FlexPod Datacenter

FlexPod

NetApp
January 21, 2025

Inhalt

FlexPod Datacenter

FlexPod Datacenter mit NetApp SnapMirror Business Continuity und ONTAP 9.10

TR-4920: FlexPod Datacenter mit NetApp SnapMirror Business Continuity und ONTAP 9.10

Jyh-shing Chen, NetApp

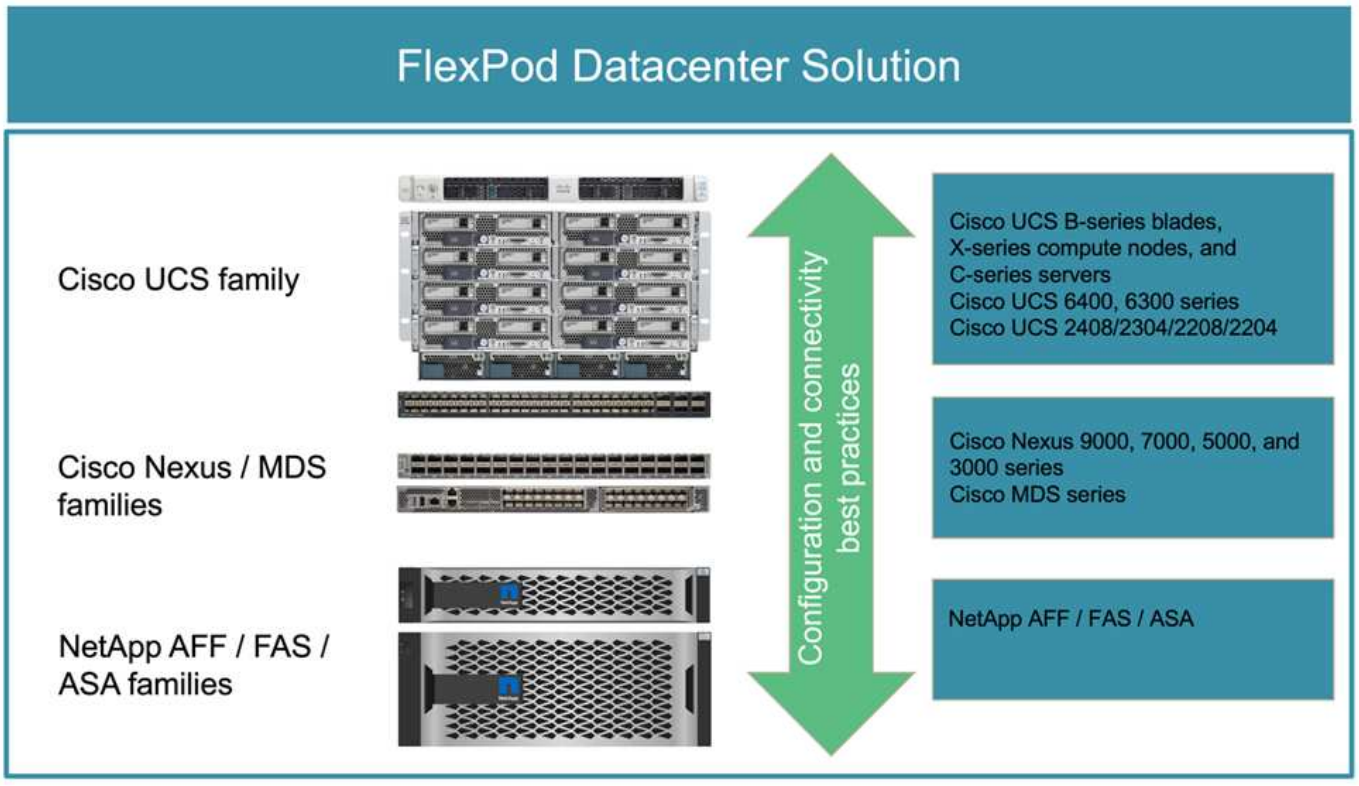
Einführung

Die FlexPod Lösung

FlexPod ist eine Best-Practice-Architektur für konvergente Infrastrukturen, die die folgenden Komponenten von Cisco und NetApp umfasst:

- Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus und MDS Switches-Familien
- NetApp FAS, NetApp AFF und NetApp All SAN Array (ASA) Systeme

Die folgende Abbildung zeigt einige der zum Erstellen von FlexPod Lösungen verwendeten Komponenten. Diese Komponenten sind sowohl von Cisco als auch von NetApp entsprechend den Best Practices miteinander verbunden und konfiguriert, sodass eine ideale Plattform für eine Vielzahl von Enterprise Workloads ohne Bedenken eingesetzt werden kann.



Es ist ein großes Portfolio von Cisco Validated Designs (CVDs) und NetApp Verified Architectures (NVAs)

erhältlich. Diese CVDs und NVAs decken alle größeren Datacenter-Workloads ab und sind das Ergebnis der kontinuierlichen Zusammenarbeit und Innovationen zwischen NetApp und Cisco auf den FlexPod-Lösungen.

FlexPod CVDs und NVAs enthalten umfangreiche Tests und Validierungen im Erstellungsprozess. Außerdem bieten sie Referenzarchitekturen-Designs sowie Schritt-für-Schritt-Anleitungen für die Implementierung von FlexPod Lösungen für Partner und Kunden. Wenn Unternehmen diese CVDs und NVAs als Leitfäden für Design und Implementierung einsetzen, können sie Risiken verringern, das Ausfallzeiten der Lösung verringern und die Verfügbarkeit, Skalierbarkeit, Flexibilität und Sicherheit der implementierten FlexPod Lösungen erhöhen.

Jede der gezeigten FlexPod-Komponentenfamilien (Cisco UCS, Cisco Nexus/MDS Switches und NetApp Storage) bietet Plattform- und Ressourcenoptionen für die vertikale und horizontale Skalierung der Infrastruktur. Gleichzeitig werden die Funktionen unterstützt, die unter den Best Practices für Konfiguration und Konnektivität von FlexPod erforderlich sind. FlexPod kann auch horizontal für Umgebungen skaliert werden, in denen mehrere konsistente Implementierungen durch die Bereitstellung weiterer FlexPod-Stacks erforderlich sind.

Disaster Recovery und Business Continuity

Unternehmen können auf verschiedene Weise sicherstellen, dass sie ihre Applikations- und Datenservices nach Ausfällen schnell wiederherstellen können. Mit einem Disaster Recovery- (DR-) und Business Continuity-Plan (BC), der Implementierung einer Lösung, die die Geschäftsziele erfüllt, und durch regelmäßige Tests der Disaster-Szenarien können Unternehmen die Wiederherstellung nach einem Notfall durchführen und wichtige Business Services nach einem Notfall aufrechterhalten.

Für verschiedene Applikations- und Datenservices können Unternehmen unterschiedliche DR- und BC-Anforderungen haben. Einige Applikationen und Daten sind möglicherweise nicht in Notfällen oder Notfallsituationen notwendig, während andere Unternehmen möglicherweise kontinuierlich zur Verfügung stehen müssen, um geschäftliche Anforderungen zu unterstützen.

Für geschäftskritische Applikations- und Datenservices, die den Betrieb stören könnten, wenn diese nicht verfügbar sind, ist eine sorgfältige Evaluierung erforderlich, um Fragen wie Wartungsarbeiten und Ausfallszenarien zu beantworten, die Ihr Unternehmen in Betracht ziehen sollte, Wie viele Daten das Unternehmen bei einem Ausfall verkraften kann und wie schnell die Recovery erfolgen kann und sollte.

Für Unternehmen, die Datenservices zur Umsatzgenerierung nutzen, müssen die Datenservices möglicherweise durch eine Lösung geschützt werden, die nicht nur verschiedenen Single-Point-of-Failure-Szenarien, sondern auch einem Ausfallszenario am Standort standhält, um den unterbrechungsfreien Geschäftsbetrieb zu gewährleisten.

Recovery-Zeitpunkt und Recovery-Zeitvorgabe

Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) bezeichnet die Menge an Daten im Hinblick auf die Zeit, die Sie sich leisten können, oder den Zeitpunkt, an dem Sie Ihre Daten wiederherstellen können. Mit einem täglichen Backup-Plan kann ein Unternehmen einen Tag an Daten verlieren, weil die Änderungen an den Daten seit dem letzten Backup in einem Notfall verloren gehen könnte. Für geschäftskritische und geschäftskritische Datenservices sind unter Umständen ein RPO von Null sowie ein Plan und eine zugehörige Infrastruktur zum Schutz von Daten ohne Datenverluste erforderlich.

Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) beschreibt, wie lange Sie sich leisten können, ohne die Daten verfügbar zu haben oder wie schnell Datenservices gesichert werden müssen. So kann ein Unternehmen beispielsweise über eine Backup- und Recovery-Implementierung verfügen, bei der aufgrund seiner Größe herkömmliche Tapes für bestimmte Datensätze verwendet werden. Das Ergebnis: Die Wiederherstellung der Daten von den Backup-Tapes kann es im Falle eines Infrastruktur-Ausfalls mehrere Stunden oder gar Tage dauern. Überlegungen zur Zeit müssen außerdem die Zeit beinhalten, die erforderlich

ist, um die Infrastruktur zusätzlich zum Wiederherstellen der Daten zu sichern. Für geschäftskritische Datenservices benötigen Sie unter Umständen ein sehr niedriges RTO und können daher für Business Continuity nur eine Failover-Zeit von Sekunden oder Minuten tolerieren, um die Datenservices schnell wieder online zu bringen.

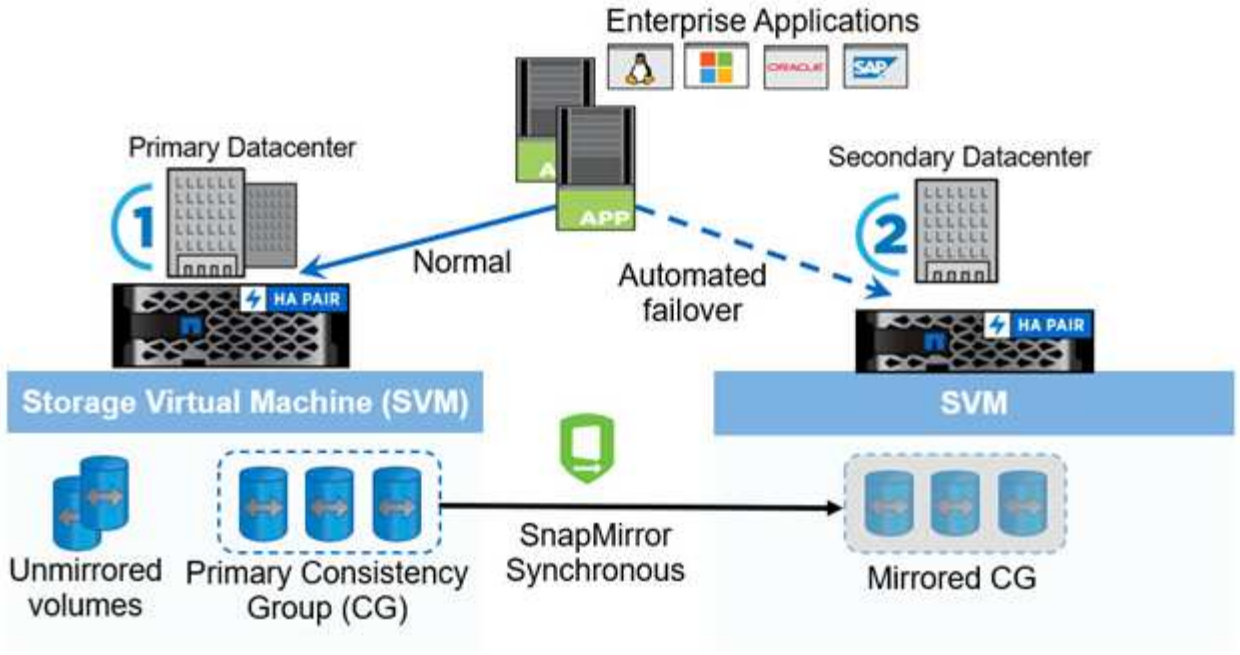
SM-BC

Ab ONTAP 9.8 können Sie SAN-Workloads für transparentes Applikations-Failover mit NetApp SM-BC sichern. Sie können Konsistenzgruppen zwischen zwei AFF Clustern oder zwei ASA Clustern erstellen, um Daten zu replizieren, damit ein Recovery Point Objective von null und ein Recovery Time Objective von fast null erreicht wird.

Die SM-BC Lösung repliziert Daten mithilfe der SnapMirror Synchronous Technologie über ein IP-Netzwerk. Die Lösung bietet Granularität auf Applikationsebene und automatisches Failover zur Sicherung geschäftskritischer Daten-Services wie Microsoft SQL Server, Oracle usw. mit iSCSI oder FC protokollbasierten SAN LUNs. Ein an einem dritten Standort bereitgestellter ONTAP Mediator überwacht die SM-BC-Lösung und ermöglicht ein automatisches Failover bei einem Standortausfall.

Eine Konsistenzgruppe (CG) ist eine Sammlung von FlexVol-Volumes, die eine konsistente Schreibreihenfolge für den Applikations-Workload gewährleistet, der zur Gewährleistung der Business Continuity geschützt werden muss. Es ermöglicht gleichzeitige, absturzkonsistente Snapshot-Kopien einer Sammlung von Volumes zu einem bestimmten Zeitpunkt. Eine SnapMirror-Beziehung, auch als CG-Beziehung bekannt, wird zwischen einer Quell-CG und einer Ziel-CG eingerichtet. Die Gruppe der Volumes, die als Teil einer CG ausgewählt wurden, kann einer Applikationsinstanz, einer Gruppe von Applikationsinstanzen oder für eine komplette Lösung zugeordnet werden. Darüber hinaus können auf der Grundlage von Geschäftsanforderungen und Änderungen die Beziehungen der SM-BC Consistency Group nach Bedarf erstellt oder gelöscht werden.

Wie in der folgenden Abbildung dargestellt, werden die Daten in der Konsistenzgruppe für Disaster Recovery und Business Continuity in einen zweiten ONTAP Cluster repliziert. Die Anwendungen haben Konnektivität zu den LUNs in beiden ONTAP-Clustern. I/O wird normalerweise vom primären Cluster bereitgestellt und setzt diesen automatisch vom sekundären Cluster fort, falls auf dem primären Cluster ein Notfall auftritt. Beim Design einer SM-BC-Lösung muss die unterstützte Objektanzahl für die CG-Beziehungen (z. B. maximal 20 CGS und maximal 200 Endpunkte) beachtet werden, um zu vermeiden, dass die unterstützten Grenzwerte überschritten werden.



"Weiter: FlexPod SM-BC Lösung."

FlexPod SM-BC Lösung

"Zurück: Einführung."

Lösungsüberblick

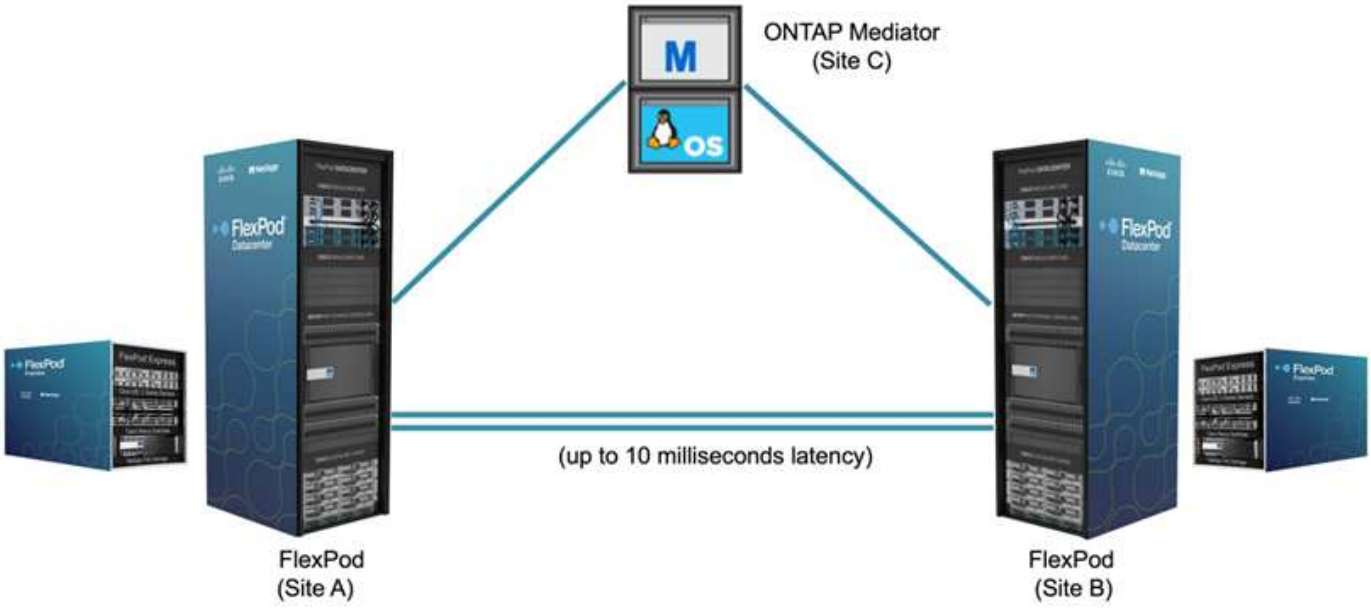
Eine FlexPod SM-BC Lösung besteht im Wesentlichen aus zwei FlexPod Systemen, die sich an zwei Standorten trennen und in Verbindung setzen, um eine hochverfügbare, äußerst flexible und hochgradig zuverlässige Datacenter-Lösung bereitzustellen, die trotz eines Standortausfalls Business Continuity bietet.

Neben der Implementierung von zwei neuen FlexPod-Infrastrukturen zur Erstellung einer FlexPod SM-BC Lösung kann die Lösung auch auf zwei vorhandenen FlexPod-Infrastrukturen implementiert werden, die mit SM-BC kompatibel sind, oder indem ein neues FlexPod hinzugefügt wird, um eine bestehende FlexPod zu nutzen.

Die beiden FlexPod Systeme in einer FlexPod SM-BC Lösung müssen in Konfigurationen nicht identisch sein. Die zwei ONTAP Cluster müssen jedoch aus den gleichen Storage-Familien stammen, entweder zwei AFF oder zwei ASA Systeme, jedoch nicht unbedingt das gleiche Hardware-Modell. Die SM-BC Lösung unterstützt keine FAS Systeme.

Die beiden FlexPod Standorte benötigen Netzwerkkonnektivität, was der Bandbreite der Lösung und den Quality of Service-Anforderungen entspricht und zwischen den Standorten weniger als 10 Millisekunden (10 ms) Latenz für Umlaufzeit hat, wie von der ONTAP SM-BC Lösung benötigt. Für diese FlexPod SM-BC Lösungsvalidierung werden die beiden FlexPod-Standorte über ein erweitertes Layer-2-Netzwerk im selben Lab miteinander verbunden.

Die NetApp ONTAP SM-BC Lösung bietet synchrone Replizierung zwischen den beiden NetApp Storage-Clustern und sorgt so für Hochverfügbarkeit und Disaster Recovery an Standorten bzw. Großraumgebieten. Der an einem dritten Standort implementierte ONTAP Mediator überwacht die Lösung und ermöglicht ein automatisiertes Failover im Falle eines Standortausfalls. Die folgende Abbildung bietet einen allgemeinen Überblick über die Komponenten der Lösung.



Mit der FlexPod SM-BC Lösung können Sie eine Private Cloud auf Basis von VMware vSphere auf Basis einer verteilten und doch integrierten Infrastruktur implementieren. Die integrierte Lösung ermöglicht die Koordinierung mehrerer Standorte als eine einheitliche Lösungsinfrastruktur, um Datenservices vor einer Vielzahl von Single Point-of-Failure und einem kompletten Standortausfall zu schützen.

In diesem technischen Bericht werden einige der End-to-End-Designüberlegungen der FlexPod SM-BC-Lösung hervorgehoben. Die Fachleute sollten Informationen in den verschiedenen FlexPod CVDs und NVAs verwenden, um weitere Einzelheiten zur Implementierung von FlexPod Lösungen zu erhalten.

Die Lösung wurde zwar durch die Implementierung von zwei FlexPod Systemen auf der Basis von Best Practices von FlexPod validiert, wie in CVDs dokumentiert. Dennoch werden die Anforderungen für die SM-BC Lösung berücksichtigt. Die in diesem Bericht vorgestellten FlexPod SM-BC Lösung wurde für Ausfallsicherheit und Fehlertoleranz während verschiedener Fehlerszenarien und in einem simulierten Standortfehler validiert.

Anforderungen der Lösung erfüllen

Die FlexPod SM-BC Lösung ist auf folgende wichtige Anforderungen ausgerichtet:

- Business Continuity für geschäftskritische Applikationen und Datenservices bei einem vollständigen Datacenter-Ausfall
- Flexible, verteilte Workload-Platzierung mit Workload-Mobilität über mehrere Datacenter hinweg
- Standortaffinität, bei der während des normalen Betriebs lokal auf Virtual Machine-Daten vom selben Datacenter-Standort zugegriffen wird
- Schnelles Recovery ohne Datenverlust bei Standortausfall

Lösungskomponenten

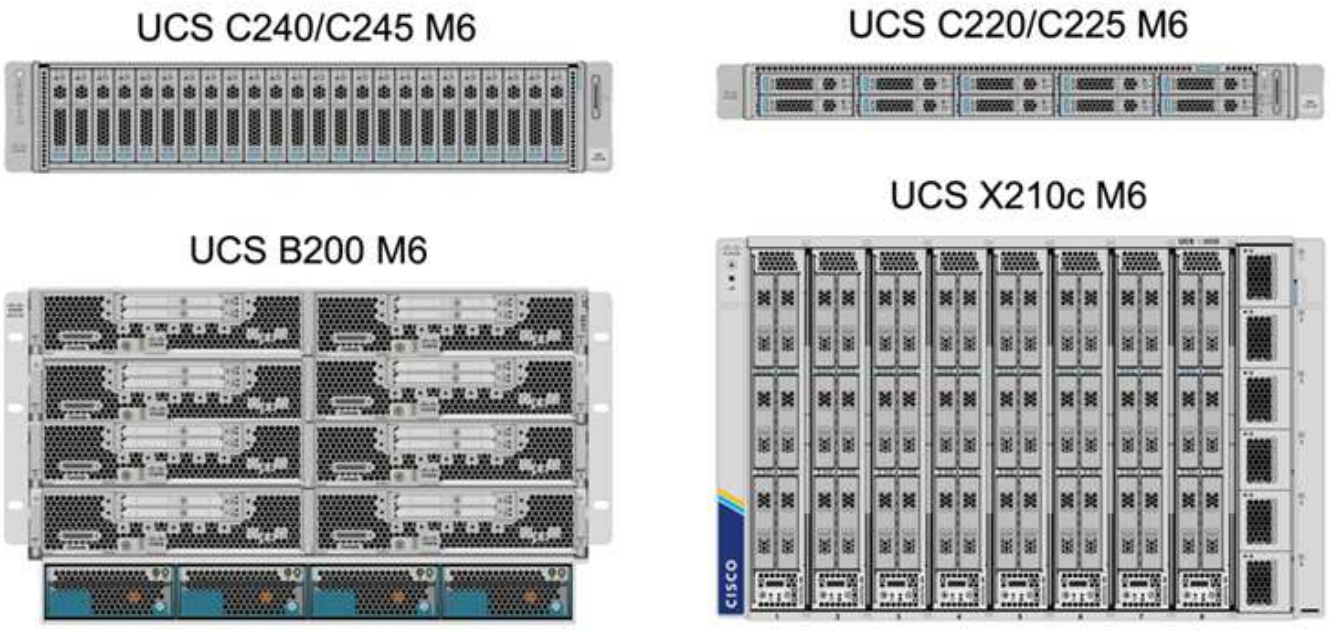
Cisco Computing-Komponenten

Cisco UCS ist eine integrierte Computing-Infrastruktur für einheitliche Computing-Ressourcen, Unified Fabric und einheitliches Management. Damit können Unternehmen den Einsatz von Applikationen, einschließlich Virtualisierung und Bare Metal Workloads, automatisieren und beschleunigen. Das Cisco UCS unterstützt eine Vielzahl von Implementierungsanwendungsfällen, einschließlich Remote-Standorten und Zweigstellen, Datacenter und Hybrid-Cloud-Anwendungsfälle. Je nach den spezifischen Lösungsanforderungen kann die

FlexPod Cisco Computing-Implementierung eine Vielzahl von Komponenten in unterschiedlichen Maßstäben verwenden. Die folgenden Abschnitte enthalten zusätzliche Informationen zu einigen der UCS Komponenten.

UCS Server und Compute-Node

Die folgende Abbildung zeigt einige Beispiele für die UCS Server-Komponenten: Rack Server der UCS C-Serie, UCS 5108 Chassis mit Blade Servern der B-Serie und das neue UCS X9508 Chassis mit Computing-Nodes der X-Serie. Die Cisco UCS C-Series Rack Server sind in einem und zwei Rack-Einheiten (RU)-Formfaktor, Intel und AMD CPU-basierten Modellen sowie mit verschiedenen CPU-Geschwindigkeiten und -Kernen, Arbeitsspeicher und I/O-Optionen verfügbar. Die Cisco UCS Blade Server der B-Serie und die neuen Computing-Nodes der X-Serie sind auch mit verschiedenen CPU-, Arbeitsspeicher- und I/O-Optionen verfügbar. Zur Erfüllung der unterschiedlichen geschäftlichen Anforderungen werden sie alle in der FlexPod Architektur unterstützt.



Neben den in der Abbildung gezeigten Rack-Servern C220/C225/C240/C245 M6, B200 M6 Blade Servern und X210c Computing-Nodes können auch ältere Rack- und Blade-Server-Generationen genutzt werden, wenn sie weiterhin unterstützt werden.

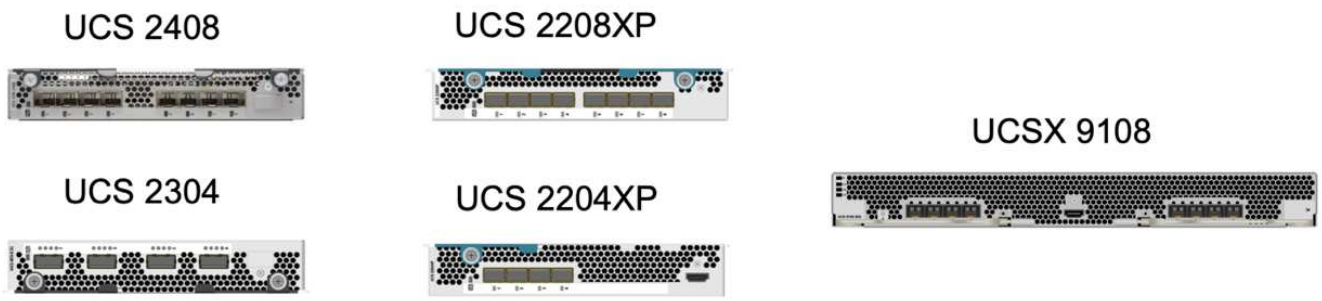
I/O-Modul und Intelligent Fabric Module

Das I/O-Modul (IOM)/Fabric Extender und das Intelligent Fabric Module (IFM) bieten eine einheitliche Fabric-Konnektivität für das Cisco UCS 5108 Blade-Server-Chassis und das Cisco UCS X9508 X-Series Gehäuse.

Die vierte Generation des UCS IOM 2408 verfügt über acht 25-G Unified Ethernet-Ports für die Verbindung des UCS 5108-Gehäuses mit Fabric Interconnects (FI). Jeder 2408 verfügt über vier 10-G-Rückwandplatine zur Ethernet-Verbindung über die Midplane zu jedem Blade-Server im Gehäuse.

Der UCSD 9108 25G IFM verfügt über acht 25-G Unified Ethernet Ports für die Verbindung der Blade Server im UCS X9508 Chassis mit Fabric Interconnects. Jeder 9108 verfügt über vier 25-G-Verbindungen zu jedem UCS X210c Computing-Node im X9108-Gehäuse. Das 9108 IFM arbeitet auch in Verbindung mit dem Fabric Interconnect für das Management der Gehäuseumgebung.

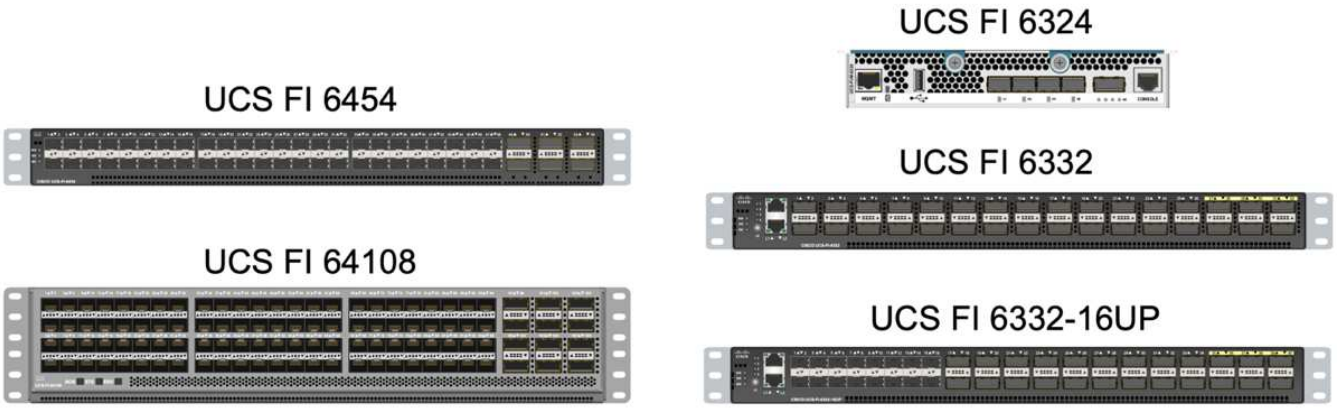
Die folgende Abbildung zeigt die UCS 2408 und früheren IOM Generationen für das UCS 5108 Chassis und den 9108 IFM für das X9508 Chassis.



UCS Fabric Interconnects

Die Cisco UCS Fabric Interconnects (FIS) sorgen für Konnektivität und Management für das gesamte Cisco UCS. Das FIS des Systems wird in der Regel als aktiv/aktiv-Paar bereitgestellt und integriert alle Komponenten in eine einzige, hochverfügbare Management-Domäne, die vom Cisco UCS Manager oder Cisco Intersight gesteuert wird. Cisco UCS FIS bieten ein einzelnes Unified Fabric für das System mit latenzarmem und verlustfreiem, Cut-Through-Switching, das LAN-, SAN- und Management-Datenverkehr über ein einziges Kabelset unterstützt.

Für den Cisco UCS FIS der vierten Generation gibt es zwei Varianten: UCS FI 6454 und 64108. Zu den Merkmalen gehören Unterstützung für 10/25 Gbps Ethernet-Ports, 1/10/25-Gbps-Ethernet-Up-Link-Ports, 40/100-Gbps-Ports und Unified Ports, die 10/25-Gigabit-Ethernet oder 8/16/32-Gbps-Fibre Channel unterstützen. Die folgende Abbildung zeigt den Cisco UCS FIS der vierten Generation zusammen mit den ebenfalls unterstützten Modellen der dritten Generation.



