssen für jedes HA-Paar in Betrieb sein).
- Die Controller-Module des Disaster-Site-Standorts müssen vollständig gebootet werden und nicht im HA-Übernahmemodus.
- Das Root-Aggregat muss gespiegelt werden.
- Die Inter-Switch Links (ISLs) müssen online sein.

- Alle erforderlichen Lizenzen müssen auf dem System installiert sein.

Schritte

1. Vergewissern Sie sich, dass sich alle Nodes im Status aktiviert befinden:

   ```
   metrocluster node show
   ```

   Im folgenden Beispiel werden die Nodes angezeigt, die sich im Status „aktiviert“ befinden:

   ```
   cluster_B::>  metrocluster node show

   DR                        Configuration  DR
   Group Cluster Node        State          Mirroring Mode
   ----- ------- ----------- -------------- --------- --------------------
   1     cluster_A
                 node_A_1    configured     enabled   heal roots completed
                 node_A_2    configured     enabled   heal roots completed
         cluster_B
                 node_B_1    configured     enabled   waiting for
   switchback recovery
                 node_B_2    configured     enabled   waiting for
   switchback recovery
   4 entries were displayed.
   ```

2. Bestätigen Sie, dass die Neusynchronisierung auf allen SVMs abgeschlossen ist:

   ```
   metrocluster vserver show
   ```

3. Überprüfen Sie, ob alle automatischen LIF-Migrationen, die durch die heilenden Vorgänge durchgeführt werden, erfolgreich abgeschlossen sind:

   ```
   metrocluster check lif show
   ```

4. Führen Sie den Wechsel zurück durch, indem Sie den folgenden Befehl von einem beliebigen Node im verbleibenden Cluster aus ausführen.

   ```
   metrocluster switchback
   ```

5. Überprüfen Sie den Fortschritt des Umschalttaschens:

   ```
   metrocluster show
   ```

   Der Umkehrvorgang läuft noch, wenn die Ausgabe „Warten auf Umkehren“ anzeigt:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

Der Umschalttavorgang ist abgeschlossen, wenn der Ausgang „Normal“ anzeigt:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Wenn ein Wechsel zurückgreift und lange dauert, können Sie den Status von Basisplänen prüfen, indem Sie den folgenden Befehl auf der erweiterten Berechtigungsebene verwenden.

```
metrocluster config-replication resync-status show
```

6. Wiederherstellung beliebiger SnapMirror oder SnapVault Konfigurationen

   In ONTAP 8.3 müssen Sie nach dem Wechsel zum MetroCluster eine verlorene SnapMirror Konfiguration manuell wiederherstellen. In ONTAP 9.0 und höher wird die Beziehung automatisch wiederhergestellt.

Überprüfen eines erfolgreichen Umschalttasches

Nach dem Wechsel zurück möchten Sie sicherstellen, dass alle Aggregate und Storage Virtual Machines (SVMs) zurück und wieder online geschaltet werden.

Schritte

1. Vergewissern Sie sich, dass die Switched-Data-Aggregate zurückgeschaltet sind:

   ```
   storage aggregate show
   ```

   Im folgenden Beispiel ist aggr_b2 an Knoten B2 zurückgeschaltet:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Wenn am Katastrophenstandort nicht gespiegelte Aggregate enthalten sind und die nicht gespiegelten Aggregate nicht mehr vorhanden sind, wird das Aggregat möglicherweise einen „unbekannten“ Zustand in der Ausgabe des angezeigt `storage aggregate show` Befehl. Wenden Sie sich an den technischen Support, um veraltete Einträge für nicht gespiegelte Aggregate zu entfernen und den Knowledge Base-Artikel zu verweisen "Wie entfernt man veraltete, nicht gespiegelte Aggregate Einträge in einer MetroCluster nach dem Zwischenfall, bei dem Speicher verloren ging."

2. Vergewissern Sie sich, dass alle SVMs mit synchronen Zielen im verbleibenden Cluster inaktiv sind (mit dem Betriebsstatus „`stopped`“):

   `vserver show -subtype sync-destination`

```
node_B_1::> vserver show -subtype sync-destination
                                 Admin    Operational  Root
Vserver       Type    Subtype    State    State        Volume
Aggregate
-----------   ------- ---------- -------- ----------   --------
----------
...
cluster_A-vs1a-mc data sync-destination
                                running    stopped    vs1a_vol   aggr_b2
```

   Für Sync-Ziel-Aggregate in der MetroCluster-Konfiguration wurde das Suffix „`-mc`“ automatisch an ihren Namen angehängt, um sie zu identifizieren.