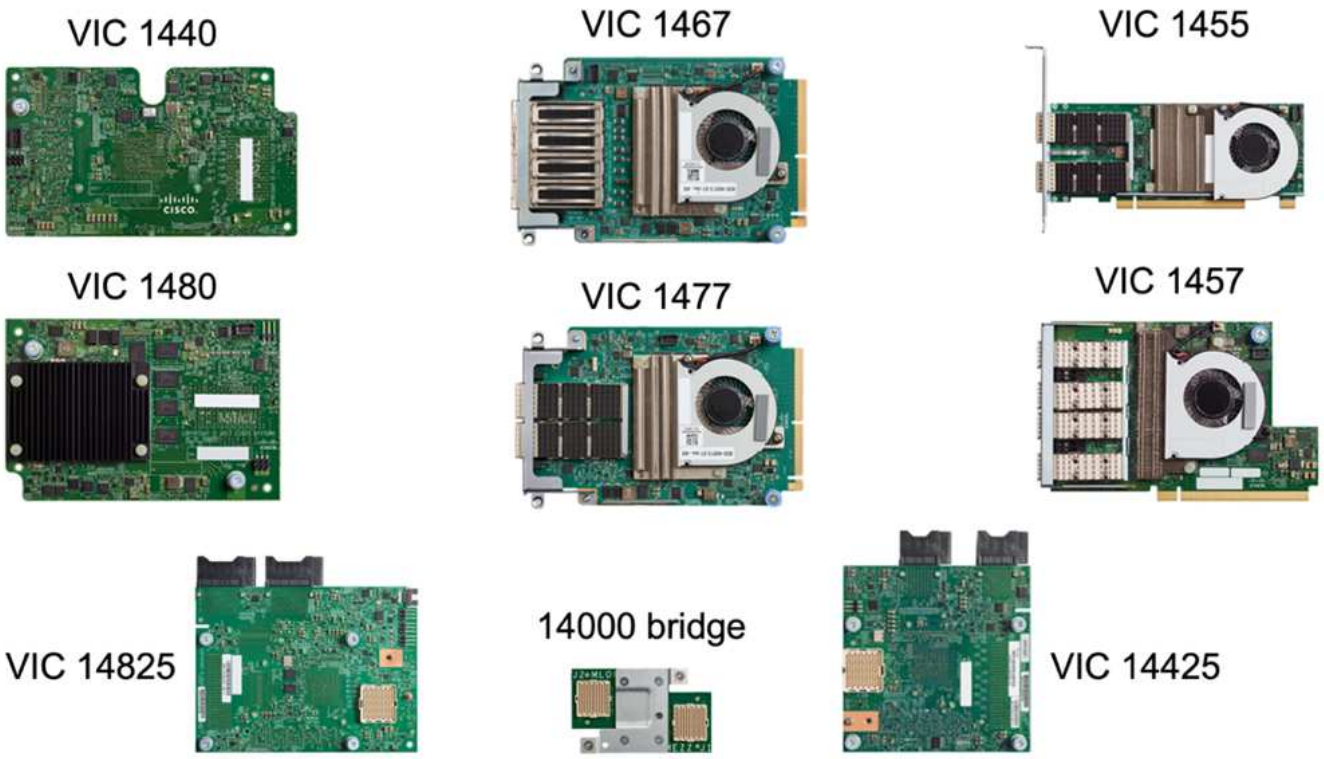
Zur Unterstützung des Cisco UCS X-Series Gehäuses sind Fabric Interconnects der vierten Generation erforderlich, die im Intersight Managed Mode (IMM) konfiguriert sind. Das Cisco UCS 5108 Gehäuse der B-Serie kann jedoch sowohl im IMM-Modus als auch im UCSM-Managed-Modus unterstützt werden.

Das UCS FI 6324 nutzt den IOM-Formfaktor und ist in ein UCS Mini-Chassis für Implementierungen eingebettet, die nur eine kleine UCS-Domäne erfordern.

UCS Virtual Interface-Karten

Cisco UCS Virtual Interface Cards (VIC) sorgen für einheitliches Systemmanagement und LAN- und SAN-Konnektivität für Rack- und Blade Server. Es unterstützt bis zu 256 virtuelle Geräte, entweder als virtuelle Netzwerkschnittstellenkarten (vNICs) oder als virtuelle Host Bus Adapter (vHBAs) mit der Cisco SingleConnect

Technologie. Durch die Virtualisierung vereinfachen VIC Karten die Netzwerk-Konnektivität erheblich und reduzieren die Anzahl der für die Lösungsimplementierung benötigten Netzwerkadapter, Kabel und Switch Ports. Die folgende Abbildung zeigt einige Cisco UCS VIC für Server der B-Serie und C-Serie und die Computing-Nodes der X-Serie.



Die verschiedenen Adaptermodelle unterstützen verschiedene Blade- und Rack-Server mit unterschiedlichen Port-Anzahlen, Port-Geschwindigkeiten und Formfaktoren für modulare LAN on Motherboard (mLOM), Mezzanine-Karten und PCIe-Schnittstellen. Die Adapter unterstützen einige Kombinationen aus 10/25/40/100-G Ethernet und Fibre Channel over Ethernet (FCoE). Sie integrieren die Cisco Converged Network Adapter (CNA)-Technologie, unterstützen ein umfassendes Funktionsset und vereinfachen das Adaptermanagement und die Bereitstellung von Anwendungen. Der VIC unterstützt beispielsweise die VM-FEX-Technologie (Data Center Virtual Machine Fabric Extender) von Cisco, die die Cisco UCS Fabric Interconnect Ports auf Virtual Machines erweitert und somit die Implementierung der Server-Virtualisierung vereinfacht.

Mit einer Kombination aus Cisco VIC in Konfigurationen für mLOM, Mezzanine und Port Expander und Bridge-Karten können Sie die Bandbreite und Konnektivität der Blade Server voll ausschöpfen. Beispielsweise besteht die kombinierte VIC-Bandbreite 2 x 50-G + 2 x 50-G, indem die beiden 25-G-Links auf dem VIC 14825 (mLOM) und 14425 (Mezzanine) sowie die 14000 (Bridge Card) für den X210c Computing-Node genutzt werden. Oder 100 GB pro Fabric/IFM und 200 G insgesamt pro Server bei dualer IFM-Konfiguration.

Details zu den Cisco UCS-Produktfamilien, technischen Spezifikationen und Dokumentationen finden Sie im "Cisco UCS" Website für Informationen.

Cisco Switching-Komponenten

Nexus Switches

FlexPod verwendet Switches der Cisco Nexus Serie, um ein Ethernet Switching Fabric für die Kommunikation zwischen Cisco UCS und NetApp Storage Controllern bereitzustellen. Für die FlexPod Implementierung werden alle derzeit unterstützten Cisco Nexus Switch Modelle, einschließlich der Cisco Nexus 3000, 5000, 7000 und 9000 Serien, unterstützt.

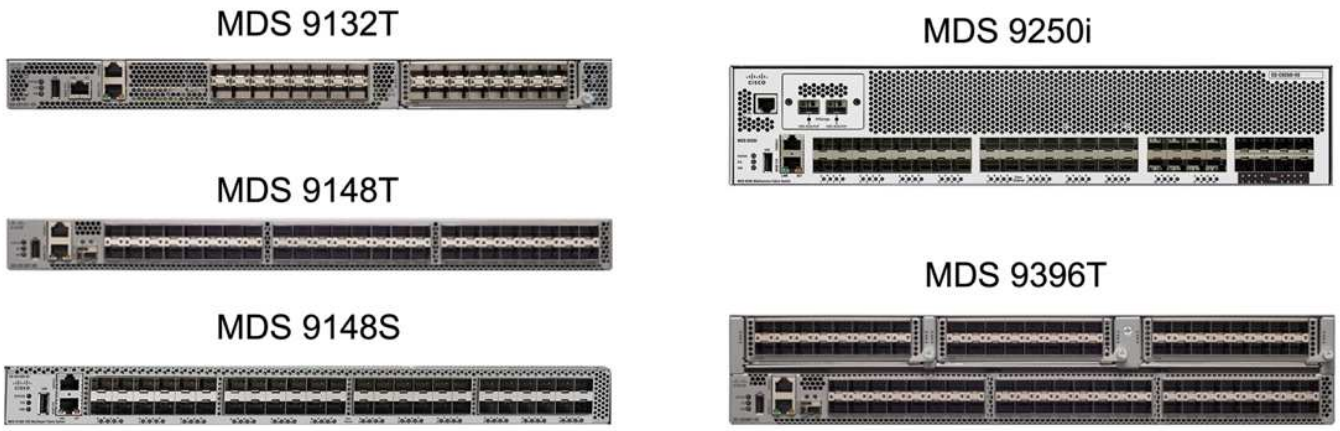
Bei der Auswahl eines Switch-Modells für FlexPod-Implementierungen müssen viele Faktoren berücksichtigt werden, beispielsweise Performance, Port-Geschwindigkeit, Port-Dichte, Switching-Latenz. Und Protokolle wie ACI und VXLAN Unterstützung, für Ihre Designziele sowie für die Unterstützung von Switches.

In der Validierung vieler aktueller FlexPod CVDs werden Switches der Cisco Nexus 9000 Serie wie Nexus 9336C-FX2 und Nexus 93180YC-FX3 verwendet, die eine hohe Performance von 40/100G- und 10/25G-Ports, eine niedrige Latenz und eine außergewöhnliche Energieeffizienz in einem kompakten 1U-Formfaktor bieten. Zusätzliche Geschwindigkeiten werden über Uplink-Ports und Breakout-Kabel unterstützt. Die folgende Abbildung zeigt einige Cisco Nexus 9k- und 3K-Switches, einschließlich des Nexus 9336C-FX2 und des Nexus 3232C-Systems für diese Validierung.

Siehe "Cisco Data Center Switches" Weitere Informationen zu den verfügbaren Nexus Switches und ihren Spezifikationen und Dokumentationen.

MDS-Switches

Die Fabric Switches der Cisco MDS 9100/9200/9300 Serie sind optional Bestandteil der FlexPod Architektur. Diese Switches sind äußerst zuverlässig, hochflexibel und sicher und bieten Sichtbarkeit des Datenflusses in der Fabric. Die folgende Abbildung zeigt einige Beispiele für MDS-Switches, die zum Aufbau redundanter FC-SAN-Fabrics für eine FlexPod-Lösung zur Erfüllung von Applikations- und Geschäftsanforderungen verwendet werden können.



Cisco MDS 9132T/9148T/9396T Hochleistungs-32G-Multilayer-Fabric-Switches sind kostengünstig und extrem zuverlässig, flexibel und skalierbar. Die erweiterten Funktionen für Speichernetzwerke sind leicht zu managen und für eine zuverlässige SAN-Implementierung mit dem gesamten Portfolio der Cisco MDS 9000-Familie kompatibel.

In diese Hardware-Plattform der nächsten Generation sind hochmoderne SAN-Analyse- und

Telemetrierungsfunktionen integriert. Die aus der Überprüfung der Frame-Header extrahierten Telemetriedaten können auf eine Analysevisualisierungsplattform wie den Cisco Data Center Network Manager gestreamt werden. Auch die MDS-Switches unterstützen 16-Gbit-FC, beispielsweise den MDS 9148S, werden in FlexPod unterstützt. Darüber hinaus sind auch Multiservice-MDS-Switches, wie beispielsweise MDS 9250i mit Unterstützung für FCoE- und FCIP-Protokolle neben FC-Protokoll, Teil des FlexPod Lösungsportfolios.

Bei semi-modularen MDS-Switches wie 9132T und 9396T können zusätzliche Port-Erweiterungsmodule und Port-Lizenzen hinzugefügt werden, um zusätzliche Gerätekonnektivität zu unterstützen. Auf den festen Switches wie 9148T können je nach Bedarf weitere Portlizenzen hinzugefügt werden. Diese Flexibilität beim „Pay-as-you-grow“-Modell stellt eine Komponente für Betriebskosten zur Verfügung, mit der sich die Investitionskosten für die Implementierung und den Betrieb einer Switch-basierten MDS-SAN-Infrastruktur verringern lassen.

Siehe "Cisco MDS Fabric Switches" Weitere Informationen zu den verfügbaren MDS Fabric Switches finden Sie im "NetApp IMT" Und "Cisco Hardware- und Software-Kompatibilitätsliste" Erhalten Sie eine vollständige Liste der unterstützten SAN Switches.

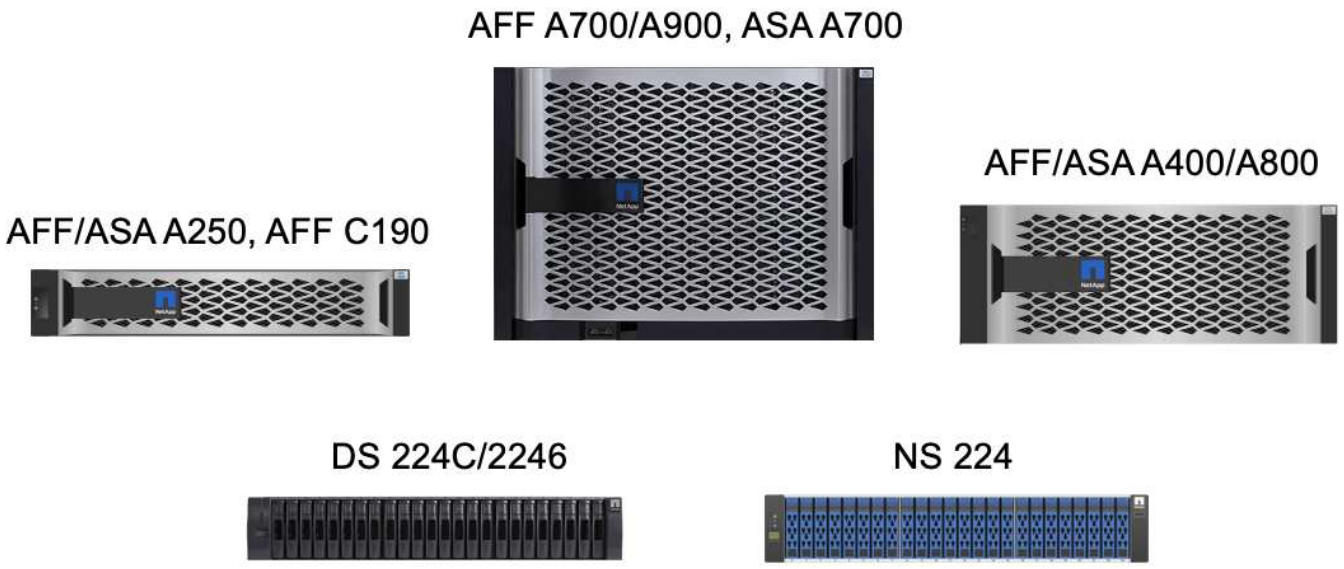
Komponenten von NetApp

Zur Erstellung einer FlexPod SM-BC Lösung sind redundante NetApp AFF oder ASA Controller mit ONTAP Software 9.8 oder neuere Versionen erforderlich. Das aktuelle ONTAP-Release, derzeit 9.10.1, wird für die SM-BC-Implementierung empfohlen, um von den kontinuierlichen ONTAP-Innovationen, Performance- und Qualitätsverbesserungen und der höheren maximalen Anzahl von Objekten für den SM-BC-Support zu profitieren.

NetApp AFF und ASA Controller bieten branchenführende Performance und Innovationen für Datensicherung der Enterprise-Klasse sowie vielseitige Datenmanagementfunktionen. Die AFF und ASA Systeme unterstützen End-to-End-NVMe-Technologien, einschließlich NVMe-Attached SSDs und NVMe over Fibre Channel (NVMe/FC) Front-End-Host-Konnektivität. Mit einer NVMe/FC-basierten SAN-Infrastruktur können Sie den Workload-Durchsatz verbessern und die I/O-Latenz verringern. NVMe/FC-basierte Datastores können jedoch derzeit nur für Workloads genutzt werden, die nicht durch SM-BC geschützt sind, da die SM-BC Lösung derzeit nur iSCSI- und FC-Protokolle unterstützt.

NetApp AFF und ASA Storage-Controller bieten Kunden auch eine Hybrid-Cloud-Grundlage, um von den Vorteilen der nahtlosen Datenmobilität mithilfe der NetApp Data-Fabric-Architektur zu profitieren. Mit Data Fabric lassen sich Daten einfach vom Edge-Bereich in den Core-Bereich verschieben, wo sie verwendet werden, und in die Cloud. So profitieren Sie von den flexiblen On-Demand-Computing- sowie KI- und ML-Funktionen und können damit schneller geschäftliche Einblicke gewinnen.

Wie in der folgenden Abbildung dargestellt, bietet NetApp verschiedene Storage Controller und Festplatten-Shelfs, um Ihre Performance- und Kapazitätsanforderungen zu erfüllen. In der folgenden Tabelle finden Sie Links zu Produktseiten für Informationen zu den Funktionen und Spezifikationen des NetApp AFF und ASA Controllers.

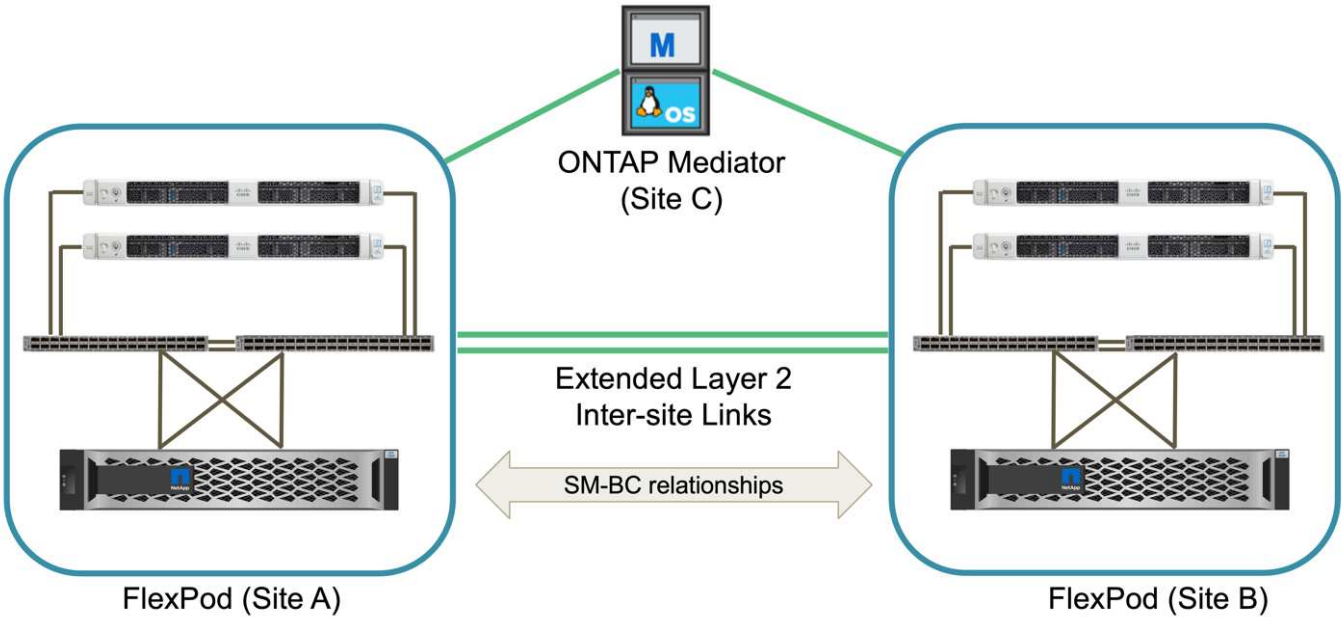


Produktfamilie	Technische Spezifikationen
AFF Serie	"Dokumentation der AFF Serie"
ASA Serie	"Dokumentation der ASA Serie"

Konsultieren Sie die "Dokumentation der Platten-Shelfs und Storage-Medien von NetApp" Und "NetApp Hardware Universe" Weitere Informationen zu den Festplatten-Shelfs und zu unterstützten Platten-Shelfs für jedes Storage-Controller-Modell

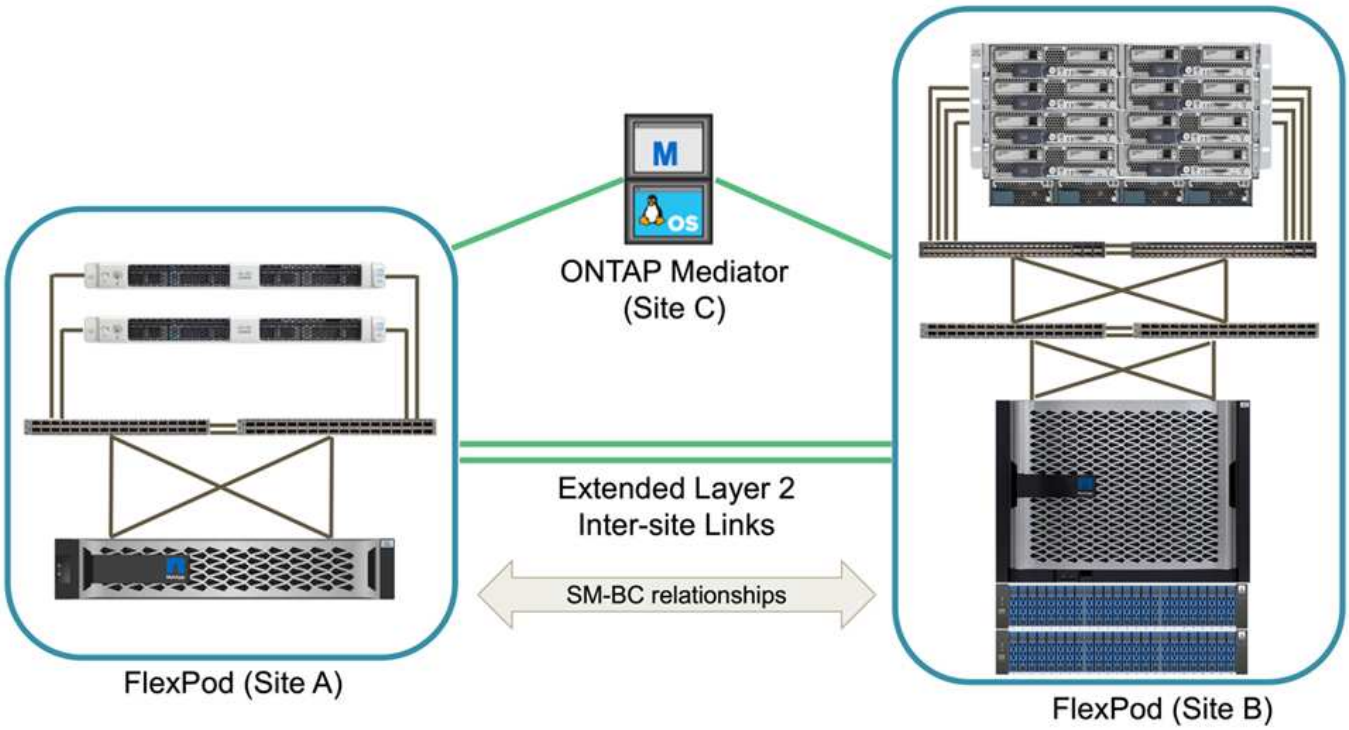
Lösungstopologien

FlexPod Lösungen sind flexibel in der Topologie und lassen sich je nach Anforderungen vertikal oder horizontal skalieren. Eine Lösung, die Business Continuity-Sicherheit erfordert und nur minimale Computing- und Storage-Ressourcen erfordert, kann eine einfache Topologie der Lösung verwenden, wie in der folgenden Abbildung dargestellt. Diese einfache Topologie verwendet Rack-Server der UCS C-Serie und AFF/ASA Controller mit SSDs im Controller ohne zusätzliche Festplatten-Shelfs.



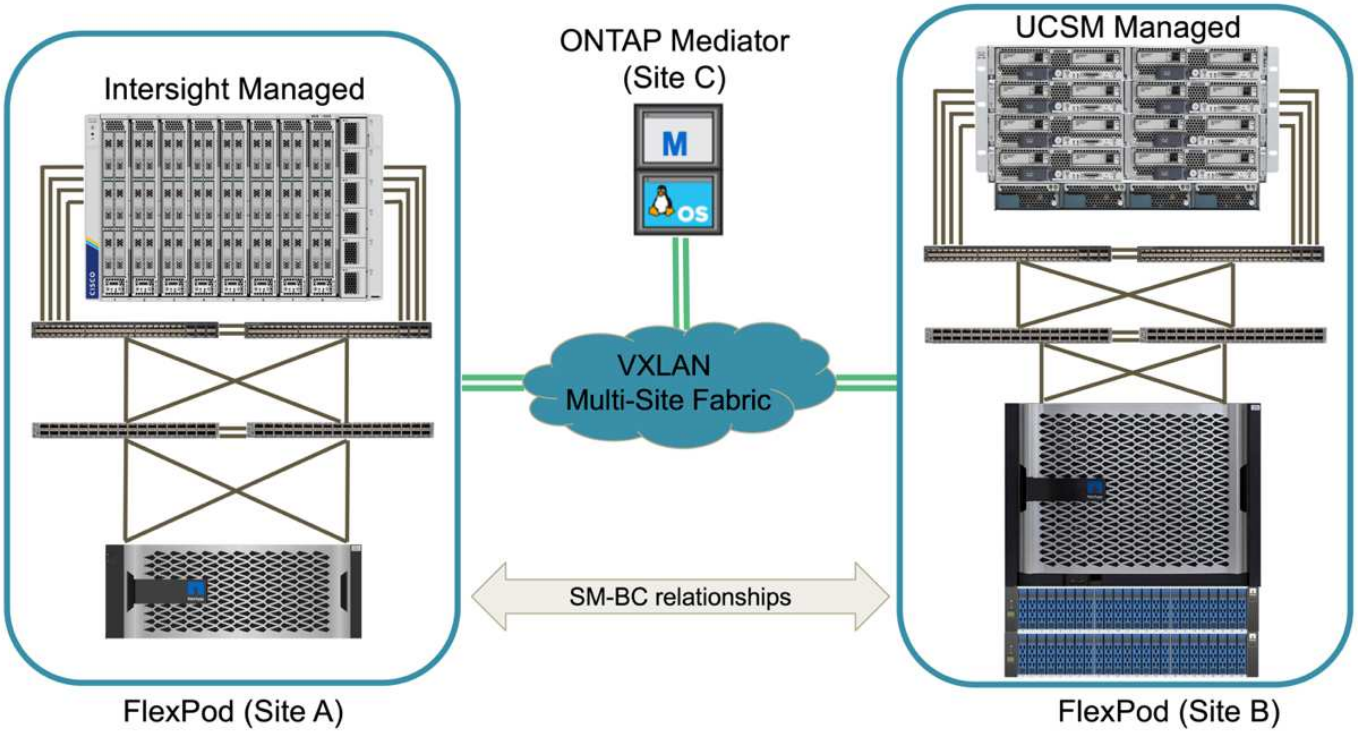
Die redundanten Computing-, Netzwerk- und Storage-Komponenten sind durch die redundante Konnektivität zwischen den Komponenten miteinander verbunden. Dieses hochverfügbare Design bietet eine zuverlässige Lösung, die sich gegen Single Point of Failure-Szenarien aushält. Trotz des standortübergreifenden Designs und der synchronen ONTAP SM-BC Datenreplizierung können geschäftskritische Daten-Services genutzt werden, selbst wenn ein Storage-Ausfall an einem einzigen Standort möglich ist.

Eine asymmetrische Implementierungstopologie, die in Unternehmen zwischen einem Datacenter und einer Niederlassung in einem Großraumgebiet eingesetzt werden kann, könnte wie folgt aussehen: Für dieses asymmetrische Design erfordert das Datacenter ein FlexPod mit höherer Performance und mehr Computing- und Storage-Ressourcen. Die Anforderungen an die Remote-Zweigstelle sind jedoch weniger und können durch eine viel kleinere FlexPod erfüllt werden.

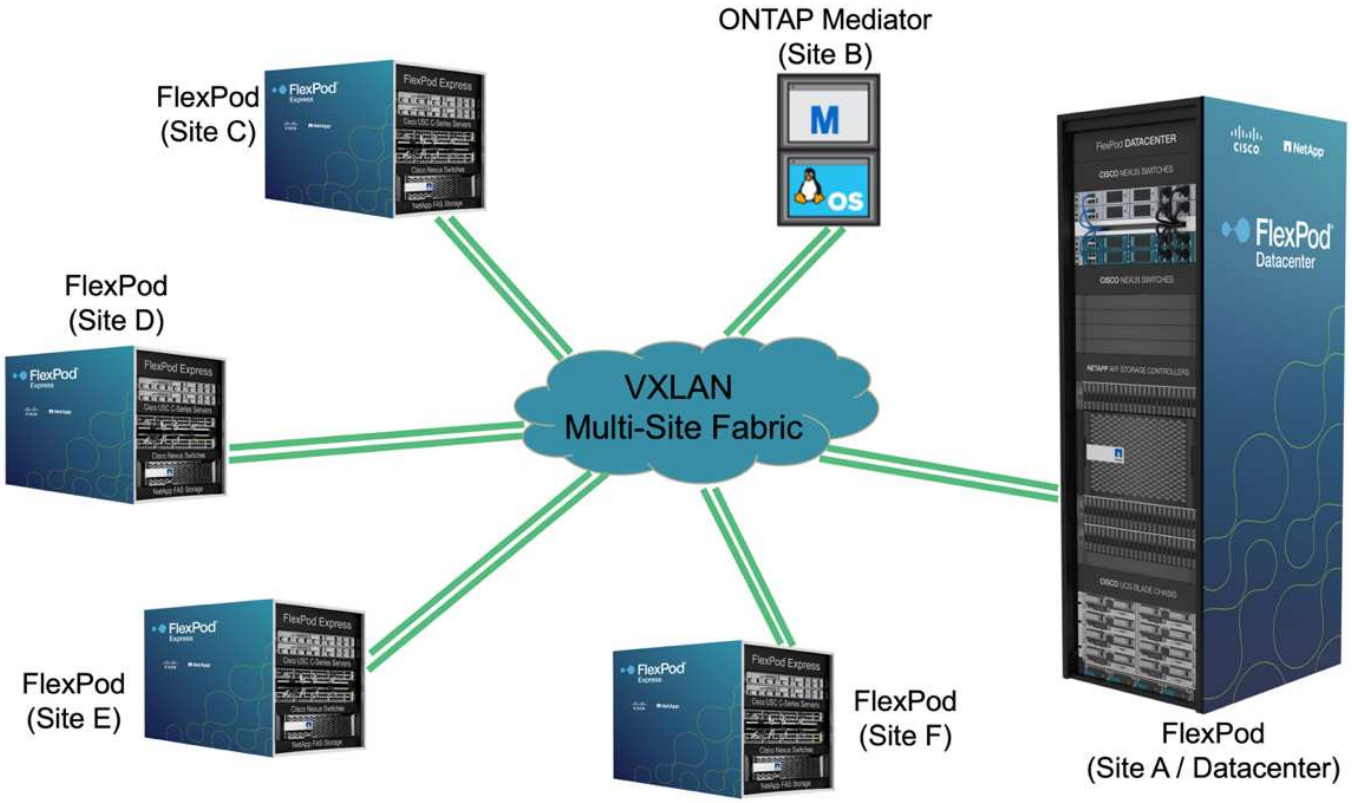


Für Unternehmen mit höheren Anforderungen an Computing- und Storage-Ressourcen und mehreren Standorten verfügt eine VXLAN-basierte Multi-Site-Fabric über eine nahtlose Netzwerk-Fabric-Infrastruktur, die die Applikationsmobilität vereinfacht, sodass eine Applikation von jedem Standort aus bedient werden kann.

Möglicherweise gibt es eine vorhandene FlexPod Lösung mit dem Cisco UCS 5108 Chassis und Blade Servern der B-Serie, die durch eine neue FlexPod Instanz geschützt werden müssen. Die neue FlexPod Instanz nutzt das neueste UCS X9508 Chassis mit X210c Computing Nodes, die von Cisco Intersight gemanagt werden, wie in der folgenden Abbildung dargestellt. In diesem Fall sind die FlexPod Systeme an jedem Standort mit einer größeren Datacenter-Fabric verbunden. Die Standorte sind über ein Interconnect-Netzwerk verbunden und bilden so eine VXLAN Multi-Site Fabric.



Für Unternehmen mit einem Datacenter und mehreren Niederlassungen in einem Großraumgebiet, die alle gesichert werden müssen, um Business Continuity sicherzustellen, Die in der folgenden Abbildung dargestellte FlexPod SM-BC Implementierungstopologie kann implementiert werden, um kritische Applikations- und Datenservices zu sichern und so ein Recovery Point Objective von null und ein Recovery Time Objective von fast null für alle Zweigstellen zu erreichen.



Bei diesem Implementierungsmodell richtet jede Niederlassung die SM-BC-Beziehungen und Consistency Groups ein, die sie für das Datacenter benötigen. Sie müssen die unterstützten SM-BC-Objektgrenzwerte berücksichtigen, sodass die Gesamtwerte für Consistency Group-Beziehungen und Endpunkte die im Datacenter unterstützten Maximalwerte nicht überschreiten.

"Weiter: Übersicht zur Lösungsvalidierung"

Lösungsvalidierung

Lösungsvalidierung – Überblick

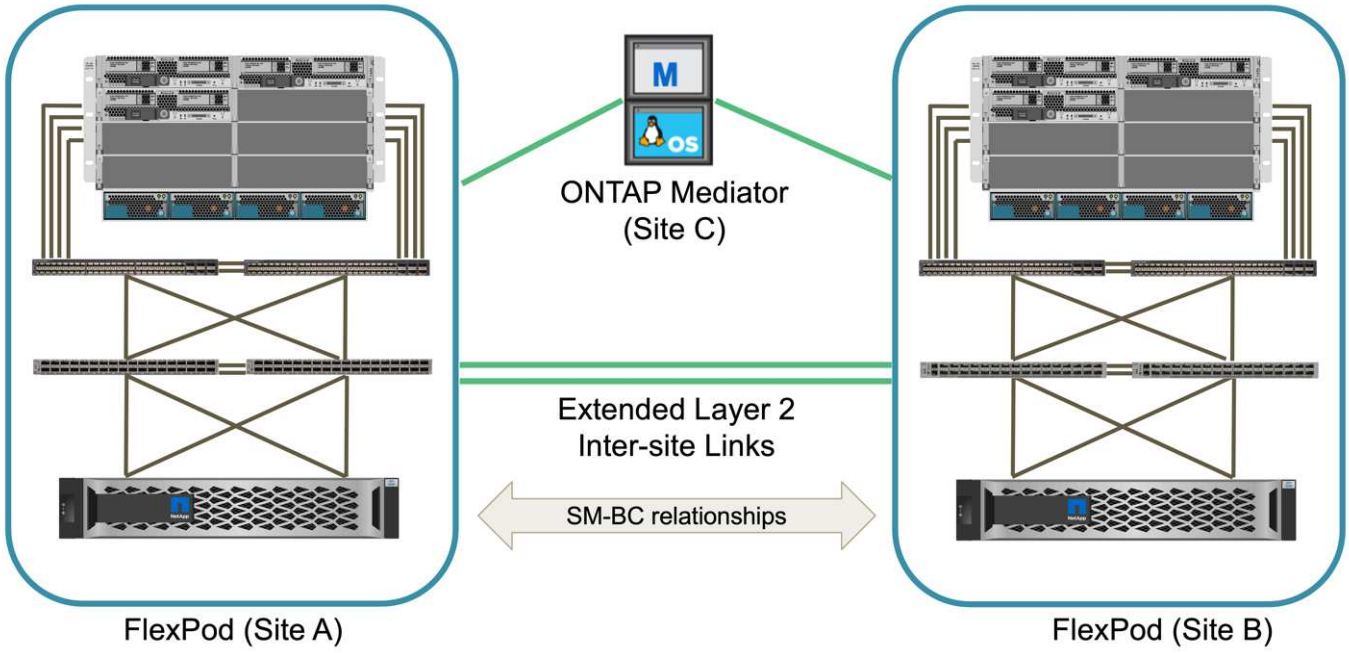
"Früher: FlexPod SM-BC Lösung."

Die Details zum Design und der Implementierung der FlexPod SM-BC Lösung hängen von der jeweiligen Konfiguration der FlexPod-Situation und den jeweiligen Lösungszielen ab. Nach Definition der allgemeinen Business Continuity-Anforderungen kann die FlexPod SM-BC Lösung erstellt werden. Dazu wird eine vollständig neue Lösung mit zwei neuen FlexPod Systemen implementiert, ein neues FlexPod an einem anderen Standort hinzugefügt und mit einem vorhandenen FlexPod gekoppelt oder zwei bestehende FlexPod Systeme verbunden.

Da FlexPod Lösungen in seinen Konfigurationen flexibel sind, können alle unterstützten FlexPod Konfigurationen und Komponenten verwendet werden. Der restliche Abschnitt enthält Informationen zu den Implementierungsprüfungen, die bei einer VMware-basierten virtuellen Infrastrukturlösung durchgeführt werden. Mit Ausnahme der SM-BC bezogenen Aspekte folgt die Implementierung den Standardprozessen des FlexPod Implementierungsauftrages. In den verfügbaren FlexPod CVDs und NVAs finden Sie die jeweiligen Konfigurationen für allgemeine FlexPod-Implementierungsdetails.

Validierungstopologie

Zur Validierung der FlexPod SM-BC Lösung kommen unterstützte Technologiekomponenten von NetApp, Cisco und VMware zum Einsatz. Die Lösung umfasst NetApp AFF A250 HA-Paare mit ONTAP 9.10.1, duale Cisco Nexus 9336C-FX2 Switches an Standort A und duale Cisco Nexus 3232C-Switches am Standort B, Cisco UCS 6454 FIS an beiden Standorten, Und drei Cisco UCS B200 M5 Server an jedem Standort mit VMware vSphere 7.0u2. Sie werden durch UCS Manager und VMware vCenter Server gemanagt. Die folgende Abbildung zeigt die Lösungstopologie auf Komponentenebene mit zwei FlexPod-Systemen, die an Standort A und Standort B ausgeführt werden. Sie sind über erweiterte Layer-2-Verbindungen zwischen Standorten und ONTAP Mediator verbunden, der an Standort C ausgeführt wird



Hardware- und Software-Suite von NetApp

In der folgenden Tabelle sind die für die Lösungsvalidierung verwendete Hardware und Software aufgeführt. Es ist wichtig zu beachten, dass Cisco, NetApp und VMware über Interoperabilitätsmatrixe verfügen, die zur Bestimmung des Supports für jede spezifische Implementierung von FlexPod eingesetzt werden:

- "http://support.netapp.com/matrix/"
- "Cisco UCS Hardware and Software Interoperability Tool"
- "http://www.vmware.com/resources/compatibility/search.php"

Kategorie	Komponente	Softwareversion	Menge
Computing	Cisco UCS Fabric Interconnect 6454	4.2 (1f)	4 (2 pro Standort)
	Cisco UCS B200 M5 Server	4.2 (1f)	6 (3 pro Standort)
	CISCO UCS IOM 2204XP	4.2 (1f)	4 (2 pro Standort)
	CISCO VIC 1440 (PID: UCSB-MLOM-40G-04)	5.2 (1a)	2 (1 pro Standort)

Kategorie	Komponente	Softwareversion	Menge
	CISCO VIC 1340 (PID: UCSB-MLOM-40G-03)	4.5 (1a)	4 (2 pro Standort)
Netzwerk	Cisco Nexus 9336C-FX2	9.3 (6)	2 (Standort A)
	Cisco Nexus 3232C	9.3 (6)	2 (Standort B)
Storage	NetApp AFF A250	9.10.1	4 (2 pro Standort)
	NetApp System Manager	9.10.1	2 (1 pro Standort)
	NetApp Active IQ Unified Manager	9.10	1
	NetApp ONTAP Tools für VMware vSphere	9.10	1
	NetApp SnapCenter Plug-in für VMware vSphere	4.6	1
	NetApp ONTAP Mediator	1.3	1
	NAbox	3.0.2	1
	NetApp Harvest	21.11.1-1	1
Einheitliche	VMware ESXi	7,0U2	6 (3 pro Standort)
	VMware ESXi Nenic Ethernet-Treiber	1.0.35.0	6 (3 pro Standort)
	VMware vCenter	7,0U2	1
	NetApp NFS Plug-in für VMware VAAI	2.0	6 (3 pro Standort)
Tests	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 pro Standort)
	Iometer	1.1.0	6 (3 pro Standort)

"Als Nächstes: Lösungsvalidierung – Computing."

Lösungsvalidierung – Computing

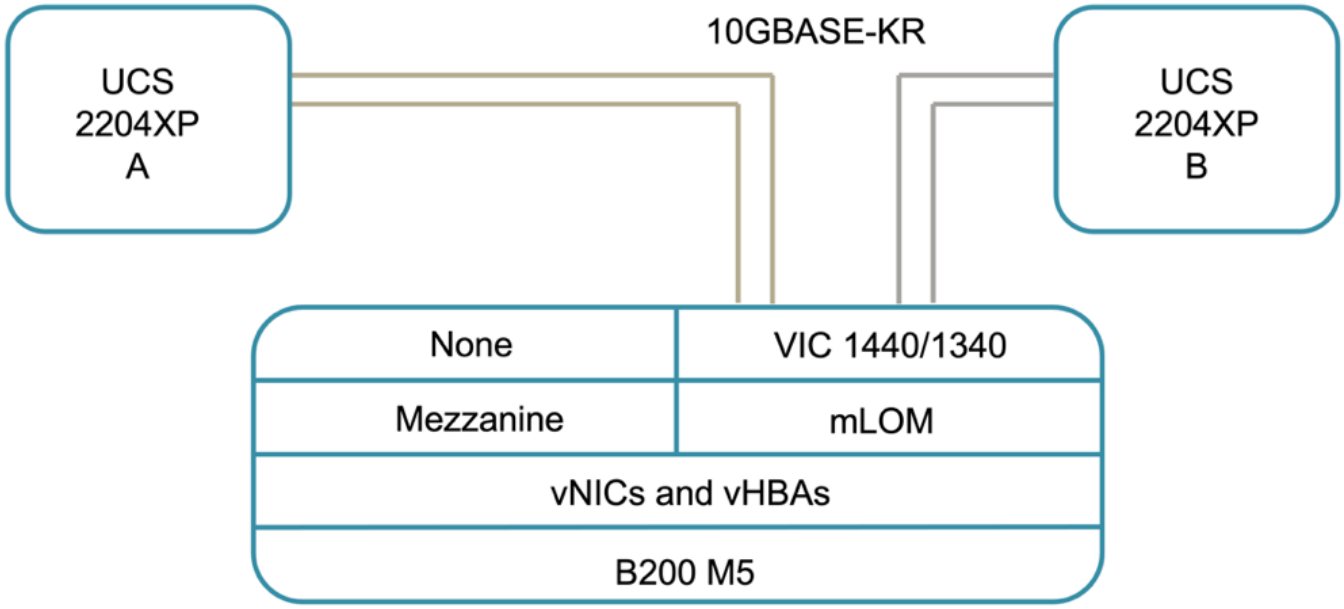
"Preiiwous: Lösungsvalidierung – Überblick."

Die Computing-Konfiguration für die FlexPod SM-BC-Lösung folgt den typischen Best Practices der FlexPod Lösung. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt. Einige Punkte, die im Zusammenhang mit SM-BC zu berücksichtigen sind, geben auch

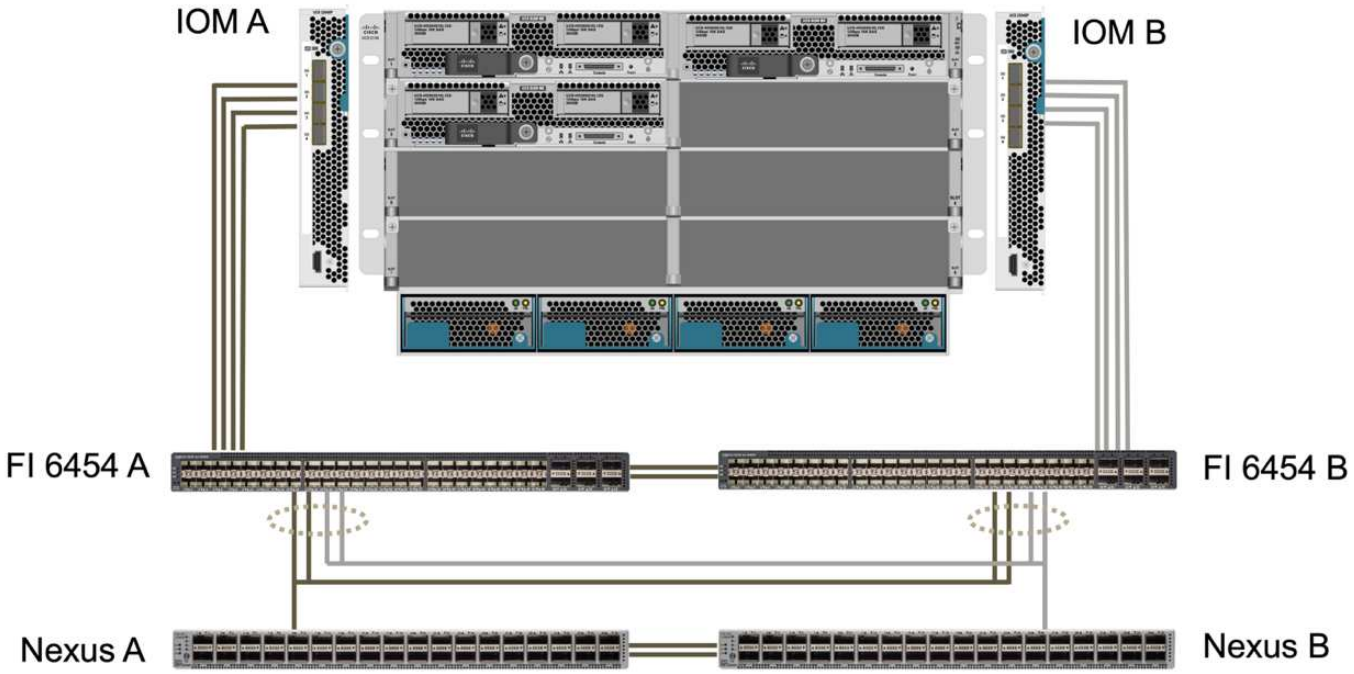
Implementierungsreferenzen und -Anleitungen an.

Konnektivität

Die Konnektivität zwischen den UCS B200 Blade Servern und den IOMs wird durch die UCS VIC-Karte über die UCS 5108 Gehäuse-Backplane-Verbindungen bereitgestellt. Die für die Validierung verwendeten UCS 2204XP Fabric Extender verfügen über sechzehn 10G-Ports, um sich mit den acht Blade Servern mit halber Breite zu verbinden, z. B. zwei für jeden Server. Zur Erhöhung der Server-Konnektivitätsbandbreite kann ein zusätzlicher Mezzanine-basierter VIC hinzugefügt werden, um den Server mit dem alternativen UCS 2408 IOM zu verbinden, das vier 10G-Verbindungen zu jedem Server bietet.



Die Konnektivität zwischen dem UCS 5108 Gehäuse und dem für die Validierung verwendeten UCS 6454 FIS wird durch das IOM 2204XP bereitgestellt, welches vier 10G-Verbindungen verwendet. Die FI-Ports 1 bis 4 sind als Serveranschlüsse für diese Verbindungen konfiguriert. Die FI-Ports 25 bis 28 sind als Netzwerk-Uplink-Ports zum Nexus-Switch A und B am lokalen Standort konfiguriert. Die folgende Abbildung und Tabelle enthalten das Konnektivitätsdiagramm und die Details zur Port-Verbindung, mit denen UCS 6454 FIS eine Verbindung zum UCS 5108-Chassis und den Nexus-Switches herstellen kann.



Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
UCS 6454 FI A	1	IOM A	1
	2		2
	3		3
	4		4
	25	Nexus A	1/13/1
	26		1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus A	1/13/3
	26		1/13/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
	L2		L2

Die obigen Verbindungen sind für beide Standorte A und B ähnlich, trotz Standort A mit Nexus 9336C-FX2Switches und Standort B mit Nexus 3232C-Switches. Breakout-Kabel von 40G bis 4X10G werden für den Nexus für FI-Verbindungen verwendet. Die FI-Verbindungen zu Nexus nutzen Port-Channel und virtuelle Port-Kanäle sind auf den Nexus-Switches konfiguriert, um die Verbindungen zu jedem FI aggregieren.

Wenn Sie eine andere Kombination aus IOM, FI und Nexus Switch-Komponenten verwenden, achten Sie bei der Kombination der Umgebung auf die entsprechenden Kabel und die Port-Geschwindigkeit.

Zusätzliche Bandbreite lässt sich durch Komponenten erreichen, die Verbindungen mit höherer Geschwindigkeit oder mehr Verbindungen unterstützen. Zusätzliche Redundanz lässt sich durch Hinzufügen weiterer Verbindungen mit Komponenten erreichen, die diese unterstützen.

Serviceprofile

Ein Blade Server Chassis mit Fabric Interconnects, das von UCS Manager (UCSM) oder Cisco Intersight gemanagt wird, kann die Server durch Nutzung von Service-Profilen abstrahieren, die in UCSM und Server-Profilen in Intersight verfügbar sind. Diese Validierung nutzt UCSM und Serviceprofile, um das Server Management zu vereinfachen. Mithilfe von Serviceprofilen können Sie einen Server einfach durch die Verknüpfung des ursprünglichen Serviceprofils mit der neuen Hardware ersetzen oder aktualisieren.

Die erstellten Serviceprofile unterstützen für VMware ESXi Hosts Folgendes:

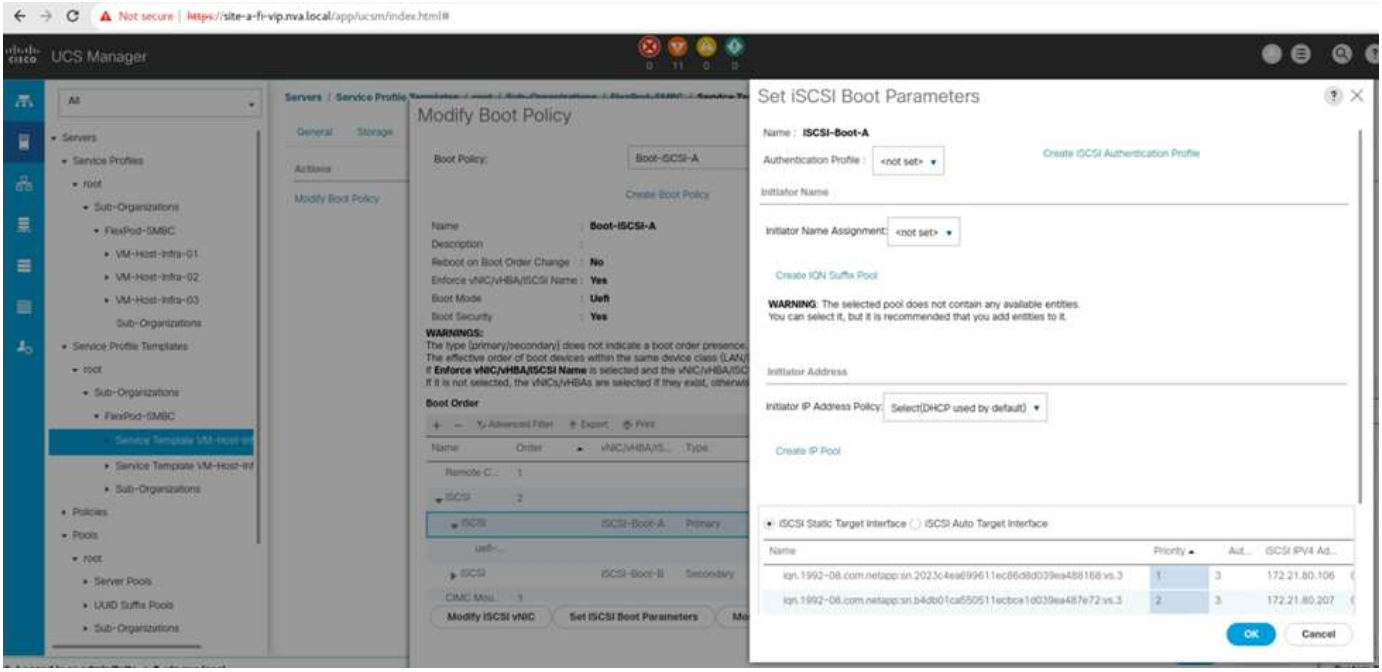
- SAN startet über den AFF A250-Storage an beiden Standorten mit iSCSI-Protokoll.
- Sechs vNICs werden für die Server erstellt, in denen:
  - Zwei redundante vNICs (vSwitch0-A und vSwitch0-B) tragen den in-Band-Management-Traffic. Optional können diese vNICs auch mit NFS-Protokolldaten verwendet werden, die nicht durch SM-BC geschützt sind.
  - Zwei redundante vNICs (VdS-A und VdS-B) werden vom vSphere Distributed Switch verwendet, um VMware vMotion und anderen Applikationsdatenverkehr zu transportieren.
  - ISCSI-A vNIC verwendet von iSCSI-A vSwitch, um Zugriff auf iSCSI-A-Pfad zu bieten.
  - ISCSI-B vNIC, die von iSCSI-B vSwitch verwendet wird, um Zugriff auf den iSCSI-B-Pfad zu ermöglichen.

SAN Booting

Für die iSCSI-SAN-Startkonfiguration sind die iSCSI-Startparameter so eingestellt, dass iSCSI von beiden iSCSI-Fabrics aus gestartet werden kann. Um das SM-BC Failover-Szenario unterzubringen, in dem ein iSCSI SAN Boot LUN vom sekundären Cluster bereitgestellt wird, wenn das primäre Cluster nicht verfügbar ist, sollte die statische iSCSI-Zielkonfiguration Ziele sowohl von Standort A als auch von Standort B umfassen Um die Boot-LUN-Verfügbarkeit zu maximieren, konfigurieren Sie darüber hinaus die iSCSI-Boot-Parameter-Einstellungen, damit sie von allen Storage Controllern gebootet werden können.

Das statische iSCSI-Ziel kann in der Boot-Policy der Service-Profile-Vorlagen unter dem Dialogfeld Set iSCSI Boot Parameter konfiguriert werden, wie in der folgenden Abbildung dargestellt. Die empfohlene Konfiguration für den iSCSI-Boot-Parameter ist in der folgenden Tabelle dargestellt, welche die oben beschriebene Boot-

Strategie implementiert, um eine hohe Verfügbarkeit zu erreichen.



ISCSI Fabric	Priorität	ISCSI-Ziel	ISCSI LIF
ISCSI A	1	ISCSI-Ziel Standort A	Standort A Controller 1 iSCSI A LIF
	2	ISCSI-Ziel Standort B	Standort B Controller 2 iSCSI A LIF
ISCSI B	1	ISCSI-Ziel Standort B	Standort B Controller 1 iSCSI B LIF
	2	ISCSI-Ziel Standort A	Standort A Controller 2 iSCSI B LIF

"Weiter: Lösungsvalidierung – Netzwerk."

Lösungsvalidierung – Netzwerk

"Früher: Lösungsvalidierung – Computing."

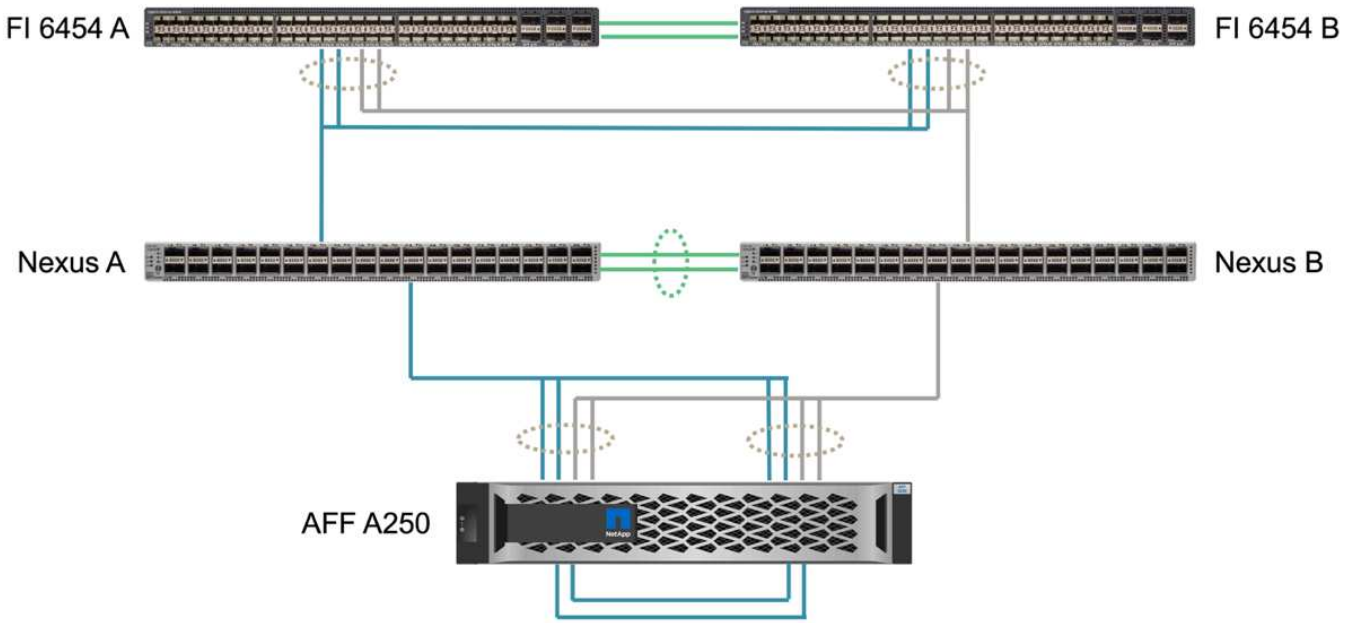
Die Netzwerkkonfiguration für die FlexPod SM-BC Lösung folgt an jedem Standort den typischen Best Practices der FlexPod Lösung. Für die Konnektivität zwischen Standorten werden die FlexPod Nexus Switches an beiden Standorten über die Lösungsvalidierung miteinander verbunden. So wird für Verbindungen zwischen den Standorten zwischen den beiden Standorten hergestellt, was die VLANs zwischen den beiden Standorten erweitert. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt.

Konnektivität

Die FlexPod Nexus Switches an jedem Standort sorgen in einer hochverfügbaren Konfiguration für die lokale Konnektivität zwischen UCS Computing und ONTAP Storage. Die redundanten Komponenten und die

redundante Konnektivität bieten die Ausfallsicherheit bei Single-Point-of-Failure-Szenarien.

Das folgende Diagramm zeigt die lokale Konnektivität von Nexus Switch an den einzelnen Standorten. Neben den im Diagramm dargestellten Informationen gibt es für jede Komponente auch Konsolen- und Management-Netzwerkverbindungen. Die 40G bis 4 x 10G-Breakout-Kabel werden zur Verbindung der Nexus-Switches mit dem UCS FIS und den ONTAP AFF A250 Storage Controllern verwendet. Alternativ können Sie mit den 100 G bis 4 x 25 G Breakout Kabeln die Kommunikationsgeschwindigkeit zwischen den Nexus Switches und den AFF A250 Storage Controllern erhöhen. Zur Vereinfachung werden die beiden AFF A250-Controller zur Verkabelungsabbildung logisch nebeneinander dargestellt. Dank der beiden Verbindungen zwischen den beiden Storage Controllern kann der Storage ein Cluster ohne Switches bilden.

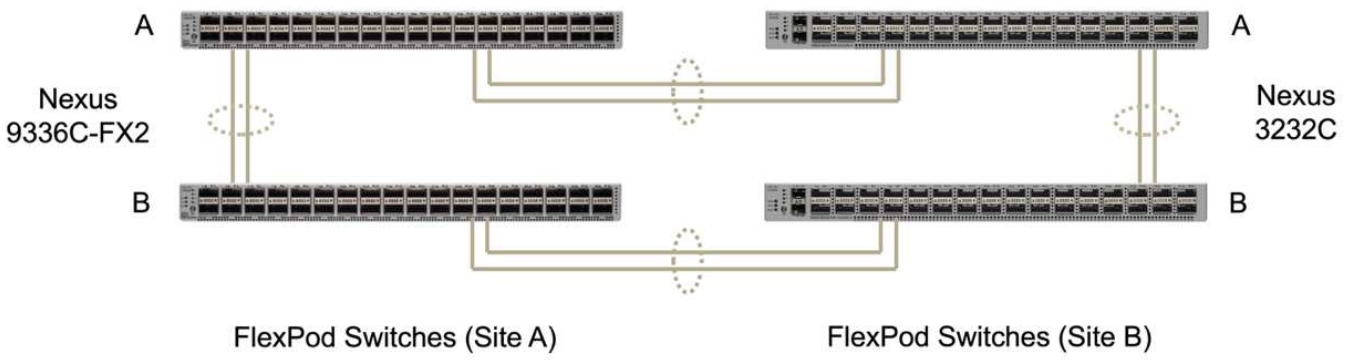


Die folgende Tabelle zeigt die Konnektivität zwischen Nexus Switches und AFF A250 Storage-Controllern an jedem Standort.

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Nexus A	1/10/1	AFF A250 A	e1a
	1/10/2		e1b
	1/10/3	AFF A250 B	e1a
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B	e1c
	1/10/4		e1d

Die Konnektivität zwischen den FlexPod-Switches an Standort A und Standort B ist in der folgenden Abbildung dargestellt. Die entsprechende Verkabelung ist in der Tabelle aufgeführt. Die Verbindungen zwischen den beiden Switches an jedem Standort gelten für die vPC-Peer-Links. Auf der anderen Seite stellen die Verbindungen zwischen den Switches über die Standorte hinweg die Verbindungen zwischen den Standorten dar. Die Links erweitern die VLANs auf mehrere Standorte für Cluster-übergreifende Kommunikation, SM-BC

Datenreplizierung, in-Band-Management und Datenzugriff für die Ressourcen des Remote-Standorts.



Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Standort A Schalter A	33	Schalter A Standort B	31
	34		32
	25	Standort A Schalter B	25
	26		26
Standort A Schalter B	33	Schalter B an Standort B	31
	34		32
	25	Standort A Schalter A	25
	26		26
Schalter A Standort B	31	Standort A Schalter A	33
	32		34
	25	Schalter B an Standort B	25
	26		26
Schalter B an Standort B	31	Standort A Schalter B	33
	32		34
	25	Schalter A Standort B	25
	26		26

In der Tabelle oben ist die Konnektivität aus der Perspektive jedes FlexPod Switches aufgeführt. Die Tabelle enthält daher doppelte Informationen zur Lesbarkeit.

Port Channel und virtueller Port Channel

Port Channel ermöglicht die Link-Aggregation mithilfe des Link Aggregation Control Protocol (LACP) für Bandbreitenaggregation und Ausfallsicherheit bei Link-Ausfällen. Über den virtuellen Port-Kanal (vPC) können die Port-Channel-Verbindungen zwischen zwei Nexus-Switches logisch als eine angezeigt werden. Dadurch wird die Ausfallsicherheit bei Szenarien wie dem Ausfall einer einzelnen Verbindung oder eines Single Switch noch weiter verbessert.

Der UCS Server-Datenverkehr zum Storage nimmt Pfade Von IOM A zu FI A und IOM B zu FI B vor dem Erreichen der Nexus-Switches. Da DIE FI-Verbindungen zu Nexus Switches auf DER FI-Seite Port Channel und der virtuelle Port Channel auf der Nexus Switch-Seite nutzen, kann der UCS Server Pfade über beide Nexus Switches effektiv nutzen und gegen Single Point-of-Failure-Szenarien überleben. Zwischen den beiden Standorten sind die Nexus Switches miteinander verbunden, wie in der vorherigen Abbildung dargestellt. Je zwei Links können die Switch-Paare zwischen den Standorten verbunden werden, und sie verwenden zudem eine Port-Channel-Konfiguration.