3. Überprüfen Sie, ob die SVMs im Disaster-Cluster mit synchronisierten Quellen betriebsbereit sind:

```
vserver show -subtype sync-source
```

```
node_A_1::> vserver show -subtype sync-source
                                   Admin    Operational  Root
Vserver        Type    Subtype    State    State        Volume
Aggregate
-----------    ------- ---------- -------- ----------   --------
----------
...
vs1a           data    sync-source
                                   running  running    vs1a_vol  aggr_b2
```

4. Vergewissern Sie sich, dass die Switch-Back-Vorgänge erfolgreich waren:

   ```
   metrocluster operation show
   ```

Wenn die Befehlsausgabe angezeigt wird…	Dann…
Dass der Betriebszustand zurückwechseln erfolgreich ist.	Der Switch-Back-Vorgang ist abgeschlossen, und Sie können den Betrieb des Systems fortsetzen.
Dass der zurückwechseln Betrieb oder `switchback-continuation-agent` Der Vorgang ist teilweise erfolgreich.	Führen Sie den vorgeschlagenen Fix aus, der in der Ausgabe des angegeben ist `metrocluster operation show` Befehl.

Nachdem Sie fertig sind

Sie müssen die vorherigen Abschnitte wiederholen, um den Umschalter in die entgegengesetzte Richtung auszuführen. Wenn Site_A die Umschaltung von Site_B durchgeführt hat, muss Site_B die Umschaltung von Site_A durchführen

Löschen von veralteten Aggregat-Auflistungen nach dem Wechsel zurück

Unter Umständen nach dem Wechsel zurück können Sie feststellen, dass *veraltete* Aggregate vorhanden sind. Veraltete Aggregate sind Aggregate, die aus ONTAP entfernt wurden, deren Informationen jedoch auf der Festplatte gespeichert bleiben. Veraltete Aggregate werden mit dem angezeigt `nodeshell aggr status -r` Befehl, aber nicht mit dem `storage aggregate show` Befehl. Sie können diese Datensätze so löschen, dass sie nicht mehr angezeigt werden.

Über diese Aufgabe

Veraltete Aggregate können auftreten, wenn Sie Aggregate verschoben haben, während die MetroCluster Konfiguration in der Umschaltung war. Beispiel:

1. Standort A schaltet zu Standort B. um
2. Sie löschen die Spiegelung für ein Aggregat und verschieben das Aggregat zur Lastverteilung von Node_B_1 auf Node_B_2.
3. Sie führen Aggregatheilung aus.

Zu diesem Zeitpunkt erscheint ein veralteten Aggregat auf Node_B_1, obwohl das eigentliche Aggregat von

diesem Node gelöscht wurde. Dieses Aggregat erscheint in der Ausgabe der `nodeshell aggr status -r` Befehl. Er wird nicht in der Ausgabe von angezeigt `storage aggregate show` Befehl.

1. Vergleichen Sie die Ausgabe der folgenden Befehle:

   ```
   storage aggregate show

   run local aggr status -r
   ```

   Veraltete Aggregate werden im angezeigt `run local aggr status -r` Ausgabe, aber nicht im `storage aggregate show` Ausgabe: Beispielsweise könnte das folgende Aggregat im angezeigt werden `run local aggr status -r` Ausgabe:

   ```
   Aggregate aggr05 (failed, raid_dp, partial) (block checksums)
   Plex /aggr05/plex0 (offline, failed, inactive)
     RAID group /myaggr/plex0/rg0 (partial, block checksums)

    RAID Disk Device  HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)
   Phys (MB/blks)
    --------- ------  ------------- ---- ---- ----  ----- --------------
   --------------
    dparity   FAILED          N/A                        82/ -
    parity    0b.5    0b    -   -   SA:A   0 VMDISK  N/A 82/169472
   88/182040
    data      FAILED          N/A                        82/ -
    data      FAILED          N/A                        82/ -
    data      FAILED          N/A                        82/ -
    data      FAILED          N/A                        82/ -
    data      FAILED          N/A                        82/ -
    data      FAILED          N/A                        82/ -
    Raid group is missing 7 disks.
   ```

2. Entfernen des veralteten Aggregats:

   a. Ändern Sie von der Eingabeaufforderung eines Node auf die erweiterte Berechtigungsebene:

      ```
      set -privilege advanced
      ```

   Sie müssen mit reagieren `y` Wenn Sie dazu aufgefordert werden, den erweiterten Modus fortzusetzen und die Eingabeaufforderung für den erweiterten Modus (*) anzuzeigen.

   a. Entfernen des veralteten Aggregats:

      ```
      aggregate remove-stale-record -aggregate aggregate_name
      ```

   b. Zurück zur Administratorberechtigungsebene:

      ```
      set -privilege admin
      ```

3. Bestätigen Sie, dass der veraltete Aggregatdatensatz entfernt wurde:

```
run local aggr status -r
```

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Sicherheitsinformationen und gesetzliche Hinweise

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945

Copyright-Informationen

Copyright © 2025 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.