Die Konnektivität zwischen in-Band-Management, Clustern und iSCSI/NFS Daten-Storage-Protokollen wird bereitgestellt, indem die Storage-Controller an jedem Standort in einer redundanten Konfiguration mit den lokalen Nexus-Switches verbunden werden. Jeder Storage-Controller ist mit zwei Nexus-Switches verbunden. Die vier Verbindungen werden als Teil einer Schnittstellengruppe auf dem Storage konfiguriert, um die Ausfallsicherheit zu erhöhen. Beim Nexus Switch sind diese Ports auch Teil eines vPC zwischen den Switches.

In der folgenden Tabelle sind die Port-Channel-ID und die Port-Nutzung an jedem Standort aufgeführt.

Port-Kanal-ID	Zu Verwenden
10	Lokale Nexus Peer-Verbindung
15	Fabric Interconnect A-Links
16	Fabric Interconnect B-Links
27	Storage Controller A-Links
28	Storage Controller B-Links
100	Wechseln Sie zwischen den Standorten A-Links
200	Switch B-Links zwischen Standorten

VLANs

In der folgenden Tabelle sind für das Einrichten der Validierungsumgebung der FlexPod SM-BC-Lösung und ihrer Verwendung konfigurierte VLANs aufgeführt.

Name	VLAN-ID	Zu Verwenden
Natives VLAN	2	VLAN 2 wird als natives VLAN statt Standard-VLAN verwendet (1)
OOB-MGMT-VLAN	3333	Out-of-Band-Management-VLAN für Geräte
IB-MGMT-VLAN	3334	In-Band-Management-VLAN für ESXi Hosts, VM Management usw.
NFS-VLAN	3335	Optionales NFS VLAN für NFS-Verkehr
ISCSI-A-VLAN	3336	ISCSI-A Fabric-VLAN für iSCSI-Datenverkehr
ISCSI-B-VLAN	3337	ISCSI-B Fabric-VLAN für iSCSI-Datenverkehr
VMotion-VLAN	3338	VMware vMotion Traffic VLAN
VM-Traffic – VLAN	3339	VMware VM Traffic VLAN

Name	VLAN-ID	Zu Verwenden
Intercluster-VLAN	3340	Intercluster-VLAN für ONTAP Cluster Peer Communications

SM-BC unterstützt zwar keine NFS- oder CIFS-Protokolle für Business Continuity, Sie können diese jedoch auch für Workloads einsetzen, die nicht zur Gewährleistung der Business Continuity gesichert werden müssen. NFS-Datastores wurden für diese Validierung nicht erstellt.

"Weiter: Lösungsvalidierung – Storage."

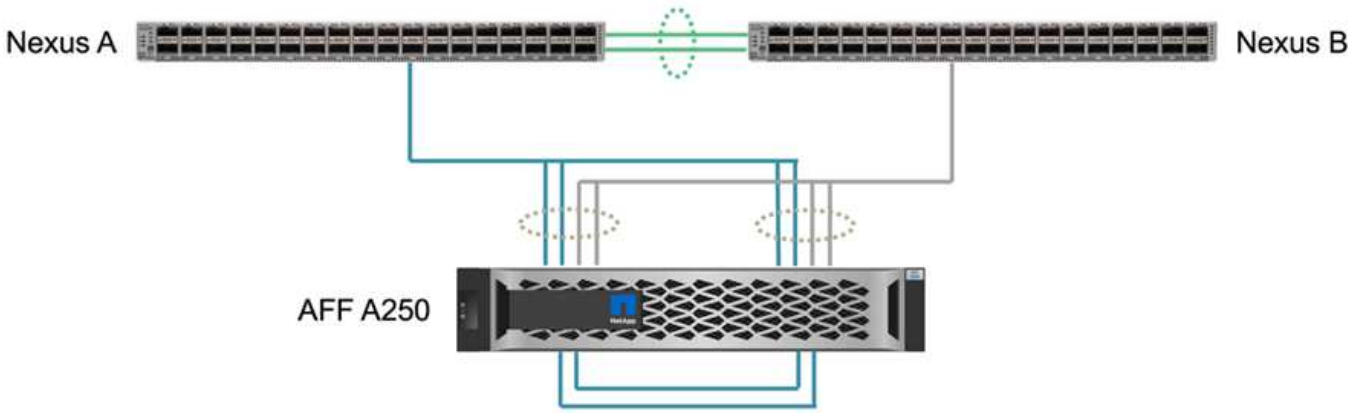
Lösungsvalidierung: Storage

"Zurück: Lösungsvalidierung - Netzwerk."

Die Storage-Konfiguration für die FlexPod SM-BC Lösung folgt den typischen Best Practices der FlexPod Lösung an jedem Standort. Für SM-BC Cluster-Peering und Datenreplizierung verwenden sie die Verbindungen zwischen den Standorten, die zwischen den FlexPod Switches an beiden Standorten hergestellt wurden. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt.

Konnektivität

Die Storage-Konnektivität mit den lokalen UCS FIS- und Blade-Servern wird von den Nexus Switches am lokalen Standort bereitgestellt. Durch die Nexus Switch-Konnektivität zwischen Standorten kann auch von den Remote UCS Blade Servern auf den Storage zugegriffen werden. Die folgende Abbildung und Tabelle zeigen das Storage-Konnektivitätsdiagramm und eine Liste der Verbindungen für die Storage-Controller an jedem Standort.



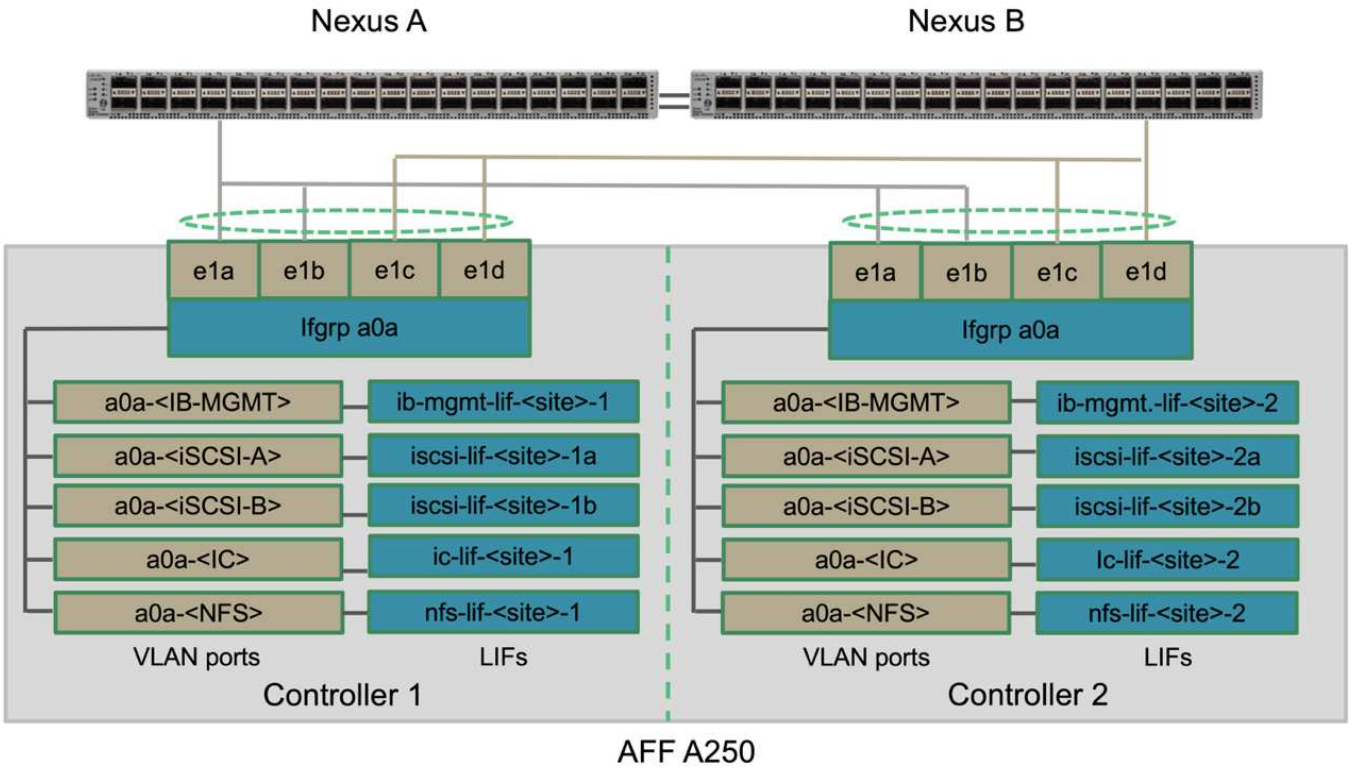
Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A	1/10/1
	e1b		1/10/2

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

Verbindungen und Schnittstellen

Zwei physische Ports an jedem Storage-Controller sind für diese Validierung mit jedem Nexus-Switch verbunden, um die Bandbreitenaggregation und Redundanz zu gewährleisten. Diese vier Verbindungen nehmen an einer Schnittstellengruppenkonfiguration auf dem Speicher Teil. Die entsprechenden Ports auf den Nexus Switches teilen sich für die Link-Aggregation und Ausfallsicherheit in einem vPC.

Die Storage-Protokolle für das in-Band-Management, Cluster-übergreifende und NFS/iSCSI-Daten verwenden VLANs. VLAN-Ports werden auf der Interface Group erstellt, um die verschiedenen Arten von Datenverkehr zu trennen. Logische Schnittstellen (LIFs) für die jeweiligen Funktionen werden auf den entsprechenden VLAN-Ports erstellt. Die folgende Abbildung zeigt die Beziehung zwischen den physischen Verbindungen, Schnittstellengruppen, VLAN-Ports und logischen Schnittstellen.

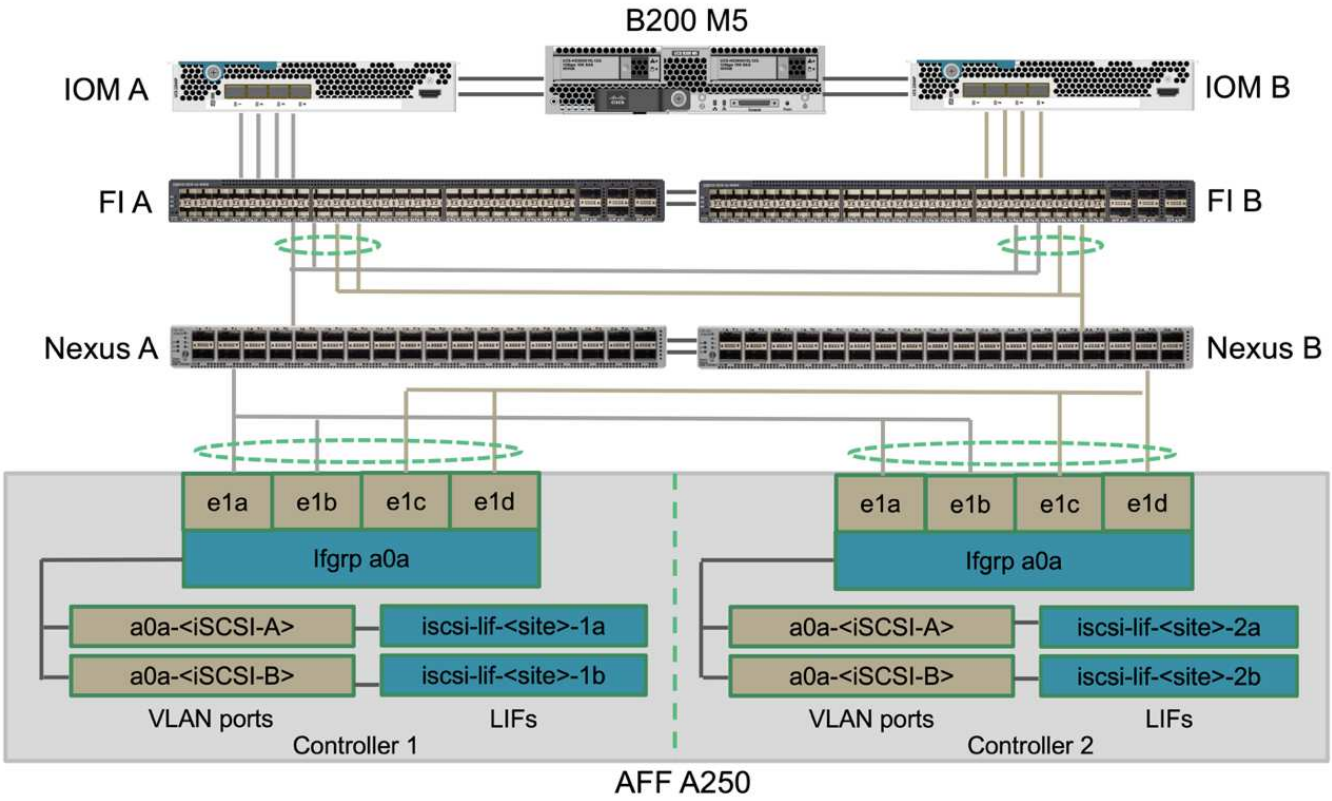


SAN Booting

NetApp empfiehlt, SAN-Boot für die Cisco UCS Server in der FlexPod Lösung zu implementieren. Die Implementierung von SAN Boot ermöglicht die sichere Sicherung des Betriebssystems im NetApp Storage-System und bietet höhere Performance und Flexibilität. Für diese Lösung wurde iSCSI SAN-Boot validiert.

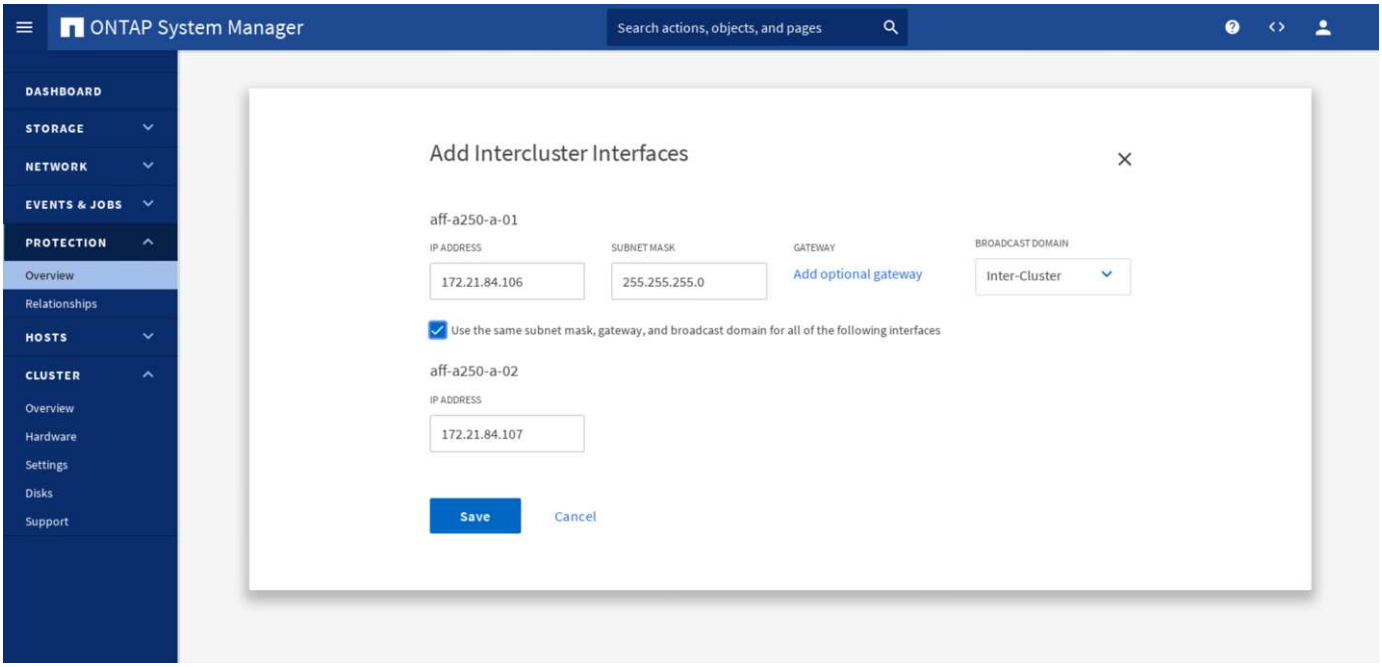
Die folgende Abbildung zeigt die Konnektivität für das iSCSI-SAN-Booten des Cisco UCS Servers aus NetApp Storage. Bei iSCSI SAN Boot wird jedem Cisco UCS Server zwei iSCSI vNICs zugewiesen (einer für jede SAN-Fabric), die redundante Konnektivität vom Server bis zum Storage bieten. Die 10/25-G Ethernet Storage Ports, die mit den Nexus Switches verbunden sind (in diesem Beispiel e1a, e1b, e1c und e1d), werden zu einer Interface Group (ifgrp) (in diesem Beispiel, a0a) gruppiert. Die iSCSI VLAN-Ports werden auf dem ifgrp erstellt, und die iSCSI LIFs werden auf den iSCSI VLAN-Ports erstellt.

Jede iSCSI-Boot-LUN wird dem Server zugeordnet, der von ihm über die iSCSI-LIFs bootet, indem die Boot-LUN mit den iSCSI-qualifizierten Namen (IQNs) des Servers in seiner Boot-Initiatorgruppe verknüpft wird. Die Boot-iGroup des Servers enthält zwei IQNs, eine für jede vNIC / SAN-Fabric. Mit dieser Funktion kann nur der autorisierte Server auf die speziell für diesen Server erstellte Boot-LUN zugreifen.



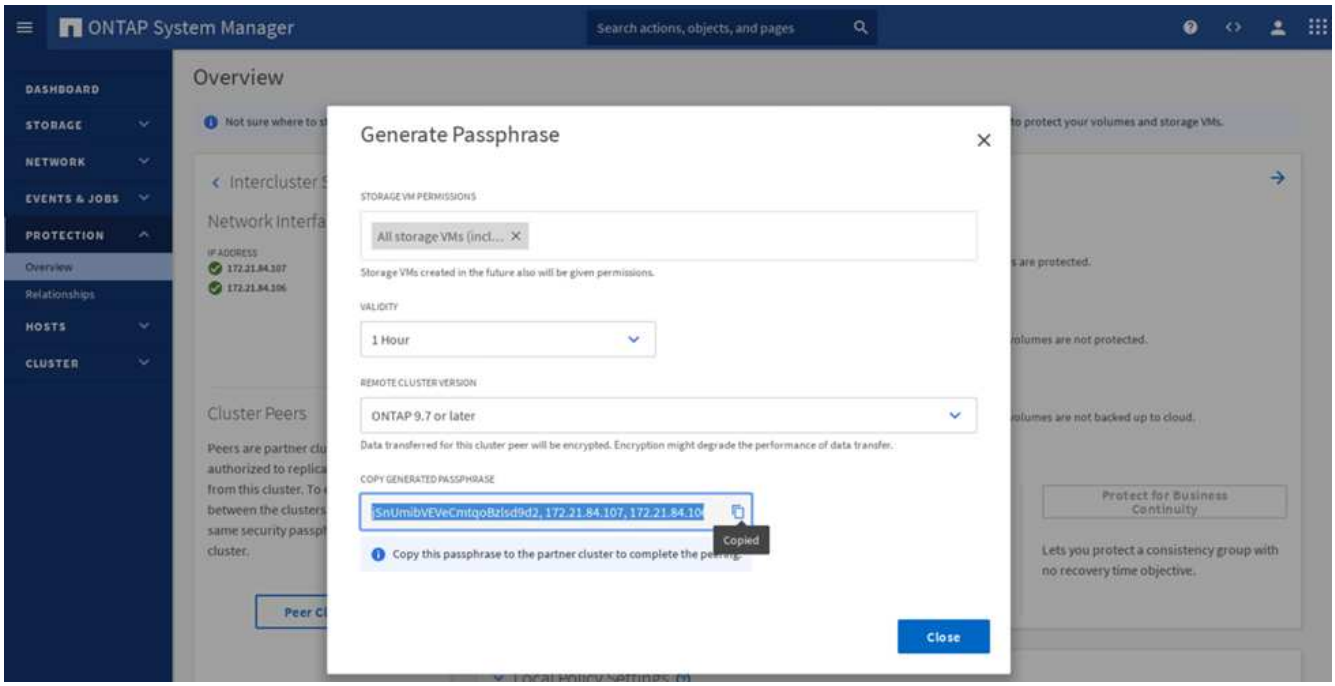
Cluster-Peering

ONTAP Cluster Peers kommunizieren über die Intercluster LIFs. Mit ONTAP System Manager für die beiden Cluster können Sie im Teilfenster „Schutz“ > „Übersicht“ die erforderlichen Intercluster-LIFs erstellen.

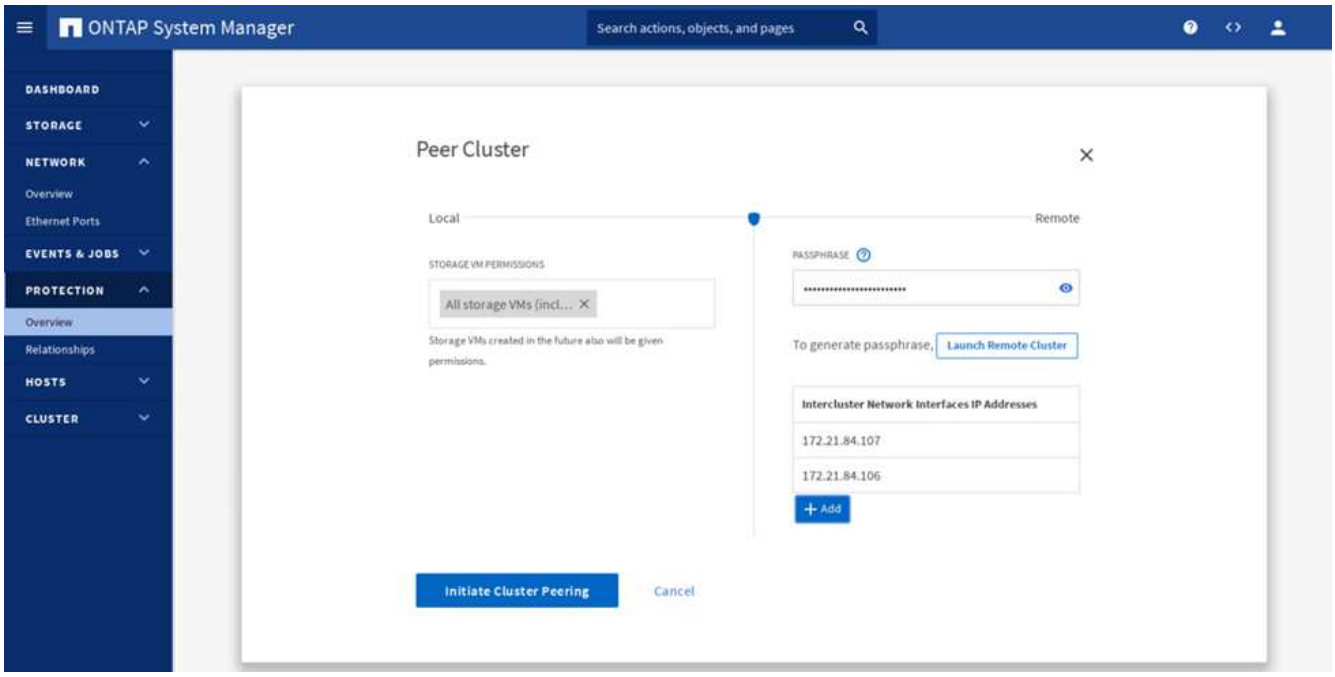


Gehen Sie wie folgt vor, um die beiden Cluster miteinander zu verbinden:

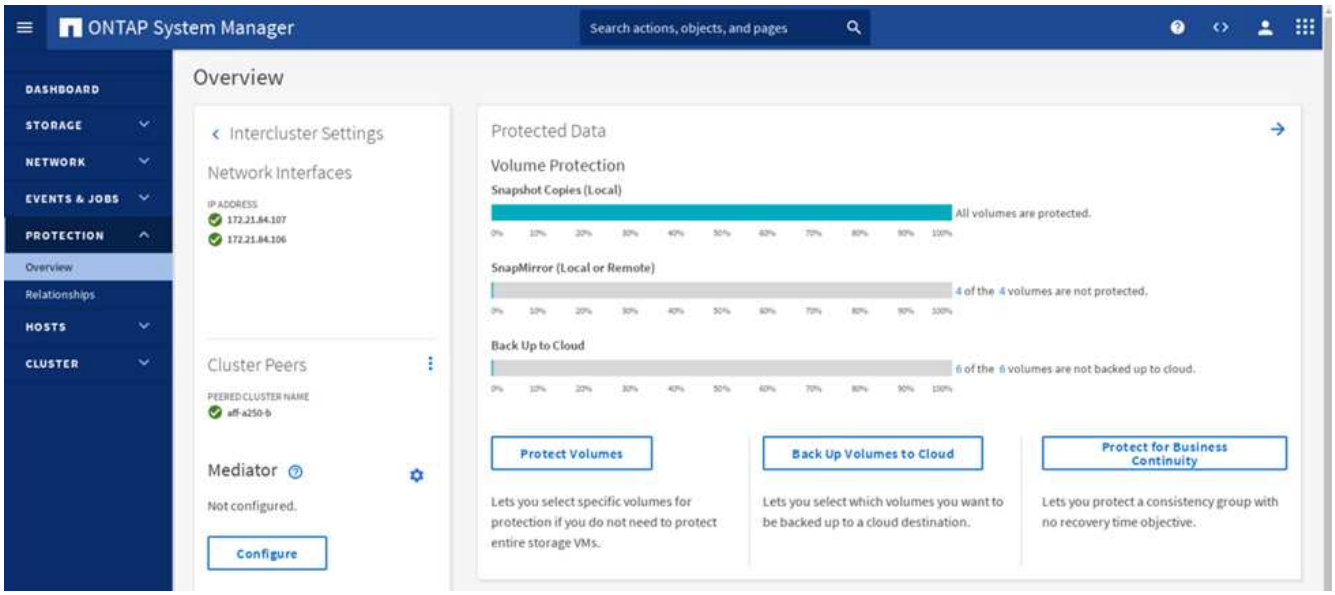
1. Erzeugen einer Cluster-Peering-Passphrase im ersten Cluster



2. Rufen Sie die Peer Cluster-Option im zweiten Cluster auf und stellen Sie die LIF-Informationen für Passphrase und Intercluster bereit.



3. Im Teilfenster System Manager Protection > Overview werden Cluster-Peer-Informationen angezeigt.

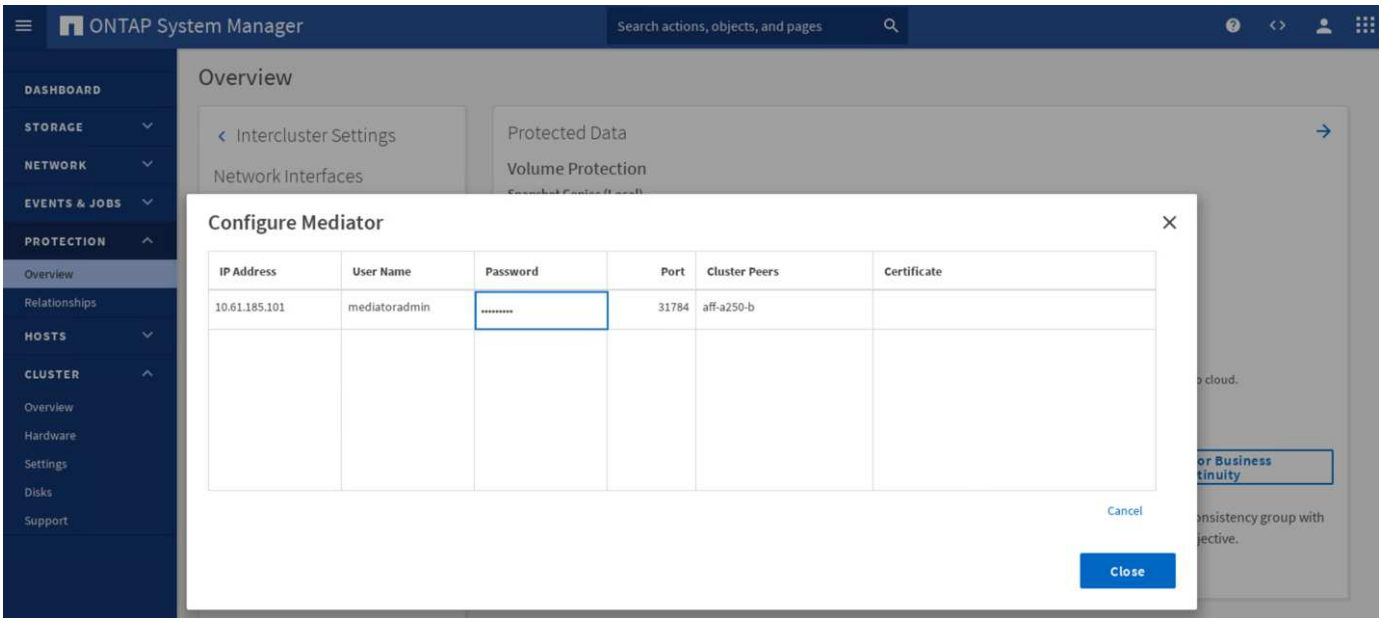


Installation und Konfiguration des ONTAP Mediators

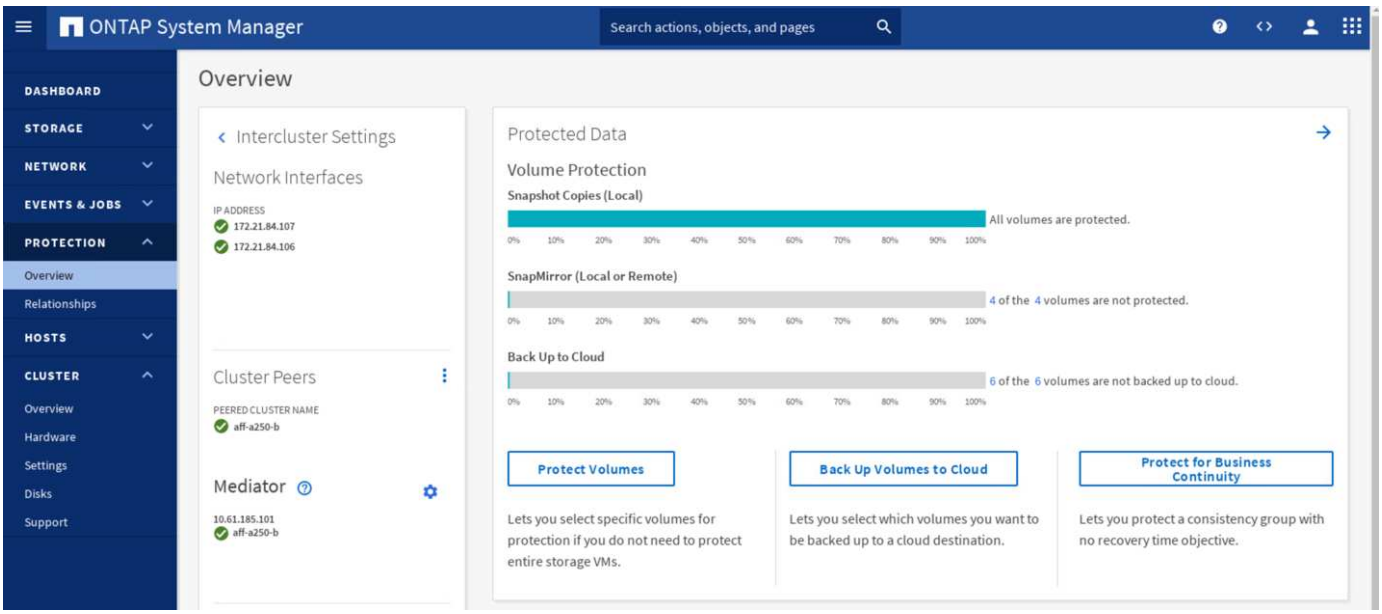
Der ONTAP Mediator stellt ein Quorum für die ONTAP Cluster in einer SM-BC Beziehung her. Es koordiniert das automatisierte Failover, wenn ein Fehler erkannt wird, und vermeidet Split-Brain-Szenarien, wenn jedes Cluster gleichzeitig versucht, die Kontrolle als primäres Cluster zu etablieren.

Bevor Sie den ONTAP Mediator installieren, überprüfen Sie den "Installieren oder aktualisieren Sie den ONTAP Mediator-Dienst" Seite für Voraussetzungen, unterstützte Linux-Versionen und die Verfahren für die Installation auf den verschiedenen unterstützten Linux-Betriebssystemen.

Nach der Installation des ONTAP Mediators können Sie das Sicherheitszertifikat des ONTAP Mediators zu den ONTAP Clustern hinzufügen und dann den ONTAP Mediator im Fenster System Manager Protection > Overview konfigurieren. Der folgende Screenshot zeigt die ONTAP Mediator Konfiguration GUI.



Nachdem Sie die erforderlichen Informationen bereitgestellt haben, wird der konfigurierte ONTAP-Mediator im Fenster System Manager-Schutz > Übersicht angezeigt.



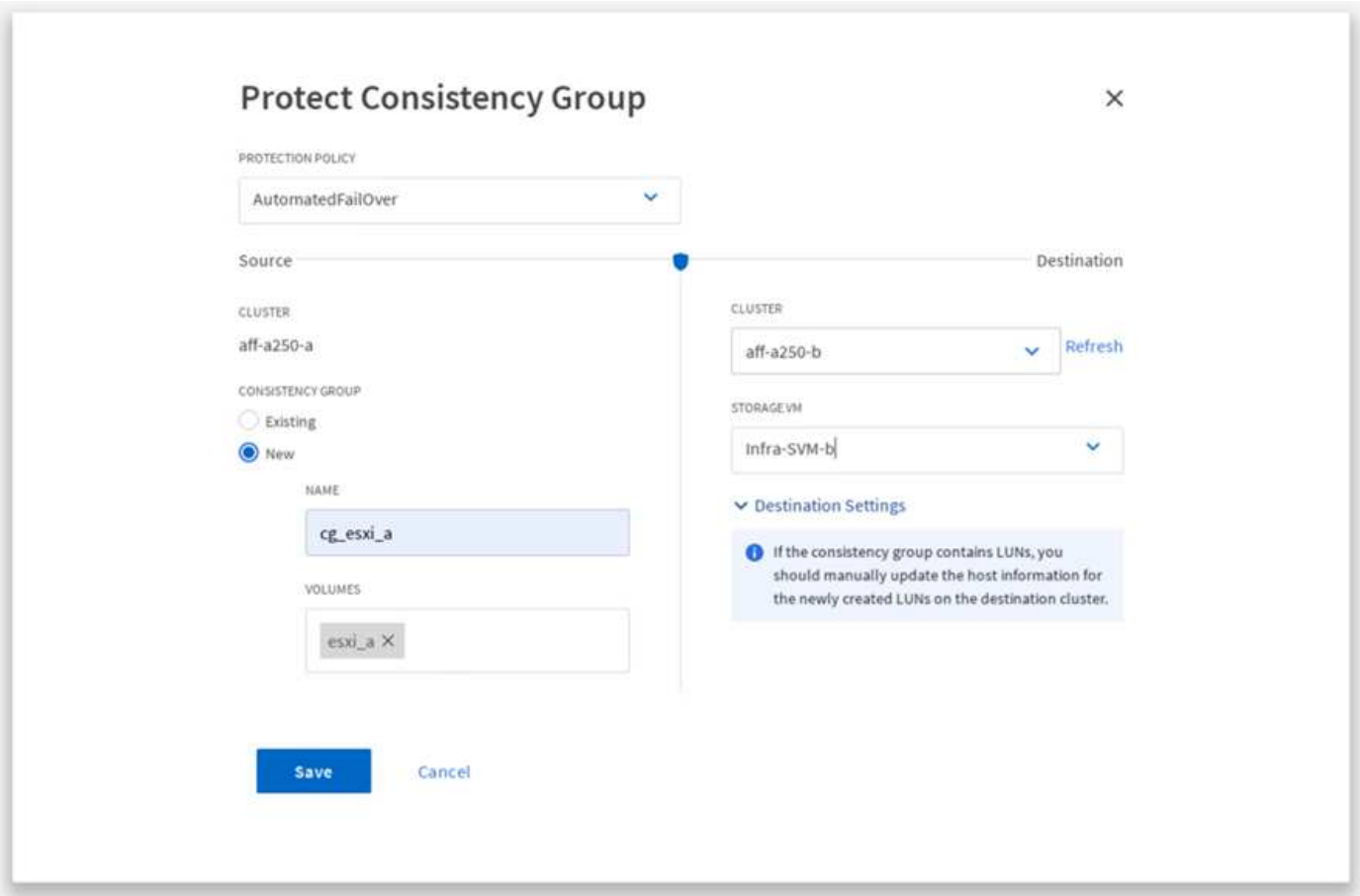
SM-BC Konsistenzgruppe

Eine Konsistenzgruppe bietet eine Schreibreihenfolge-Konsistenzgarantie für einen Applikations-Workload, der eine Sammlung angegebener Volumes umfasst. Für ONTAP 9.10.1 sind hier einige der wichtigen Einschränkungen und Grenzen zu sehen.

- Die maximale Anzahl von SM-BC-Konsistenzgruppenbeziehungen in einem Cluster ist 20.
- Die maximale Anzahl von unterstützten Volumen pro SM-BC-Beziehung ist 16.
- Die maximale Anzahl von Quell- und Ziel-Endpunkten in einem Cluster beträgt 200.

Weitere Informationen finden Sie in der Dokumentation zu ONTAP SM-BC auf der "Einschränkungen und Einschränkungen".

Für die Validierungskonfiguration wurde ONTAP System Manager verwendet, um die Konsistenzgruppen zu erstellen, um sowohl die ESXi Boot-LUNs als auch die gemeinsam genutzten Datenspeicher-LUNs für beide Standorte zu schützen. Auf das Dialogfeld zur Erstellung von Konsistenzgruppen kann unter „Protection“ > „Overview“ > „Protect for Business Continuity“ > „Protect Consistency Group“ zugegriffen werden. Zum Erstellen einer Konsistenzgruppe geben Sie die erforderlichen Quell-Volumes, Ziel-Cluster und Ziel-Storage Virtual Machine-Informationen für die Erstellung ein.

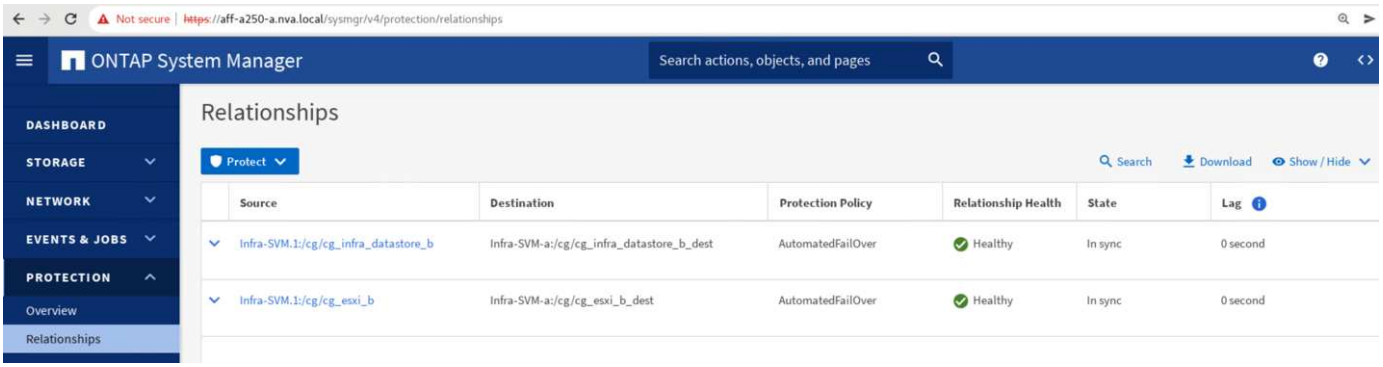


In der folgenden Tabelle werden die vier erstellten Konsistenzgruppen und die Volumes aufgeführt, die in jeder Konsistenzgruppe für die Validierungstests enthalten sind.

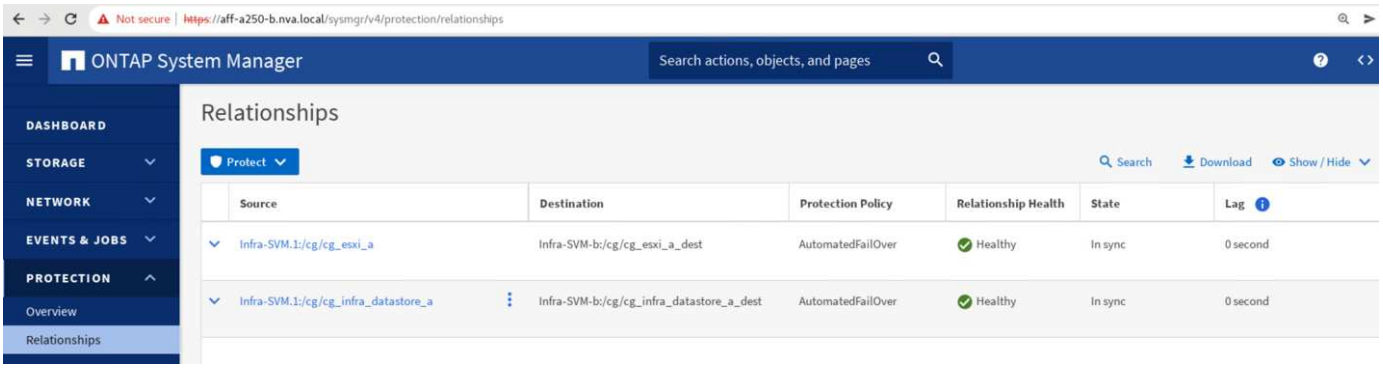
System Manager	Konsistenzgruppe	Volumes
Standort A	cg_esxi_A	esxi_A
Standort A	cg_Infra_Datastore_A	Infra_Datastore_A_01 Infra_Datastore_A_02
Standort B	cg_esxi_b	esxi_b
Standort B	cg_Infra_Datastore_b	Infra_Datastore_b_01 Infra_Datastore_b_02

Nach dem Erstellen der Konsistenzgruppen werden sie unter den jeweiligen Schutzbeziehungen an Standort A und Standort B angezeigt

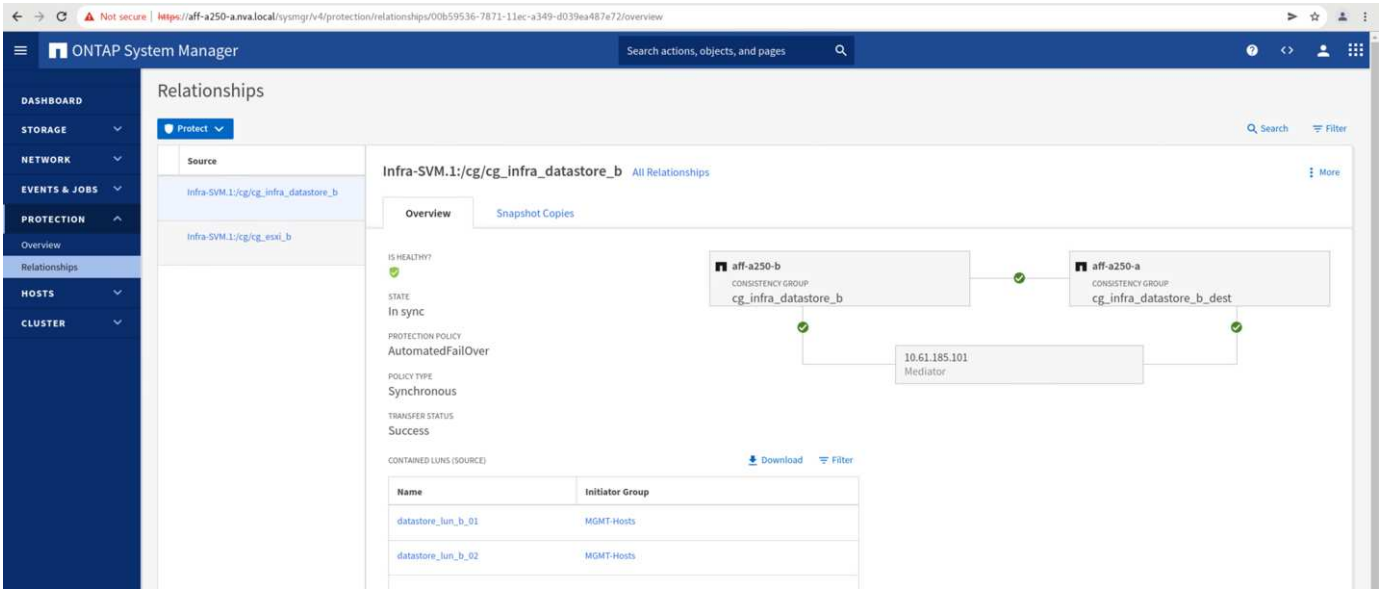
In diesem Screenshot werden die Beziehungen zu Konsistenzgruppen an Standort A angezeigt



In diesem Screenshot werden die Beziehungen zu Konsistenzgruppen an Standort B. angezeigt



In diesem Screenshot werden die Details zur Consistency Group-Beziehung für die cg_Infra_Datastore_b-Gruppe angezeigt.



Volumes, LUNs und Host-Zuordnungen

Nach der Erstellung der Konsistenzgruppen synchronisiert SnapMirror die Quell- und Ziel-Volumes, damit die Daten immer synchron sind. Die Ziel-Volumes am Remote-Standort tragen die Volume-Namen mit dem _dest-Ende. Zum Beispiel gibt es für das esxi_A-Volume in Standort-Cluster ein entsprechendes esxi_A_dest Data Protection (DP)-Volume in Standort B.

In diesem Screenshot werden die Volume-Informationen für Standort A angezeigt

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Dieser Screenshot zeigt die Volume-Informationen für Standort B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Um ein transparentes Applikations-Failover zu ermöglichen, müssen die gespiegelten SM-BC LUNs auch den Hosts aus dem Ziel-Cluster zugeordnet werden. Dadurch können die Hosts Pfade zu den LUNs sowohl von den Quell- als auch von den Ziel-Clustern ordnungsgemäß sehen. Der `igroup show` Und `lun show` Die Ausgänge für Standort A und Standort B werden in den folgenden beiden Screenshots erfasst. Mit den erstellten Zuordnungen sehen jeder ESXi Host im Cluster seine eigene Boot-LUN als ID 0 und alle vier gemeinsamen iSCSI-Datenspeicher-LUNs.

In diesem Screenshot werden die Host-Initiatorgruppen und die LUN-Zuordnung für Standort-Ein-Cluster angezeigt.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01          VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02          VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03          VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                  MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01     VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02     VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03     VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b             MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

In diesem Screenshot werden die Host-Initiatorgruppen und die LUN-Zuordnung für Standort B-Cluster angezeigt.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Weiter: Lösungsvalidierung – Virtualisierung."

Lösungsvalidierung – Virtualisierung

"Früher: Lösungsvalidierung – Storage."

In der FlexPod SM-BC Lösung an mehreren Standorten managt ein einzelnes VMware vCenter die Ressourcen der virtuellen Infrastruktur für die gesamte Lösung. Die Hosts in beiden Datacentern Teil des einzelnen VMware HA Clusters, der beide Datacenter umfasst. Die Hosts haben Zugriff auf die NetApp SM-BC Lösung, bei der auf Storage mit definierten SM-BC-Beziehungen von beiden Standorten aus zugegriffen werden kann.

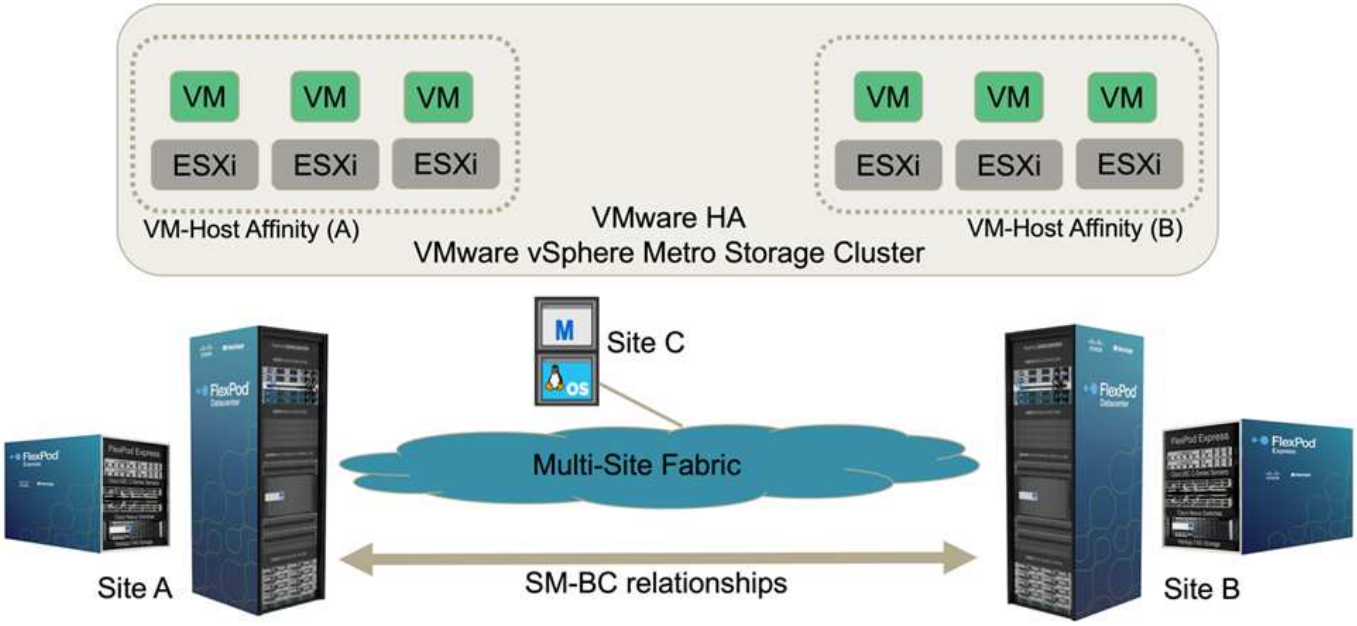
Der Storage für SM-BC Lösung entspricht dem einheitlichen Zugriffsmodell in der VMware vSphere Metro Storage Cluster (vMSC) Funktion zur Vermeidung von Ausfällen und Ausfallzeiten. Für eine optimale Performance der Virtual Machines sollten die Virtual-Machine-Festplatten auf den lokalen NetApp AFF A250 Systemen gehostet werden, um die Latenz und den Datenverkehr über WAN-Links im normalen Betrieb zu minimieren.

Im Rahmen der Design-Implementierung muss die Verteilung der Virtual Machines auf die beiden Standorte ermittelt werden. Sie können die Standortaffinität dieser Virtual Machine und die Applikationsverteilung über die beiden Standorte entsprechend den Vorlieben Ihres Standorts und den Applikationsanforderungen festlegen. Die VMware Cluster VM/Host Groups und VM/Host Rules werden verwendet, um die VM/Host-Affinität zu konfigurieren, um sicherzustellen, dass die VMs auf den Hosts am gewünschten Standort

ausgeführt werden.

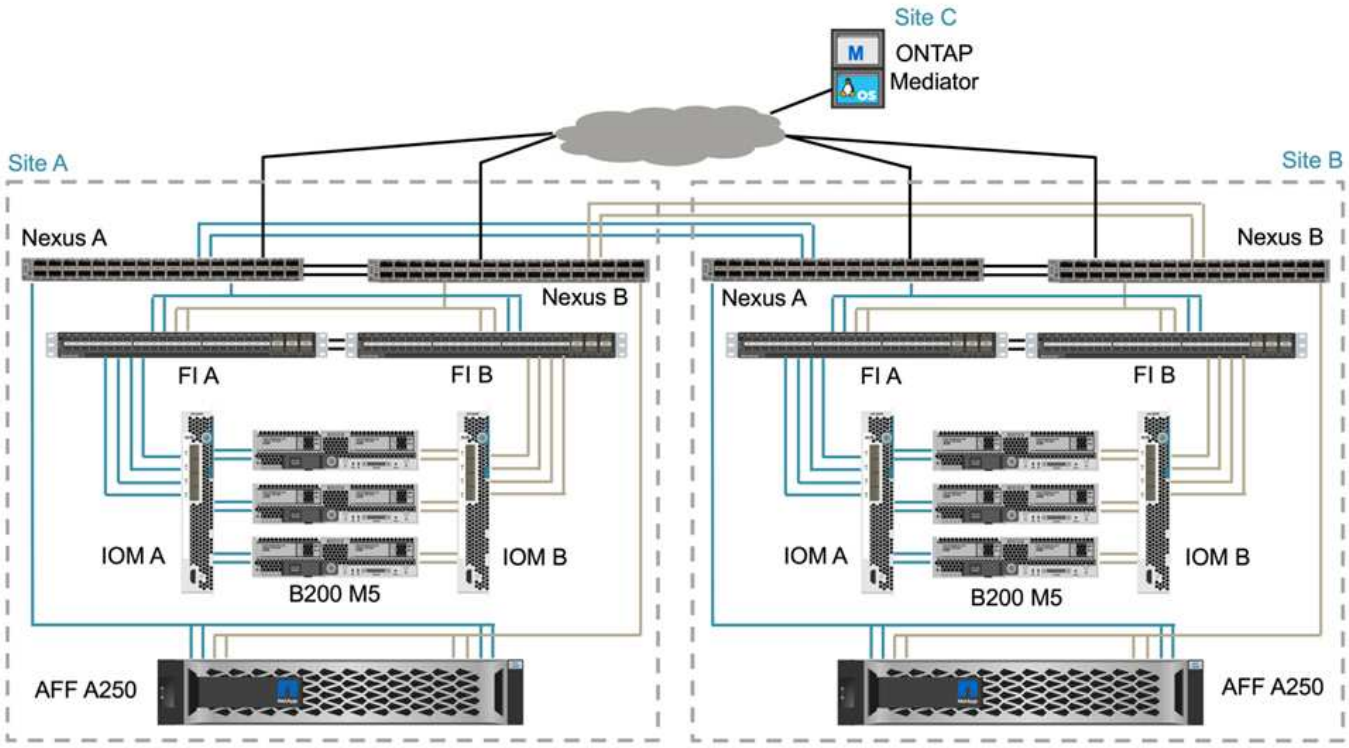
Konfigurationen, mit denen die VMs an beiden Standorten ausgeführt werden können, stellen jedoch sicher, dass VMs durch VMware HA an den Remote-Hosts neu gestartet werden können, um die Stabilität der Lösung zu gewährleisten. Damit die Virtual Machines auf beiden Seiten ausgeführt werden können, müssen alle gemeinsam genutzten iSCSI-Datenspeicher auf allen ESXi Hosts eingebunden werden, um einen reibungslosen vMotion Betrieb der Virtual Machines zwischen den Standorten sicherzustellen.

Die folgende Abbildung zeigt eine allgemeine Virtualisierungsansicht einer FlexPod SM-BC Lösung mit VMware HA- und vMSC-Funktionen für eine hohe Verfügbarkeit von Computing- und Storage-Services. Die aktiv/aktiv-Architektur für Datacenter-Lösungen ermöglicht Workload-Mobilität zwischen Standorten und bietet DR/BC-Schutz.



Umfassende Netzwerkkonnektivität

Die FlexPod SM-BC Lösung umfasst FlexPod-Infrastrukturen an jedem Standort, Netzwerkkonnektivität zwischen Standorten und den ONTAP Mediator, der an einem dritten Standort implementiert wird, um die erforderlichen RPO- und RTO-Vorgaben zu erfüllen. Die folgende Abbildung zeigt die End-to-End-Netzwerkkonnektivität zwischen den Cisco UCS B200M5 Servern an jedem Standort und dem NetApp Storage mit SM-BC Funktionen innerhalb eines Standorts und über mehrere Standorte hinweg.



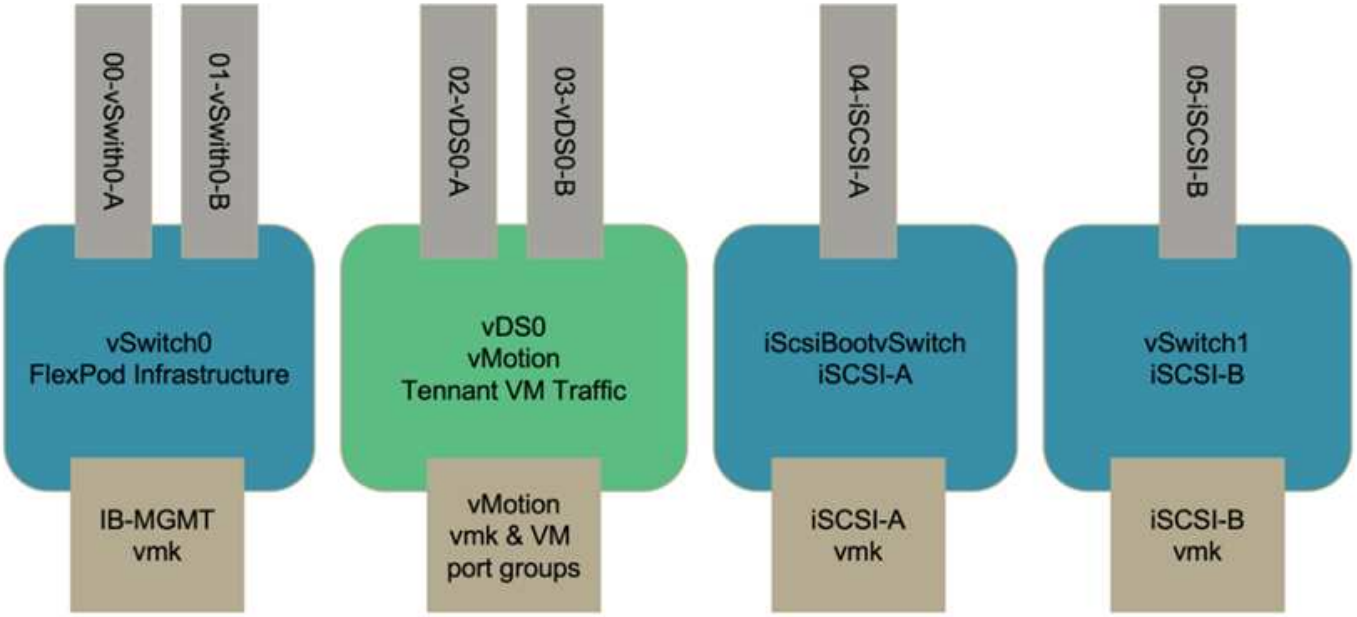
Die FlexPod Implementierungsarchitektur ist bei dieser Lösungsvalidierung an jedem Standort identisch. Die Lösung unterstützt jedoch asymmetrische Implementierungen und kann, wenn sie die Anforderungen erfüllen, auch zu vorhandenen FlexPod Lösungen hinzugefügt werden.

Die erweiterte Layer-2-Architektur dient einer nahtlosen Multi-Site-Data-Fabric-Architektur, die eine Konnektivität zwischen dem Port-gechannelten Cisco UCS-Computing und NetApp Storage in jedem Datacenter sowie Konnektivität zwischen Datacentern bietet. Die Port-Channel-Konfiguration und gegebenenfalls die Konfiguration des virtuellen Port-Kanals werden für die Bandbreitenaggregation und Fehlertoleranz zwischen den Computing-, Netzwerk- und Storage-Ebenen sowie für die standortübergreifenden Links verwendet. Das Ergebnis: Konnektivität und Multipath-Zugriff auf lokalen und Remote NetApp Storage sind die UCS Blade Server.

Virtuelle Netzwerke

Jeder Host im Cluster wird unabhängig vom Speicherort für identische virtuelle Netzwerke bereitgestellt. Das Design trennt die verschiedenen Traffic-Typen mit VMware Virtual Switches (vSwitch) und VMware Virtual Distributed Switches (VdS). Der VMware vSwitch wird hauptsächlich für die FlexPod-Infrastrukturnetzwerke und VdS für Applikationsnetzwerke verwendet, ist aber nicht erforderlich.

Die virtuellen Switches (vSwitch, VdS) werden mit zwei Uplinks pro virtuellen Switch bereitgestellt; die Uplinks auf der ESXi Hypervisor-Ebene werden als VMkernel und virtuelle NICs (vNICs) auf der Cisco UCS Software bezeichnet. Die vNICs werden auf dem Cisco UCS VIC Adapter in jedem Server mit Cisco UCS Service-Profilen erstellt. Sechs vNICs sind definiert, zwei für vSwitch0, zwei für vDS0, zwei für vSwitch1 und zwei für die iSCSI-Uplinks wie in der folgenden Abbildung dargestellt.



VSwitch0 wird während der VMware ESXi Host-Konfiguration definiert. Es enthält das FlexPod Infrastruktur-Management-VLAN und die ESXi Host VMkernel (VMK)-Ports für das Management. Für alle erforderlichen kritischen Virtual Machines für das Infrastrukturmanagement wird zudem eine VM-Portgruppe für vSwitch0 hinzugefügt.

Es ist wichtig, solche Management-Infrastruktur-Virtual Machines auf vSwitch0 statt auf den VdS zu platzieren, da wenn die FlexPod-Infrastruktur heruntergefahren oder aus- und wieder eingeschaltet wird und Sie versuchen, diese Management-Virtual Machine auf einem anderen Host als dem Host zu aktivieren, auf dem sie ursprünglich ausgeführt wurde, Es startet gut im Netzwerk auf vSwitch0. Dieser Prozess ist besonders wichtig, wenn VMware vCenter die Management-Virtual Machine ist. Wenn vCenter auf dem VdS wäre und zu einem anderen Host verschoben und dann gestartet wurde, wäre es nicht mit dem Netzwerk nach dem Booten verbunden.

In diesem Design werden zwei iSCSI Boot vSwitches verwendet. Beim Booten von Cisco UCS iSCSI sind separate vNICs für iSCSI erforderlich. Diese vNICs verwenden das iSCSI-VLAN des entsprechenden Fabric als natives VLAN und sind an den entsprechenden iSCSI-Boot-vSwitch angeschlossen. Optional können Sie auch iSCSI-Netzwerke auf VdS bereitstellen, indem Sie einen neuen VdS oder eine vorhandene einsetzen.

VM-Host-Gruppen und Regeln

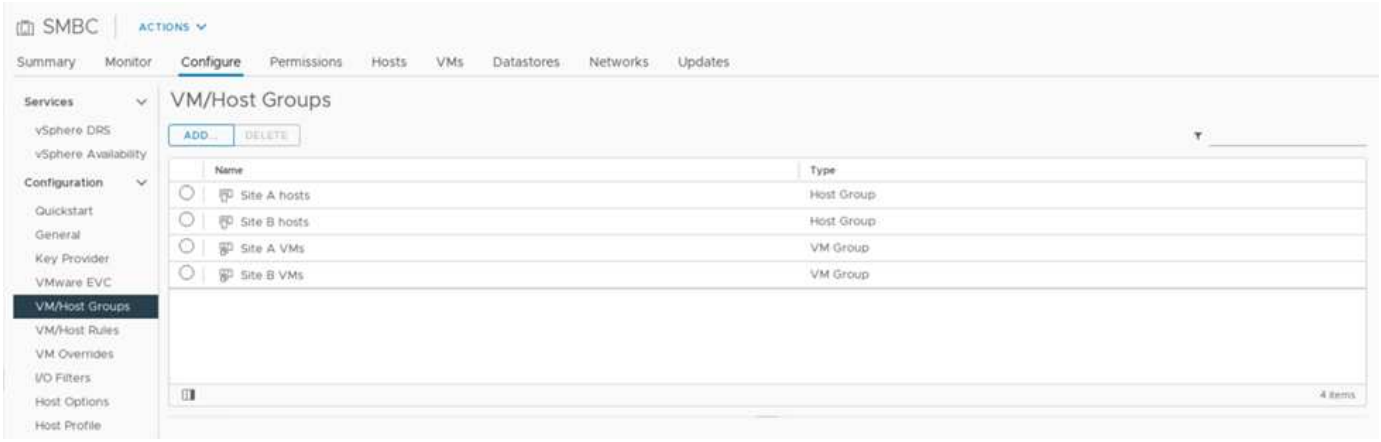
Damit Virtual Machines auf jedem ESXi Host an beiden SM-BC-Sites ausgeführt werden können, müssen alle ESXi Hosts die iSCSI-Datenspeicher von beiden Standorten aus mounten. Wenn die Datastores von beiden Standorten ordnungsgemäß von allen ESXi Hosts eingebunden werden, können Sie eine Virtual Machine zwischen beliebigen Hosts mit vMotion migrieren, und die VM bleibt weiterhin Zugriff auf alle ihre virtuellen Festplatten, die aus diesen Datastores erstellt wurden.

Bei einer virtuellen Maschine, die lokale Datenspeicher verwendet, wird der Zugriff auf virtuelle Festplatten Remote, wenn sie zu einem Host am Remote-Standort migriert wird und somit die Verzögerung beim Lesevorgang aufgrund der physischen Entfernung zwischen den Standorten erhöht. Daher empfiehlt es sich, die Virtual Machines auf lokalen Hosts aufzubewahren und den lokalen Storage am Standort zu nutzen.

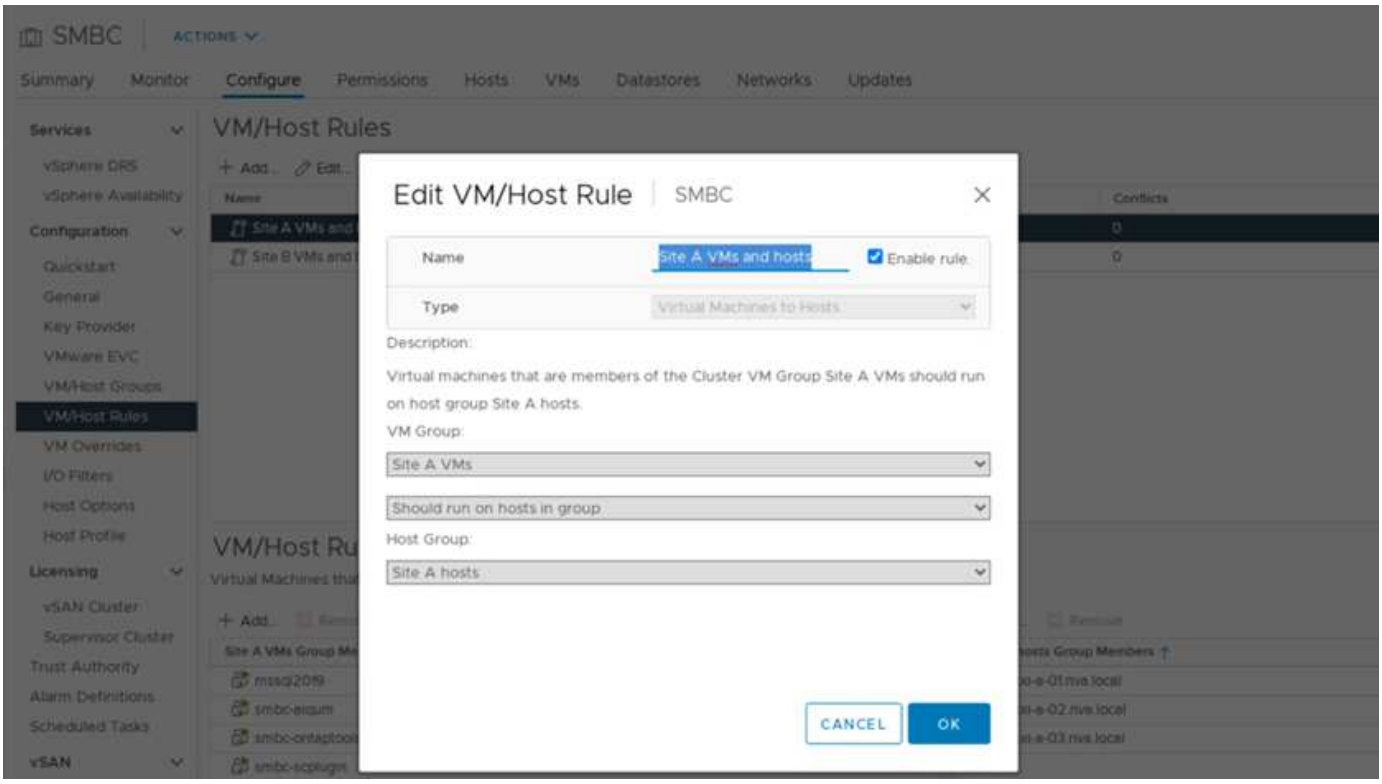
Mithilfe eines Mechanismus zur VM-/Hostorientierung können Sie VM-/Host-Gruppen verwenden, um eine VM-Gruppe und eine Host-Gruppe für Virtual Machines und Hosts zu erstellen, die sich an einem bestimmten Standort befinden. Mithilfe von VM-/Host-Regeln können Sie die Richtlinie für die folgenden VMs und Hosts festlegen. Um eine standortübergreifende Migration virtueller Maschinen während einer Standortwartung oder

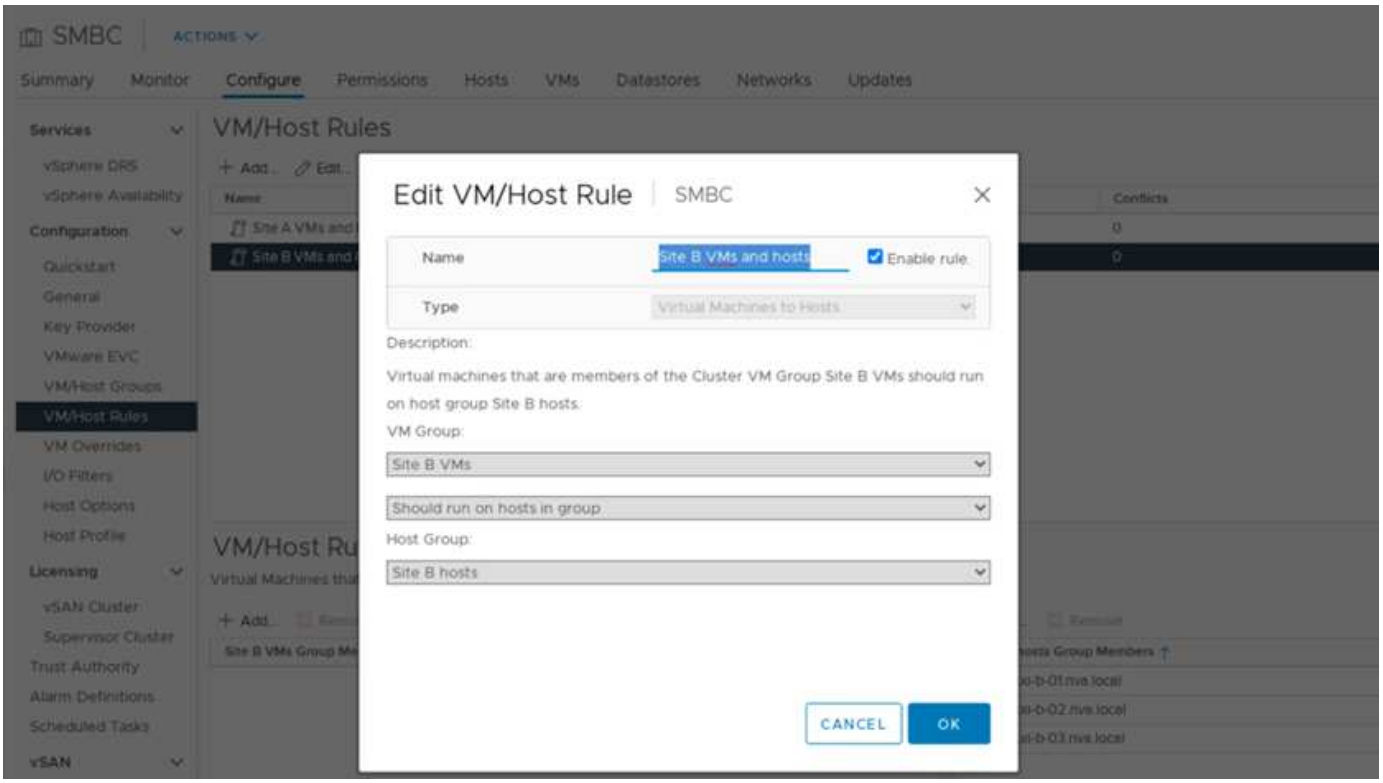
eines Notfallszenarios zu ermöglichen, verwenden Sie die Richtlinienspezifikation „sollte auf Hosts in der Gruppe ausgeführt werden“, um diese Flexibilität zu gewährleisten.

Der folgende Screenshot zeigt, dass zwei Host-Gruppen und zwei VM-Gruppen für Hosts und VMs an Standort A und Standort B erstellt werden



Zusätzlich zeigen die folgenden beiden Abbildungen die VM/Host Regeln, die für Standort A und Standort B VMs erstellt werden, um auf den Hosts auf ihren jeweiligen Seiten mit der "sollte auf Hosts in der Gruppe laufen"-Politik zu laufen.

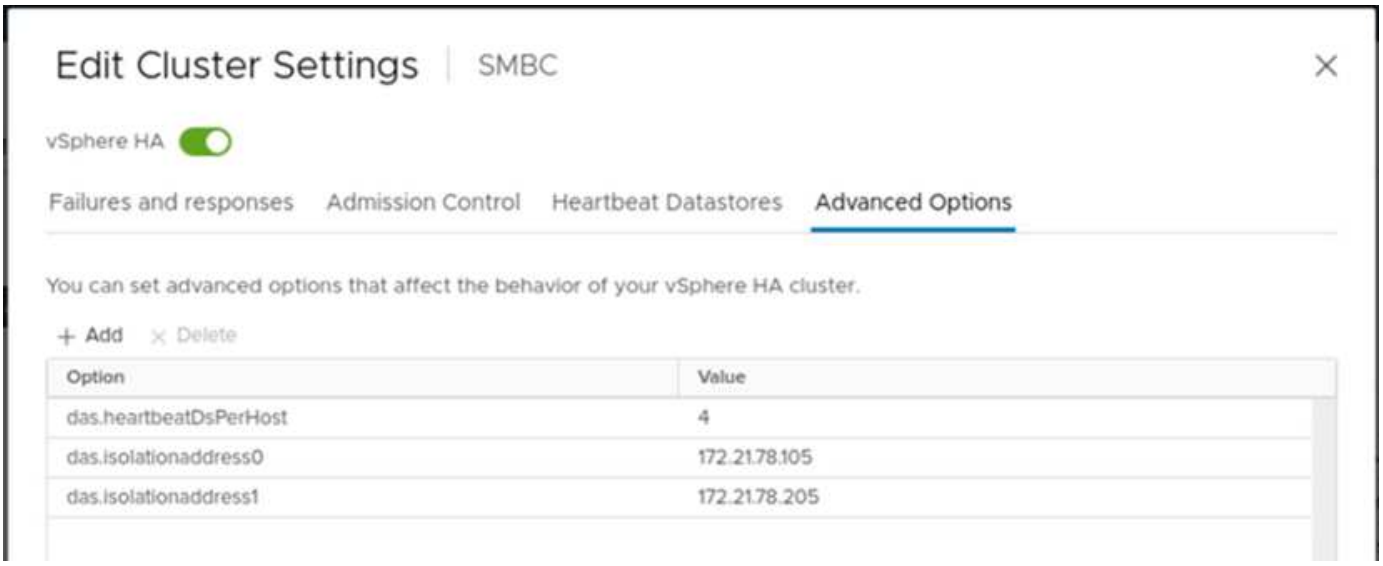




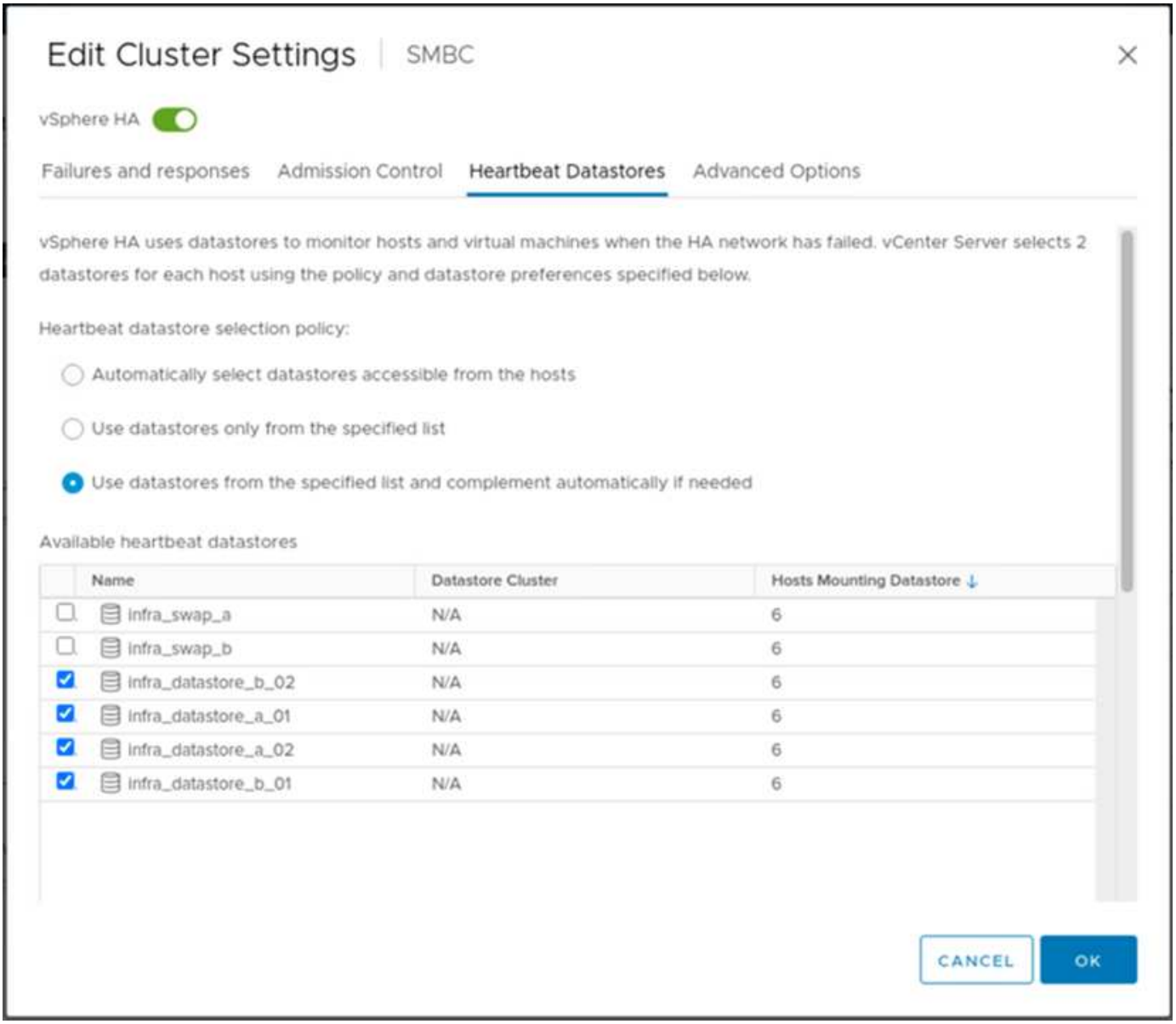
Ha-Herzschlag von vSphere

VMware vSphere HA verfügt über einen Heartbeat-Mechanismus zur Validierung des Hoststatus. Der primäre Heartbeat-Mechanismus wird über das Netzwerk durchgeführt. Der sekundäre Heartbeat-Mechanismus erfolgt über den Datenspeicher. Wenn keine Herzschläge empfangen werden, entscheidet sie dann, ob sie vom Netzwerk isoliert wird, indem sie das Standard-Gateway oder die manuell konfigurierten Isolationsadressen pingen. Beim Herzschlag des Datenspeichers empfiehlt VMware, die Heartbeat-Datenspeicher für ein dehnbares Cluster von mindestens zwei auf vier zu erhöhen.

Für die Lösungsvalidierung werden die beiden ONTAP-Cluster-Management-IP-Adressen als Isolationsadresse verwendet. Darüber hinaus die empfohlene vSphere HA Advanced Option `ds.heartbeatDsPerHost` Mit einem Wert von 4 wurde hinzugefügt, wie in der folgenden Abbildung dargestellt.



Geben Sie für den Heartbeat-Datenspeicher die vier gemeinsam genutzten Datenspeicher aus dem Cluster an und ergänzen Sie sie automatisch, wie in der folgenden Abbildung dargestellt.



Weitere Best Practices und Konfigurationen für VMware HA Cluster und VMware vSphere Metro Storage Cluster finden Sie unter "Erstellen und Verwenden von vSphere HA-Clustern", "VMware vSphere Metro Storage-Cluster (vMSC)" Und der VMware KB für "NetApp ONTAP mit NetApp SnapMirror Business Continuity (SM-BC) und VMware vSphere Metro Storage Cluster (vMSC)".

"Weiter: Lösungsvalidierung – validierte Szenarien."

Lösungsvalidierung – validierte Szenarien

"Zurück: Lösungsvalidierung – Virtualisierung."

Die FlexPod Lösung für SM-BC von Datacenter schützt Datenservices für verschiedene Single-Point-of-Failure-Szenarien und für einen Standortausfall. Das an jedem Standort implementierte redundante Design sorgt für Hochverfügbarkeit. Die SM-BC Implementierung mit synchroner Datenreplizierung an allen Standorten schützt

Datenservices vor einem standortweiten Ausfall. Die implementierte Lösung wurde für die gewünschte Funktionalität der Lösung sowie für verschiedene Ausfallszenarien validiert, bei denen die Lösung zum Schutz entwickelt wurde.

Validierung der Funktionen der Lösung

In verschiedenen Testfällen werden die Funktionen der Lösung überprüft und teilweise oder vollständige Ausfallszenarien am Standort simuliert. Um die Duplizierung durch die bereits in den vorhandenen FlexPod Datacenter-Lösungen im Rahmen des Cisco Validated Design Programms durchgeführten Tests zu minimieren, liegt der Schwerpunkt dieses Berichts auf den SM-BC-bezogenen Aspekten der Lösung. Einige allgemeine FlexPod-Validierungen sind enthalten, damit die Praktizierenden für ihre Umsetzung Validierungen gehen.

Für die Lösungsvalidierung wurde ein Virtual Machine unter Windows 10 pro ESXi Host auf allen ESXi Hosts an beiden Standorten erstellt. Das IOMeter Tool wurde installiert und zur Generierung von I/O-Vorgängen zu zwei virtuellen Datenfestplatten verwendet, die aus den gemeinsam genutzten lokalen iSCSI-Datenspeichern zugeordnet werden. Die konfigurierten IOMeter Workload-Parameter waren 8-KB I/O, 75 % Lesezugriffe und 50 % zufällige Zugriffe, mit 8 ausstehenden I/O-Befehlen für jede Datenfestplatte. Die Fortsetzung der IOMeter I/O-Vorgänge liefert bei den meisten durchgeführten Testszenarien an, dass ein Szenario keinen Ausfall des Datenservice verursacht hat.

Da SM-BC für Business-Applikationen wie Datenbankserver wichtig ist, Die Microsoft SQL Server 2019 Instanz auf einer Windows Server 2022 Virtual Machine wurde auch als Teil der Tests eingeschlossen, um zu bestätigen, dass die Applikation weiter ausgeführt wird, wenn Storage am lokalen Standort nicht verfügbar ist und der Datenservice ohne Applikation am Remote-Standort fortgesetzt wird Unterbrechungen.

Bootstest für ESXi Host iSCSI SAN

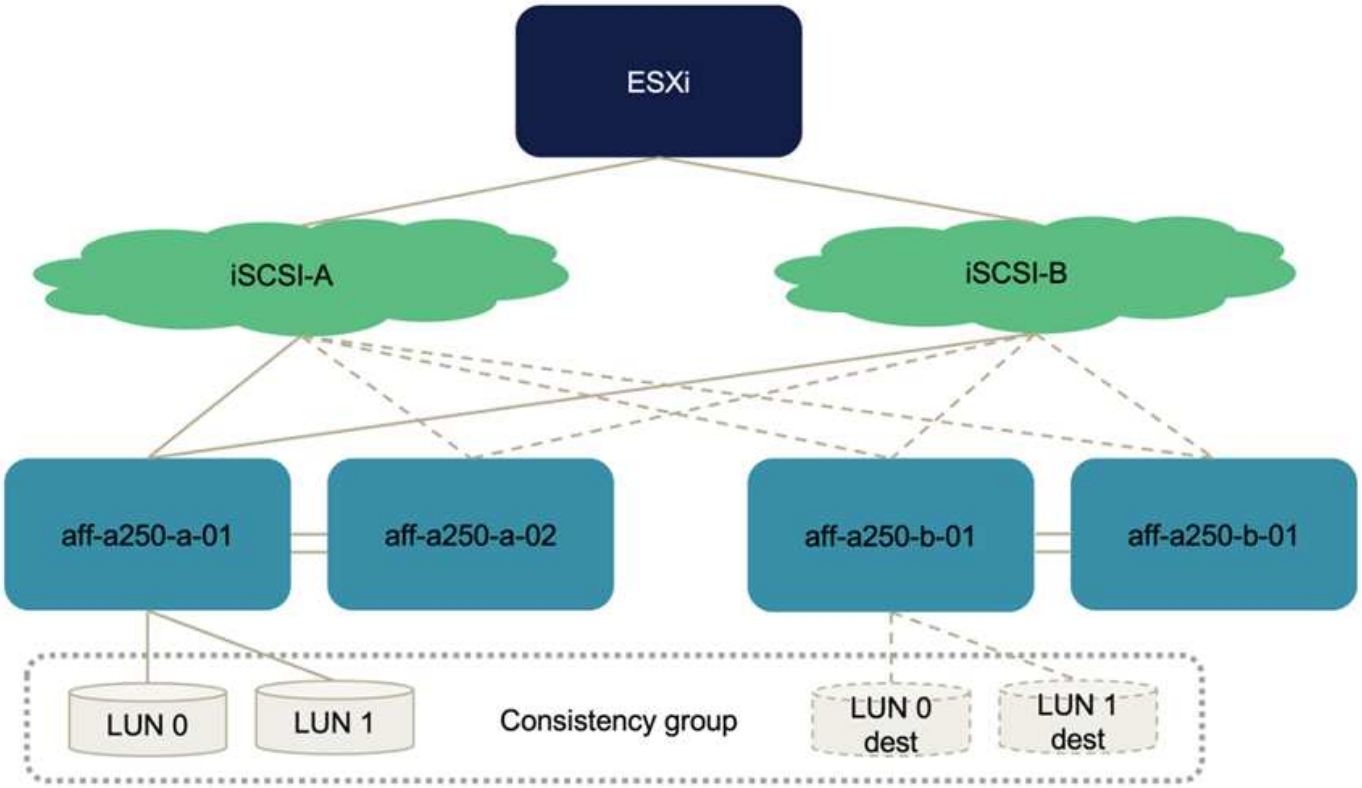
Die ESXi-Hosts in der Lösung sind für das Booten über das iSCSI-SAN konfiguriert. Die Verwendung von SAN-Boot vereinfacht das Servermanagement beim Austausch eines Servers, da das Serviceprofil des Servers einem neuen Server zugewiesen werden kann, damit der IT-Server ohne zusätzliche Konfigurationsänderungen gestartet werden kann.

Zusätzlich zum Booten eines ESXi Hosts an einem Standort von seiner lokalen iSCSI-Boot-LUN wurden Tests zum Booten des ESXi Hosts durchgeführt, wenn sich der lokale Storage-Controller im Übernahmemodus befindet oder dessen lokaler Storage-Cluster vollständig nicht verfügbar ist. Mithilfe dieser Validierungsszenarien wird sichergestellt, dass die ESXi Hosts je Design ordnungsgemäß konfiguriert sind und während einer Storage-Wartung oder eines Disaster Recovery-Szenarios hochgefahren werden können, um Business Continuity zu gewährleisten.

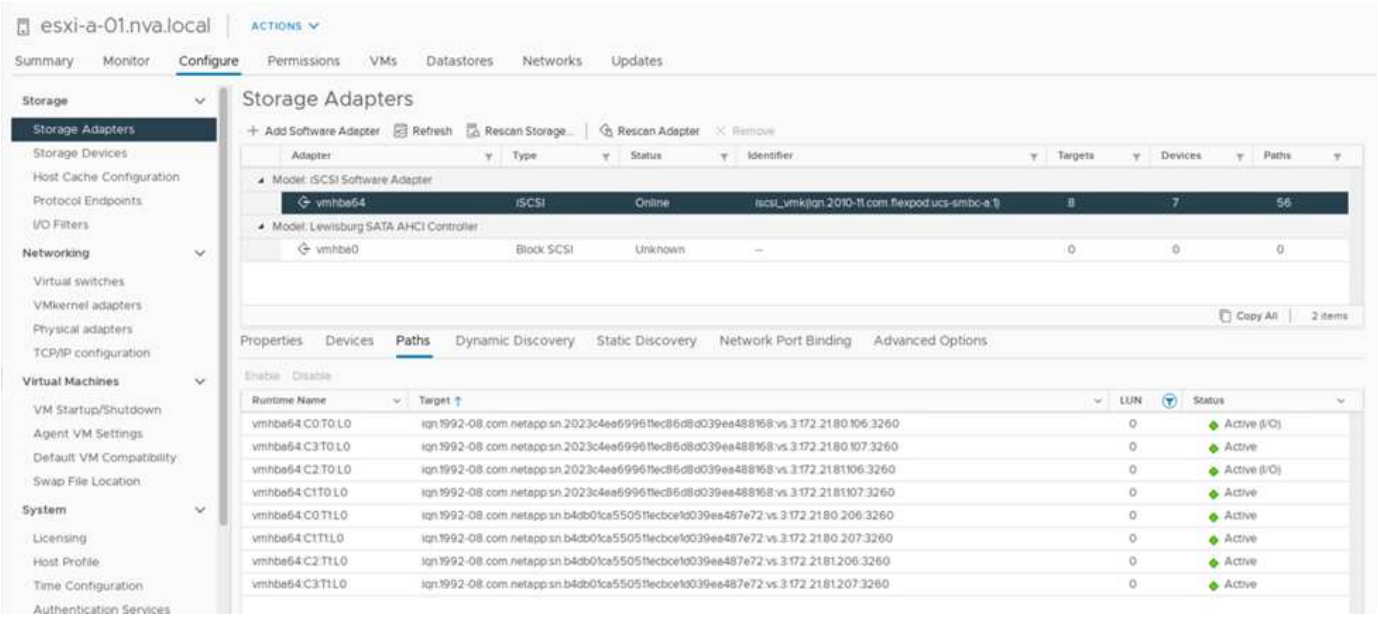
Bevor die SM-BC Konsistenzgruppenbeziehung konfiguriert ist, verfügt ein iSCSI-LUN, das von einem Storage Controller HA-Paar gehostet wird, über vier Pfade, zwei über jede iSCSI-Fabric, basierend auf der Implementierung von Best Practices. Ein Host kann über die zwei iSCSI-VLANs/Fabrics zum LUN-Hosting Controller gelangen und über den hochverfügbaren Partner des Controllers zur LUN gelangen.

Nachdem die SM-BC Konsistenzgruppe-Beziehung konfiguriert ist und die gespiegelten LUNs den Initiatoren ordnungsgemäß zugeordnet sind, verdoppelt sich die Pfadanzahl für die LUN. Für diese Implementierung reicht es von zwei aktiven/optimierten Pfaden und zwei aktiv/nicht-optimierte Pfade bis hin zu zwei aktiv/optimierten Pfaden und sechs aktiv/nicht optimierte Pfade.

In der folgenden Abbildung werden die Pfade dargestellt, die ein ESXi Host für den Zugriff auf eine LUN nutzen kann, beispielsweise LUN 0. Da die LUN an den Standort A Controller 01 angeschlossen ist, sind nur die beiden Pfade, die direkt über diesen Controller auf die LUN zugreifen, aktiv/optimiert und alle verbleibenden sechs Pfade sind aktiv/nicht optimiert.



Der folgende Screenshot mit den Informationen zum Pfad für das Storage-Gerät zeigt, wie der ESXi Host die zwei Typen von Gerätepfaden sieht. Die beiden aktiven/optimierten Pfade werden als haben angezeigt `active (I/O)` Pfadstatus, während die sechs aktiven/nicht optimierten Pfade nur als angezeigt werden `active`. Beachten Sie außerdem, dass in der Spalte Ziel die beiden iSCSI-Ziele und die entsprechenden iSCSI-LIF-IP-Adressen angezeigt werden, um die Ziele zu erreichen.



Wenn einer der Storage Controller für Wartungsarbeiten oder Upgrades ausfällt, stehen die beiden Pfade zum Erreichen des heruntergekommen Controllers nicht mehr zur Verfügung und zeigen den Pfadstatus von an `dead` Stattdessen.

Wenn ein Failover der Konsistenzgruppe auf dem primären Storage Cluster erfolgt, entweder aufgrund von

manuellen Failover-Tests oder aufgrund von automatischem Disaster Failover, stellt das sekundäre Storage-Cluster weiterhin Datenservices für die LUNs in der SM-BC-Konsistenzgruppe bereit. Da die LUN-Identitäten erhalten bleiben und die Daten synchron repliziert werden, bleiben alle durch SM-BC-Konsistenzgruppen geschützten ESXi Host-Boot-LUNs über das Remote-Storage-Cluster verfügbar.

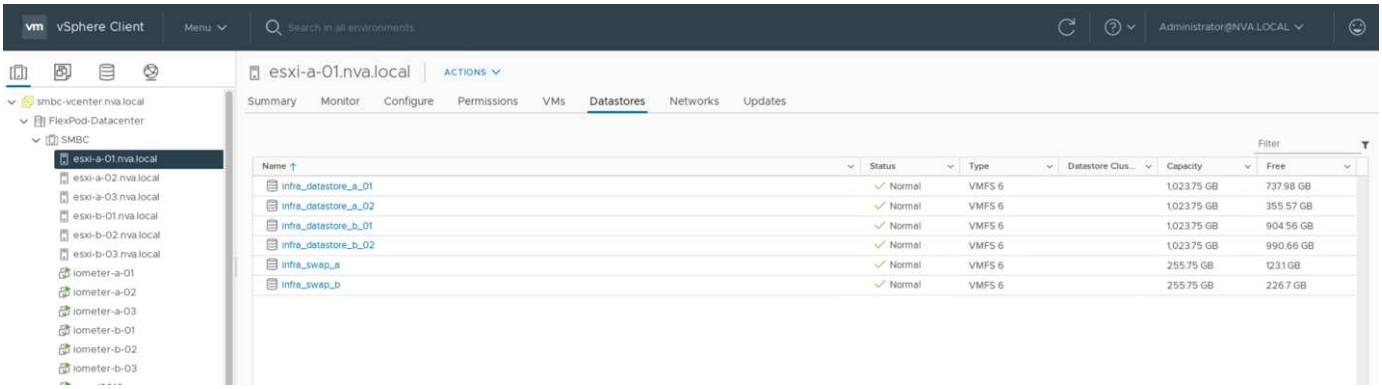
VMware vMotion und VM/Host-Affinitätstest

Obwohl eine allgemeine FlexPod VMware Datacenter Lösung Multi-Protokolle wie FC, iSCSI, NVMe und NFS unterstützt, unterstützt die FlexPod SM-BC Lösungsfunktion FC und iSCSI SAN-Protokolle, die üblicherweise für geschäftskritische Lösungen verwendet werden. Diese Validierung verwendet nur iSCSI-protokollbasierte Datenspeicher und iSCSI SAN Boot.

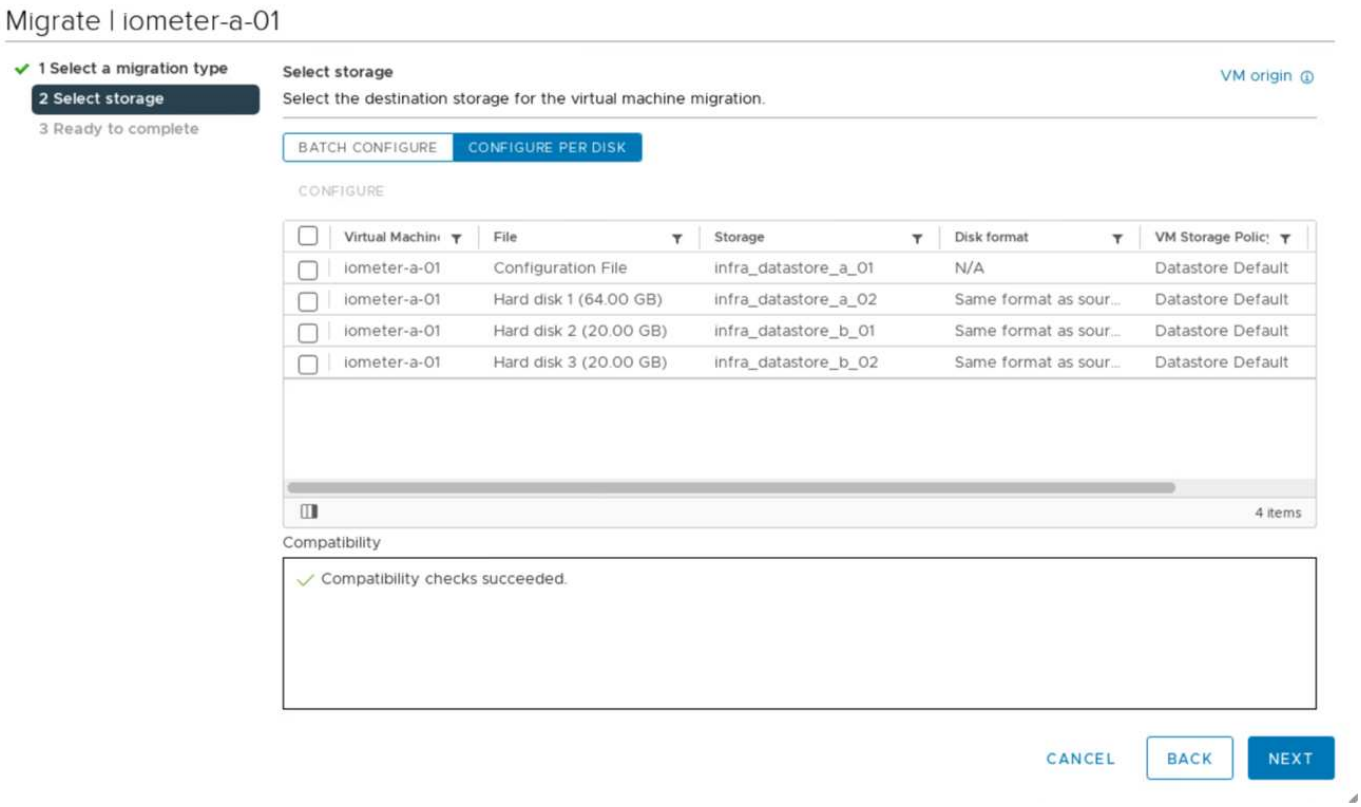
Damit Virtual Machines Storage-Services von einem SM-BC-Standort aus verwenden können, müssen die iSCSI-Datenspeicher beider Standorte von allen Hosts im Cluster gemountet werden, um die Migration von Virtual Machines zwischen beiden Standorten und für Disaster Failover-Szenarien zu ermöglichen.

Für Applikationen, die auf der virtuellen Infrastruktur ausgeführt werden, die über Standorte hinweg keinen SM-BC-Konsistenzgruppenschutz benötigen, können auch NFS-Protokoll und NFS-Datenspeicher verwendet werden. In diesem Fall ist Vorsicht zu beachten, wenn Storage für VMs zugewiesen wird, damit geschäftskritische Applikationen die durch SM-BC Consistency Group geschützten SAN-Datenspeicher ordnungsgemäß verwenden, um Business Continuity zu gewährleisten.

Der folgende Screenshot zeigt, dass Hosts konfiguriert sind, um iSCSI-Datenspeicher von beiden Seiten einzubinden.



Sie haben die Möglichkeit, Laufwerke von Virtual Machines zwischen verfügbaren iSCSI-Datenspeichern beider Standorte zu migrieren, wie in der folgenden Abbildung dargestellt. Bei Performance-Überlegungen ist es optimal, Virtual Machines zu nutzen, die Storage aus dem lokalen Storage-Cluster verwenden, um die Festplatten-I/O-Latenzen zu verringern. Dies gilt insbesondere, wenn sich beide Standorte aufgrund der physischen Latenz für die hin- und Rückfahrt von ca. 1 ms pro 100 km Entfernung in einigen Entfernungen voneinander unterscheiden.



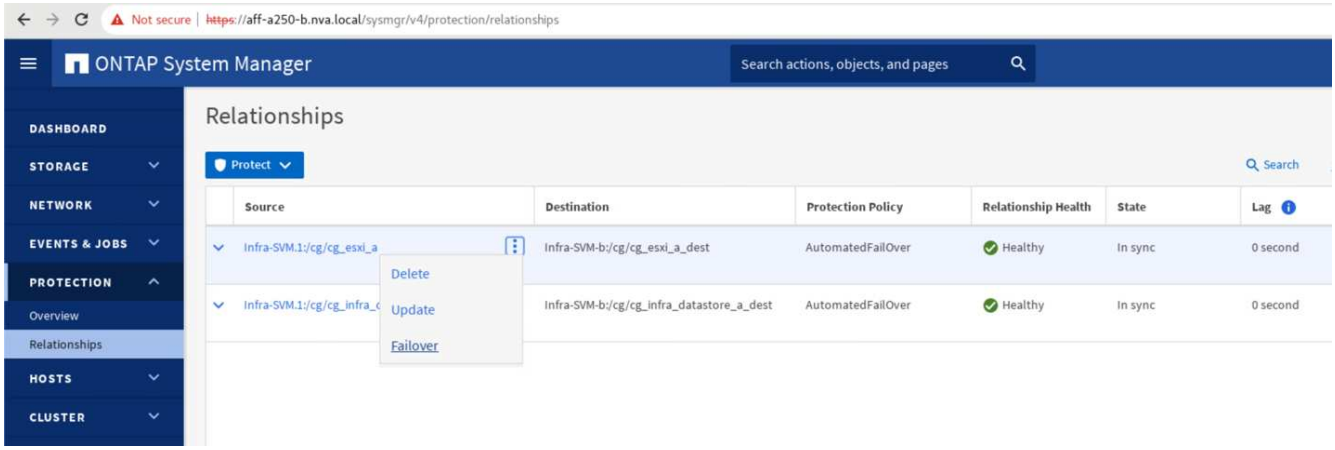
Tests von vMotion von Virtual Machines auf einem anderen Host an demselben Standort und über mehrere Standorte hinweg wurden durchgeführt und erfolgreich durchgeführt. Nach der manuellen Migration einer virtuellen Maschine über Standorte hinweg wird die Regel für die VM/Hostaffinität aktiviert und die virtuelle Maschine zurück zur Gruppe migriert, in der sie unter dem normalen Zustand gehört.

Geplantes Storage-Failover

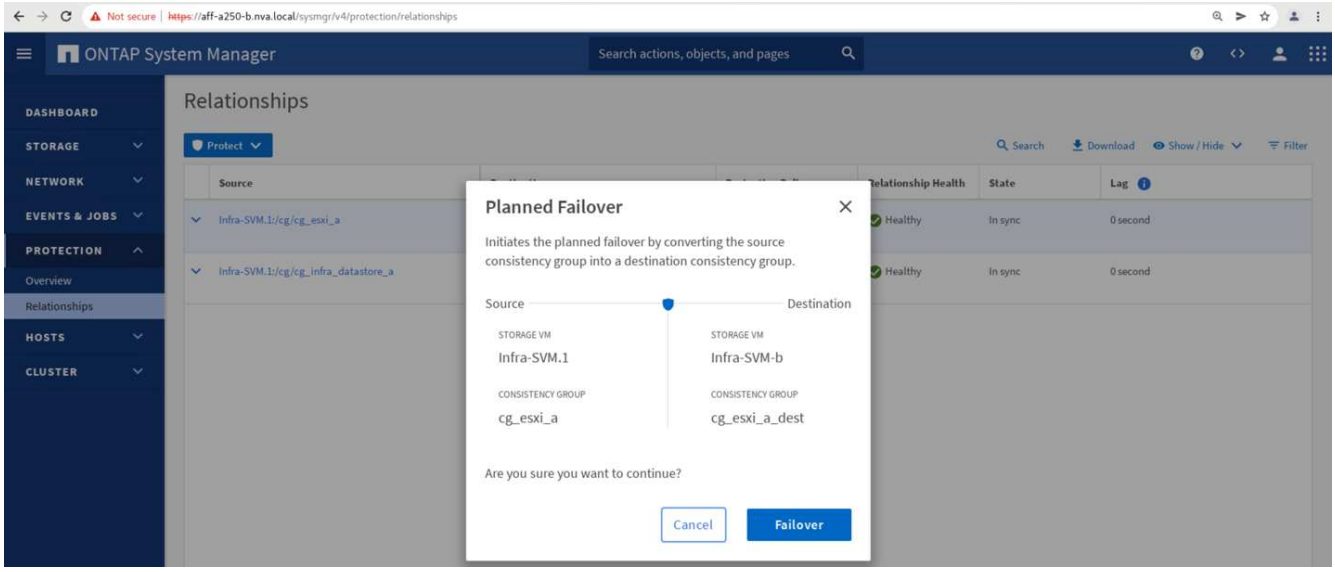
Geplante Storage Failover-Vorgänge sollten nach der Erstkonfiguration der Lösung ausgeführt werden, um festzustellen, ob die Lösung nach dem Storage Failover ordnungsgemäß funktioniert. Der Test kann dabei helfen, alle Verbindungs- oder Konfigurationsprobleme zu identifizieren, die zu I/O-Unterbrechungen führen können. Durch regelmäßige Tests und Behebung von Verbindungs- oder Konfigurationsproblemen können im Falle eines wirklichen Standortausfalls unterbrechungsfreie Datenservices bereitgestellt werden. Geplante Storage-Failovers können auch vor geplanten Aktivitäten zur Storage-Wartung verwendet werden, damit Datenservices vom nicht betroffenen Standort bedient werden können.

Um einen manuellen Failover von Standort-A-Speicherdatendiensten an Standort B zu initiieren, können Sie die Aktion mithilfe des Standort B ONTAP-System Managers durchführen.

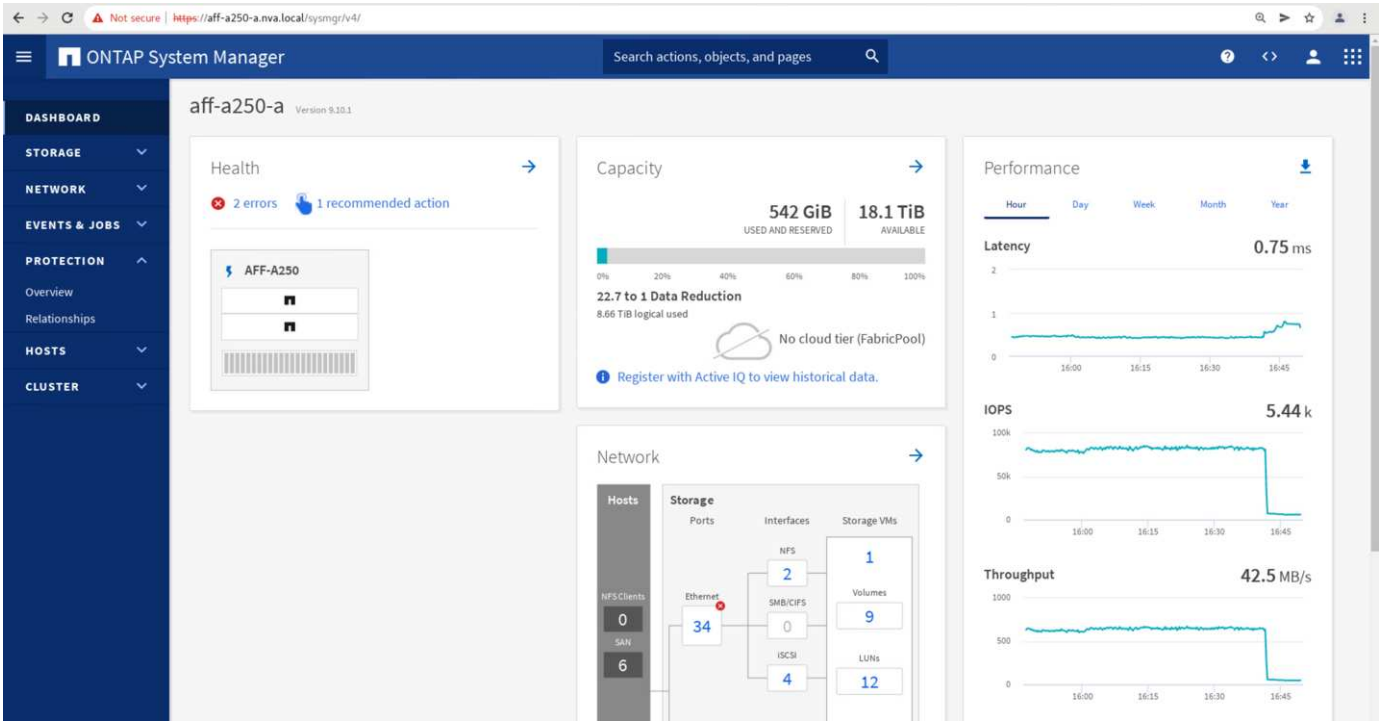
1. Wechseln Sie zum Bildschirm Schutz > Beziehungen, um zu bestätigen, dass der Status der Beziehungen zu Konsistenzgruppen lautet `In Sync`. Wenn es noch im ist `Synchronizing` Status: Warten Sie, bis der Status in lautet `In Sync` Vor dem Durchführen eines Failover.
2. Erweitern Sie die Punkte neben dem Quellnamen, und klicken Sie auf Failover.



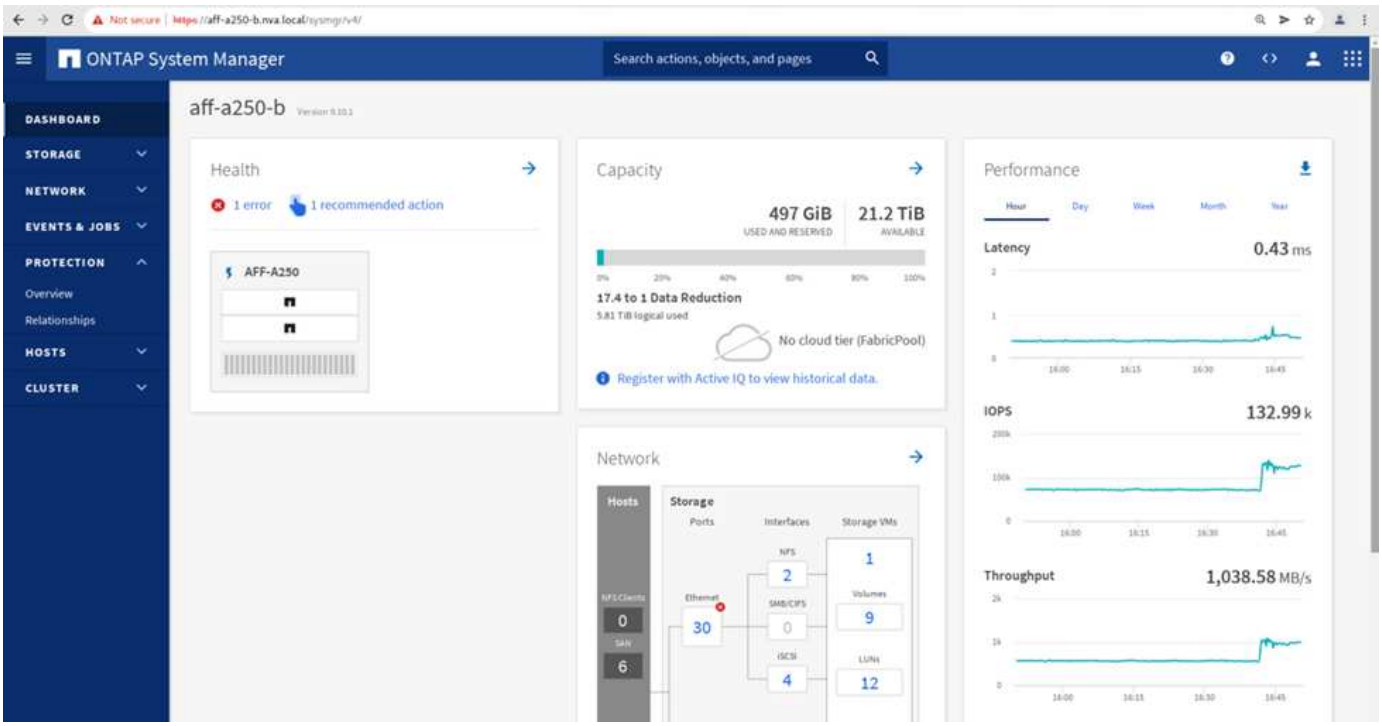
3. Bestätigen Sie das Failover für den Start der Aktion.



Kurz nach dem Start des Failover der beiden Konsistenzgruppen, `cg_esxi_a` Und `cg_infra_datastore_a`, Auf der Website B System Manager GUI ist der Standort A I/O, der die beiden Konsistenzgruppen bereitstellt, auf Standort B. verschoben Dadurch wird die I/O an Standort Erheblich reduziert, wie am Standort Das Performance-Teilfenster „System Manager“ dargestellt.

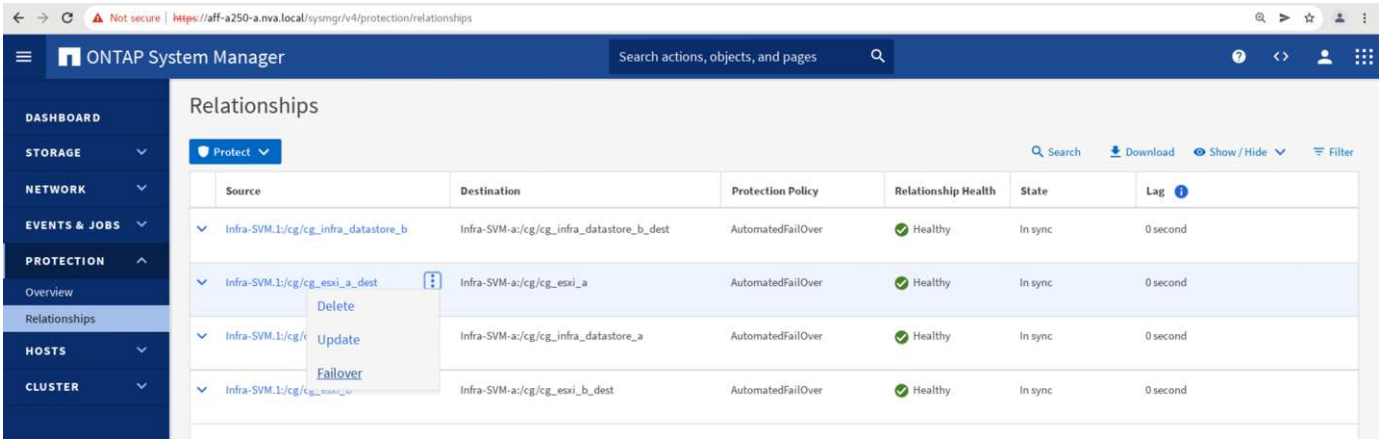


Auf der anderen Seite zeigt das Teilfenster „Performance“ des Dashboards von Standort B System Manager einen deutlich höheren IOPS-Wert, da zusätzliche I/O-Vorgänge von Standort A auf ca. 130.000 IOPS verschoben werden. Und erreichte einen Durchsatz von etwa 1 GB/s bei einer I/O-Latenz von unter 1 Millisekunde.



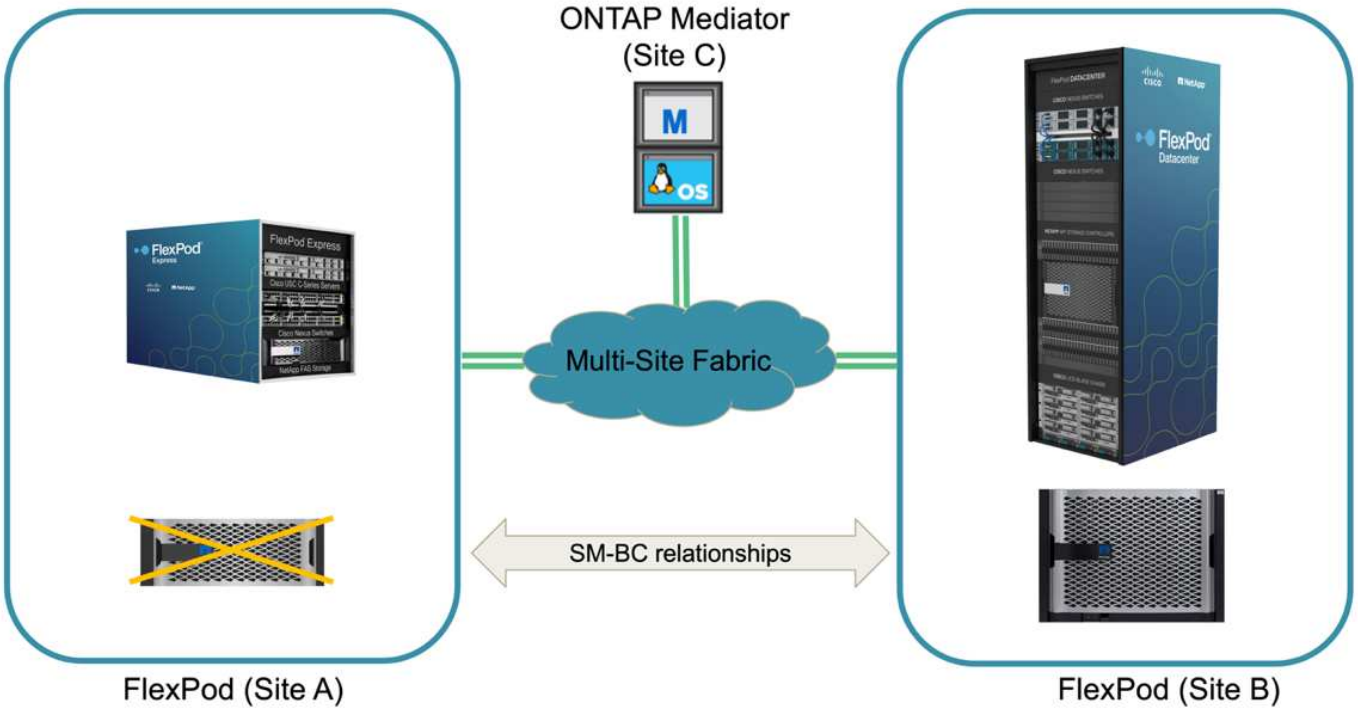
Wenn die I/O-Vorgänge transparent von Standort A nach Standort B migriert werden, können Storage-Controller an Standort A zu geplanten Wartungsarbeiten heruntergefahren werden. Nachdem die Wartungsarbeiten oder Tests abgeschlossen und ein Storage Cluster wieder betriebsbereit gemacht wurde, prüfen und warten Sie, bis sich der Sicherungsstatus der Konsistenzgruppe wieder in ändert `In sync` Bevor Sie ein Failover durchführen, um die Failover-I/O von Standort B zurück zu Standort A zurückzugeben Beachten Sie bitte, dass je länger ein Standort zu Wartungszwecken oder für das Testen ausfällt, desto länger

dauert es, bis die Daten synchronisiert und die Konsistenzgruppe wieder an den zurückgesendet wird `In sync` Bundesland.



Ungeplantes Storage-Failover

Wenn ein echter Notfall eintritt oder während einer Disaster Simulation auftritt, kann ein ungeplantes Storage-Failover erfolgen. Die folgende Abbildung zeigt beispielsweise, in der das Storage-System an Standort A einen Stromausfall hat, ein ungeplantes Storage-Failover ausgelöst wird und die Datenservices für Standort A LUNs, die durch die SM-BC-Beziehungen gesichert sind, von Standort B fortgesetzt werden



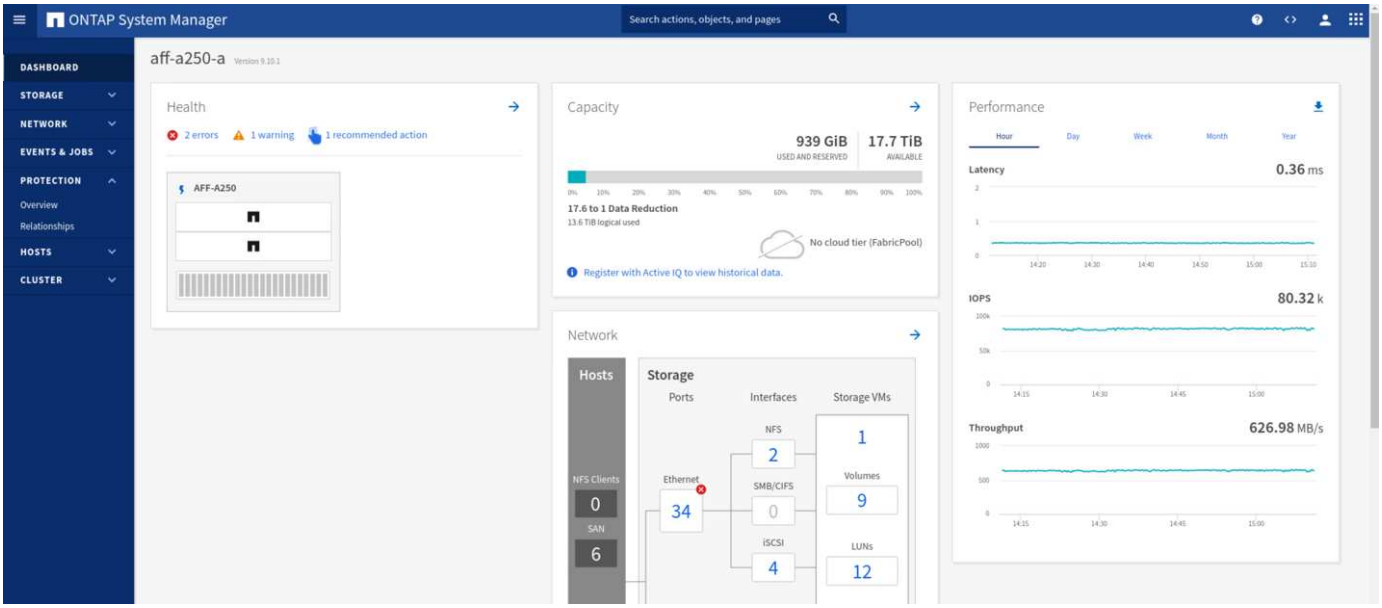
Um einen Storage-Ausfall an Standort A zu simulieren, können beide Storage Controller an Standort A ausgeschaltet werden, indem der Netzschalter deaktiviert wird, um die Stromversorgung der Controller einzustellen, Oder mit dem System Power Management Befehl der Speichercontroller-Prozessoren zum Ausschalten der Controller.

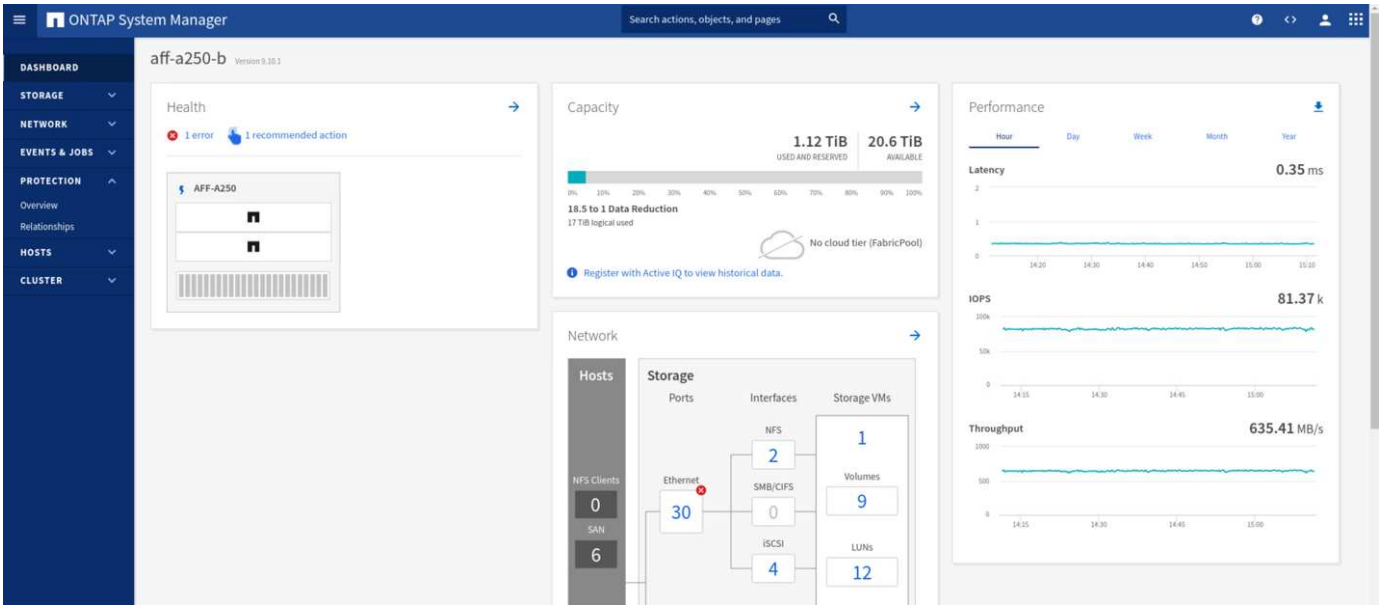
Wenn der Storage Cluster an Standort Mit Strom versorgt wird, findet ein plötzlicher Stopp der Datenservices statt, die von Standort A Storage-Cluster bereitgestellt werden. Anschließend erkennt der ONTAP Mediator, der die SM-BC-Lösung von einem dritten Standort aus überwacht, den Standort Als Storage-Ausfall und ermöglicht der SM-BC-Lösung ein automatisiertes ungeplantes Failover. Dadurch können Standort B Storage

Controller Datenservices für die LUNs fortsetzen, die in den SM-BC-Konsistenzgruppenbeziehungen mit Standort A konfiguriert sind

Aus der Applikationsperspektive stehen die Datenservices kurz vor der Pause, während das Betriebssystem den Pfadstatus der LUNs überprüft und mit den verfügbaren Pfaden zu den verbleibenden Storage Controllern am Standort B fortfahren.

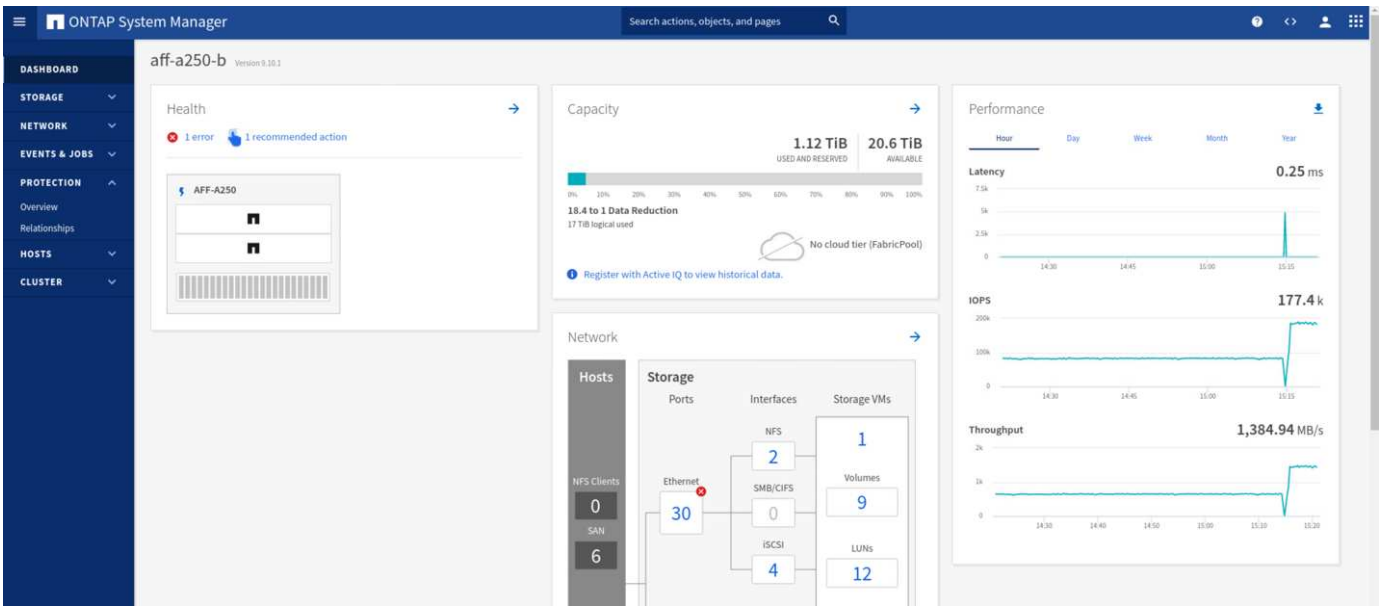
Während der Validierungstests generiert das IOMeter Tool auf den VMs an beiden Standorten I/O-Vorgänge für die lokalen Datenspeicher. Nachdem der Standort Ein Cluster ausgeschaltet war, wurden die I/O-Vorgänge kurz angehalten und danach wieder aufgenommen. In den folgenden beiden Abbildungen sind die Dashboards des Storage-Clusters an Standort A und Standort B bzw. vor dem Desaster dargestellt, die rund 80.000 IOPS und einen Durchsatz von 600 MB/s an jedem Standort zeigen.



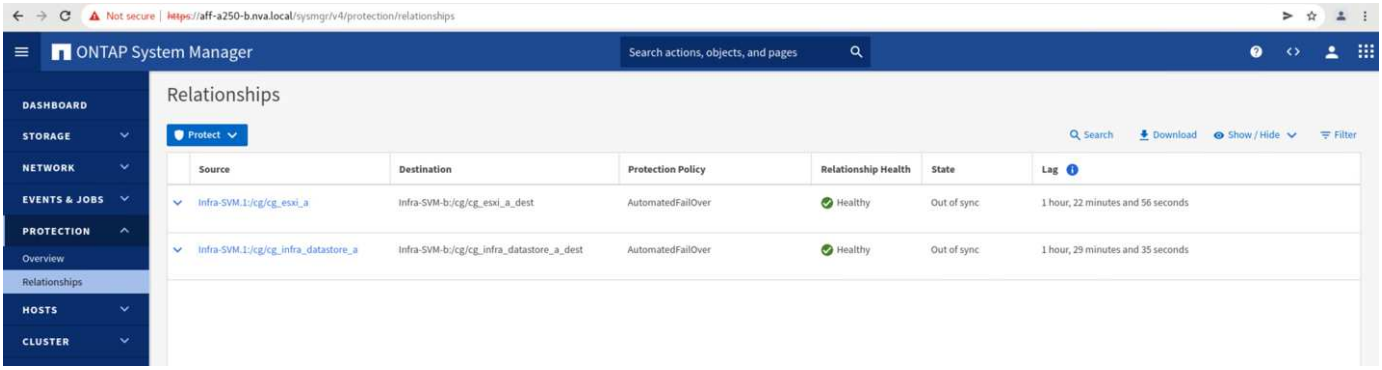


Nach dem Ausschalten der Storage-Controller an Standort A können wir visuell validieren, dass der I/O-Wert des Standort B Storage-Controllers stark erhöht wird, um zusätzliche Datenservices für Standort A bereitzustellen (siehe folgende Abbildung). Darüber hinaus zeigte die GUI der IOMeter VMs außerdem, dass die I/O-Vorgänge trotz eines Ausfalls des Standorts Im Storage-Cluster fortgesetzt wurden. Beachten Sie bitte, dass bei einem Storage-Ausfall zusätzliche Datastores, die von LUNs nicht durch SM-BC-Beziehungen

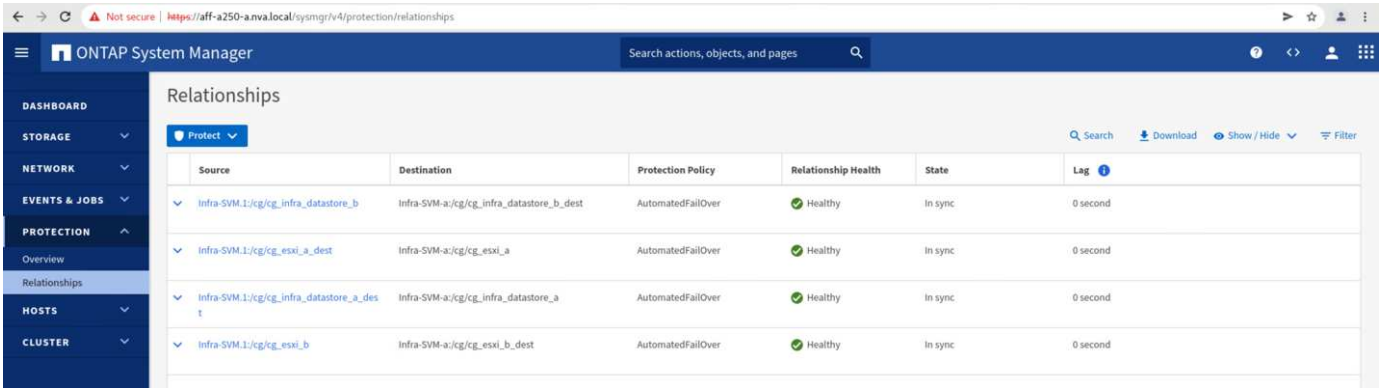
gesichert werden, nicht mehr zugänglich sind. Daher ist es wichtig, die geschäftlichen Anforderungen der verschiedenen Applikationsdaten zu bewerten und sie ordnungsgemäß in durch SM-BC-Beziehungen gesicherten Datenspeichern abzulegen, um Business Continuity zu gewährleisten.



Während der Standort Ein Cluster ausfällt, werden die Beziehungen der konsistenten Gruppen angezeigt `Out of sync` Status wie in der folgenden Abbildung dargestellt. Nachdem die Stromversorgung für die Storage-Controller an Standort A wieder eingeschaltet ist, startet das Storage-Cluster und die Datensynchronisierung zwischen Standort A und Standort B erfolgt automatisch.



Bevor Sie die Datenservices von Standort B zurück an Standort A zurücksenden, müssen Sie Standort A System Manager überprüfen und sicherstellen, dass die SM-BC-Beziehungen erfasst werden und der Status wieder synchron ist. Nachdem Sie bestätigt haben, dass die Konsistenzgruppen synchron sind, kann ein manueller Failover-Vorgang gestartet werden, um Datendienste in den Beziehungen der Konsistenzgruppen zurück an Standort A zurückzugeben



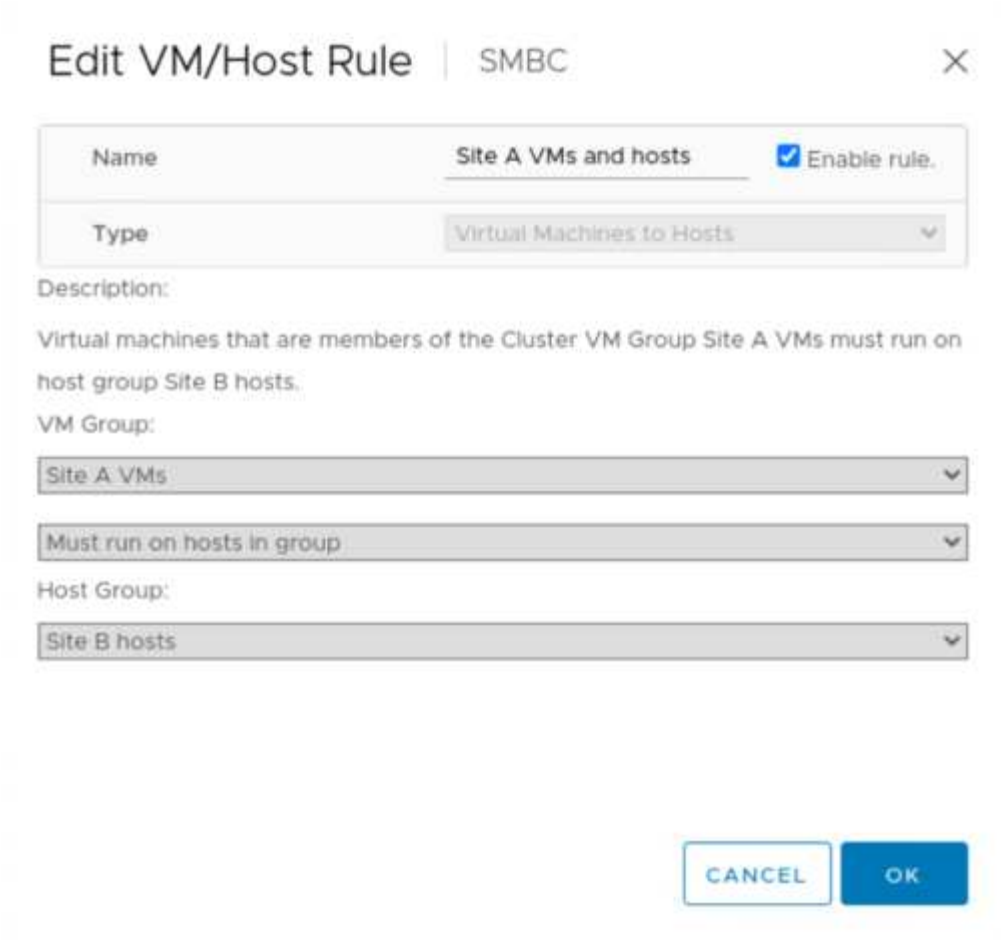
Komplette Wartung des Standorts oder des Standorts

Möglicherweise müssen Standortwartungsarbeiten durchgeführt, Stromverluste oder Naturkatastrophen wie Hurrikan oder Erdbeben ihre Auswirkungen haben. Daher ist es von entscheidender Bedeutung, dass geplante und ungeplante Standortausfälle angewendet werden, um sicherzustellen, dass Ihre FlexPod SM-BC Lösung richtig konfiguriert ist, damit diese Ausfälle all Ihrer geschäftskritischen Applikationen und Datenservices überleben können. Die folgenden standortbezogenen Szenarien wurden validiert.

- Geplantes Szenario für die Standortwartung durch Migration von Virtual Machines und wichtigen Datenservices zu einem anderen Standort
- Szenario mit ungeplanten Standortausfällen durch Ausschalten von Servern und Storage Controllern zur Disaster Simulation

Um einen Standort für die geplante Standortwartung vorbereitet zu sein, sind eine Kombination aus der Migration der betroffenen Virtual Machines vom Standort mit vMotion und ein manuelles Failover der SM-BC Consistency Group-Beziehungen erforderlich, um Virtual Machines und wichtige Datenservices auf einen alternativen Standort zu migrieren. Die Tests wurden in zwei verschiedenen Bestellungen durchgeführt: VMotion, zuerst gefolgt von SM-BC Failover und SM-BC Failover, gefolgt von vMotion, um sicherzustellen, dass die Virtual Machines weiterhin ausgeführt werden und die Datenservices nicht unterbrochen werden.

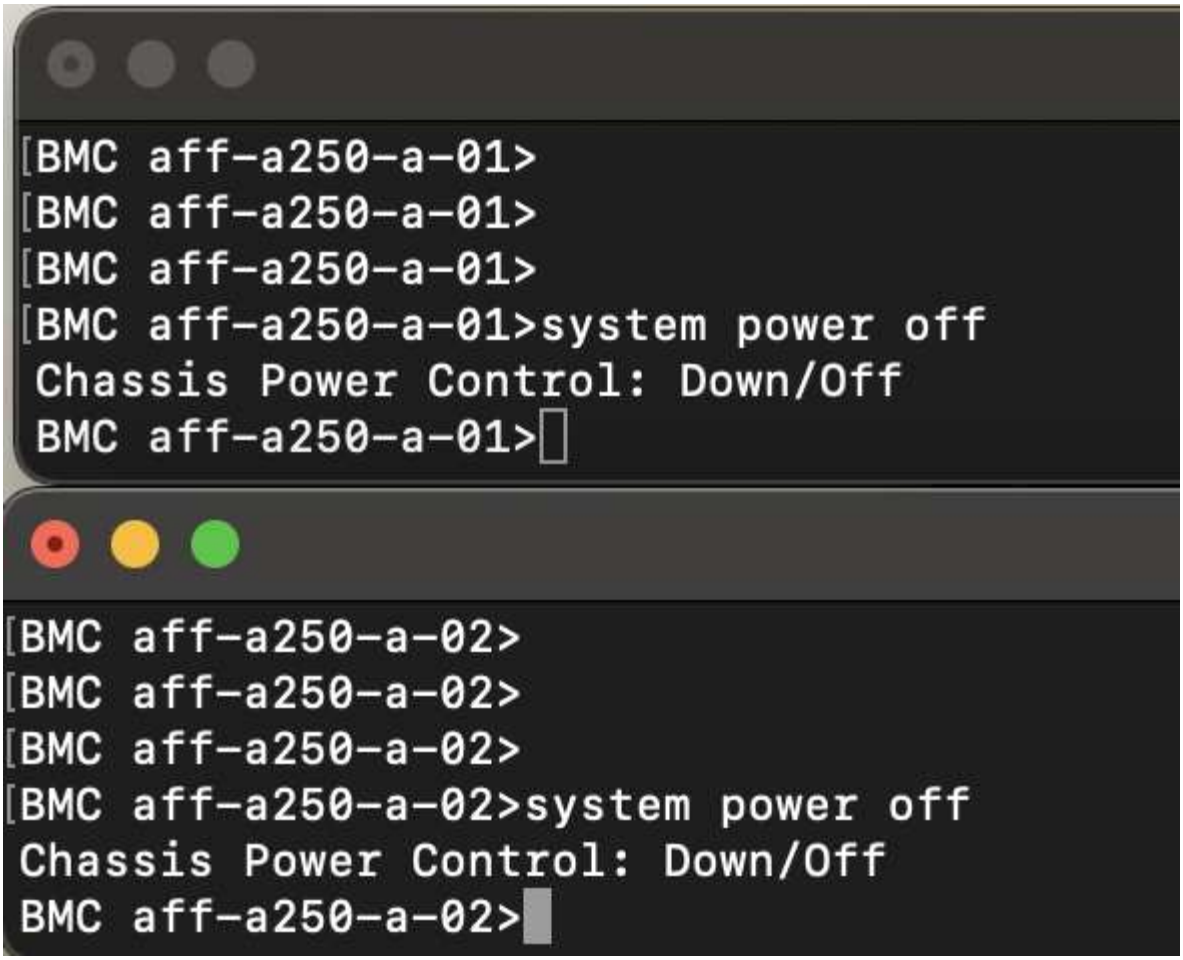
Aktualisieren Sie vor Durchführung der geplanten Migration die VM-/Host-Affinitätsregel, damit die VMs, die aktuell am Standort ausgeführt werden, automatisch von dem Wartungsort migriert werden. Der folgende Screenshot zeigt ein Beispiel für die Änderung der Regel für eine VM/Host-Affinität, die von VMs automatisch von Standort A nach Standort B migriert werden soll. Sie müssen nicht angeben, dass die VMs nun auf Standort B ausgeführt werden müssen, sondern können die Affinitätsregel vorübergehend deaktivieren, sodass die VMs manuell migriert werden können.



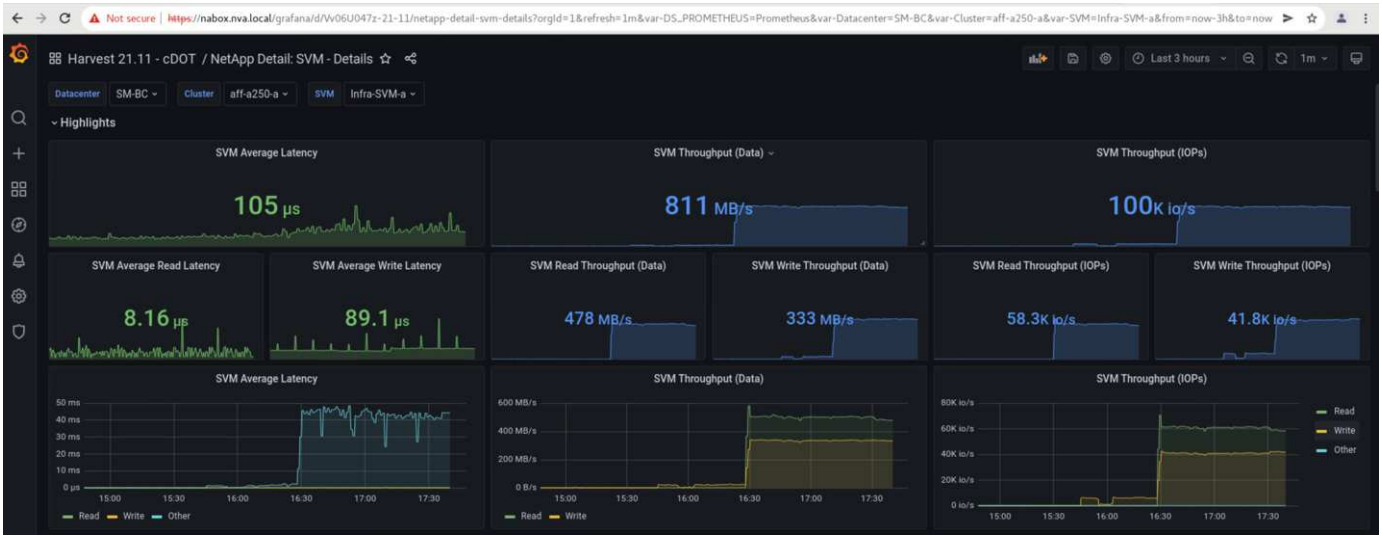
Nach der Migration von Virtual Machines und Storage Services können Sie Server, Storage Controller, Platten-Shelves und Switches ausschalten und die erforderlichen Wartungsarbeiten am Standort durchführen. Wenn die Standortwartung abgeschlossen ist und die FlexPod Instanz wieder aufgenommen wird, können Sie die Host-Gruppenaffinität für die VMs ändern, um wieder an den ursprünglichen Standort zurückzukehren. Danach sollten Sie die Regel „muss auf Hosts in Gruppe laufen“ VM/Host Site Affinity zurück zu „sollte auf Hosts in der Gruppe laufen“ ändern, so dass virtuelle Maschinen auf Hosts an dem anderen Standort ausgeführt werden dürfen, sollte eine Katastrophe stattfinden. Für die Validierungstests wurden alle Virtual Machines erfolgreich an den anderen Standort migriert, und die Datenservices werden nach dem Failover für die SM-BC-Beziehungen ohne Probleme fortgesetzt.

Bei der ungeplanten Disaster-Simulation am Standort wurden die Server und Storage Controller ausgeschaltet, um einen Standortausfall zu simulieren. Die VMware HA-Funktion erkennt die heruntergefahrenen Virtual Machines und startet die Virtual Machines am noch intakten Standort neu. Zudem erkennt der ONTAP Mediator, der an einem dritten Standort ausgeführt wird, den Standortausfall und der überlebende Standort initiiert einen Failover und beginnt mit der Bereitstellung von Datenservices für den Down-Standort wie erwartet.

Der folgende Screenshot zeigt, dass die Speicher-Controller Service-Prozessor-CLI verwendet wurden, um den Standort Ein Cluster abrupt auszuschalten, um eine Speicherkatastrophe zu simulieren.



Die Storage Virtual Machine Dashboards von Storage-Clustern, die vom NetApp Harvest Datenerfassungs-Tool erfasst und in Grafana Dashboard im NABox-Monitoring-Tool angezeigt werden, sind in den folgenden zwei Screenshots dargestellt. Wie auf der rechten Seite der IOPS- und Durchsatzdiagramme zu sehen ist, wählt der Cluster B sofort einen Storage-Workload aus, nachdem Standort Ein Cluster ausfällt.

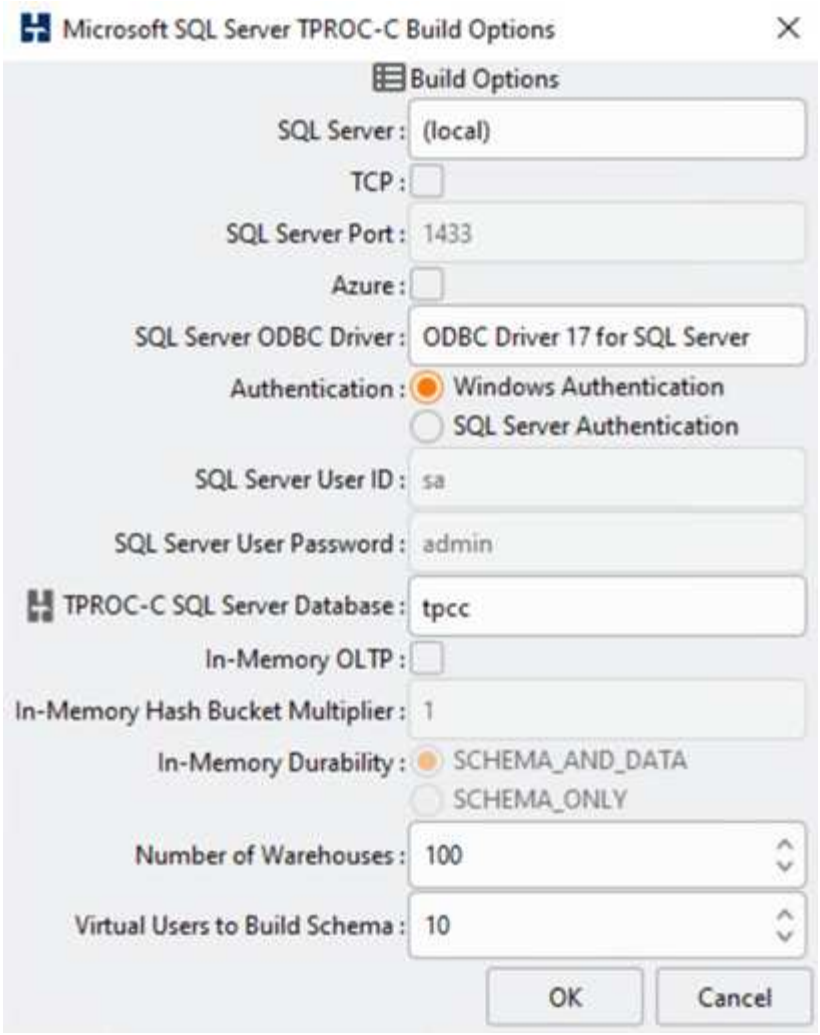


Microsoft SQL Server

Microsoft SQL Server ist eine weit verbreitete und implementierte Datenbankplattform für DIE IT in Unternehmen. Die Version Microsoft SQL Server 2019 enthält zahlreiche neue Funktionen und Verbesserungen für seine relationalen und analytischen Engines. Sie unterstützt Workloads bei Applikationen, die lokal, in der Cloud und bei hybriden Umgebungen über eine Kombination dieser Applikationen ausgeführt werden. Darüber hinaus kann die Lösung auf diversen Plattformen implementiert werden, darunter Windows, Linux und Container.

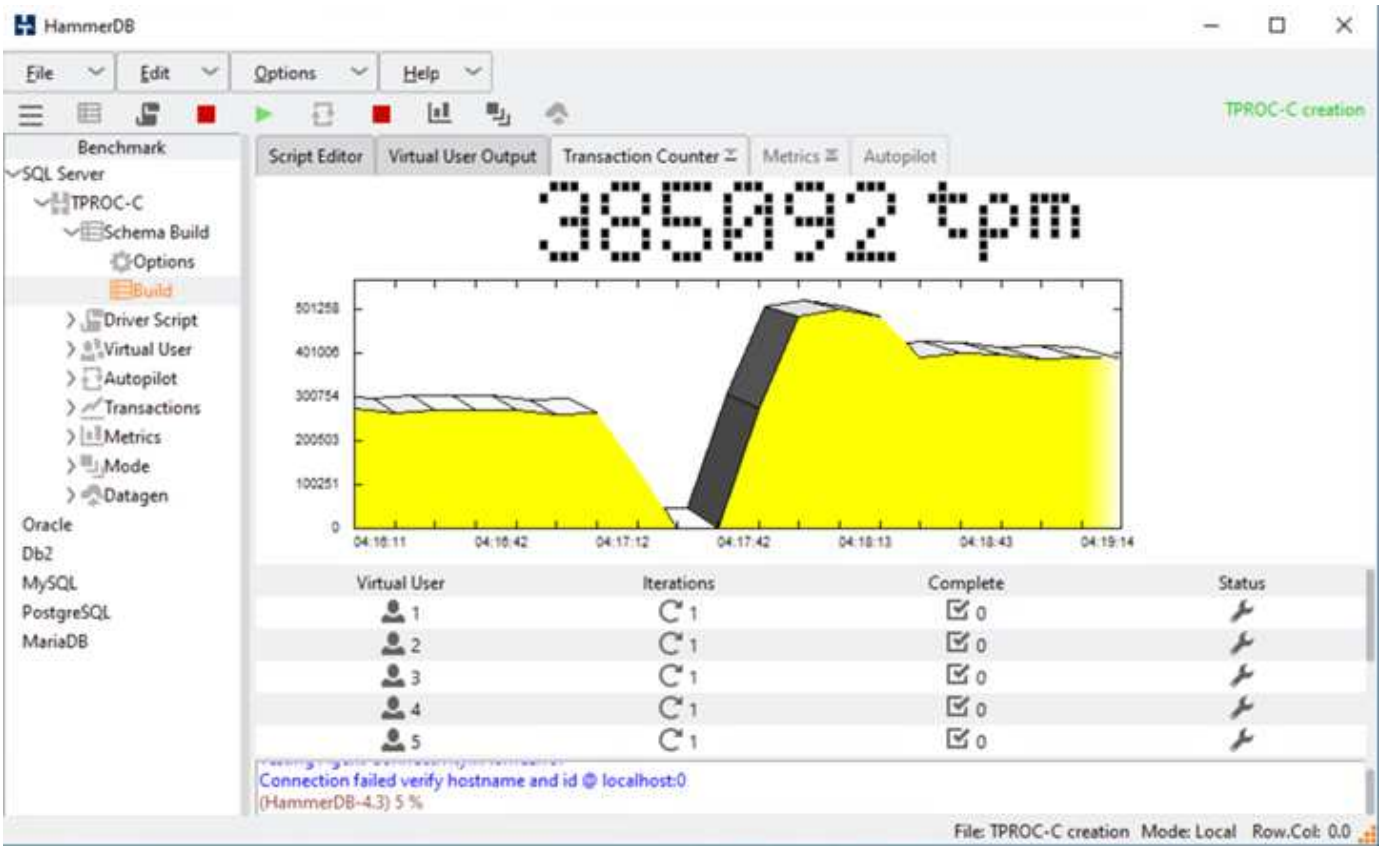
Im Rahmen der geschäftskritischen Workload-Validierung für die FlexPod SM-BC Lösung wird Microsoft SQL Server 2019 auf einer Windows Server 2022 VM installiert. Außerdem sind die IOMeter VMs für geplante und ungeplante Storage Failover-Tests enthalten. Auf der Windows Server 2022 VM wird SQL Server Management Studio installiert, um den SQL Server zu verwalten. Das Datenbanktool HammerDB wird für Tests zur Generierung von Datenbanktransaktionen eingesetzt.

Das HammerDB Datenbank-Testtool wurde für die Prüfung mit dem Microsoft SQL Server TPROC-C Workload konfiguriert. Für die Schemakonfigurationen wurden die Optionen aktualisiert, um 100 Lagerhäuser mit 10 virtuellen Benutzern zu verwenden, wie im folgenden Screenshot dargestellt.



Nachdem die Optionen zum Erstellen des Schemas aktualisiert wurden, wurde der Prozess zum Erstellen des Schemas gestartet. Einige Minuten später wurde ein ungeplanter Storage-Cluster an Standort B durch das gleichzeitige Herunterfahren beider Nodes des AFF A250 Storage-Clusters mit zwei Nodes mithilfe von CLI-Befehlen eingeleitet.

Nach einer kurzen Pause von Datenbanktransaktionen trat das automatisierte Failover zur Disaster-Korrektur ein und die Transaktionen wurden wieder aufgenommen. Der folgende Screenshot zeigt den HammerDB Transaction Counter Screenshot um diese Zeit. Da sich die Datenbank für den Microsoft SQL Server normalerweise im Storage-Cluster vor Ort B befindet, pausierte die Transaktion kurz, als der Storage an Standort B ausfällt und nach dem automatisierten Failover wieder aufgenommen wurde.



Die Storage Cluster-Kennzahlen wurden mithilfe des NAbox Tools mit dem installierten NetApp Harvest Monitoring Tool erfasst. Die Ergebnisse werden in den vordefinierten Grafana Dashboards für die Storage Virtual Machine und andere Speicherobjekte angezeigt. Das Dashboard bietet Matrizen für Latenz, Durchsatz, IOPS und zusätzliche Details mit Lese- und Schreibstatistiken, die sowohl für Standort B als auch Standort A getrennt sind

Dieser Screenshot zeigt das NAbox Grafana Performance-Dashboard für Storage-Cluster an Standort B.

Die IOPS für das Storage-Cluster am Standort B wiesen circa 100.000 IOPS auf, bevor der Ausfall einführte. Anschließend zeigte die Performance-Metriken einen deutlichen Rückgang auf Null auf der rechten Seite der Diagramme aufgrund des Ausfalls. Da der Storage-Cluster Standort B ausgefallen war, konnte nach der Katastrophe kein Storage-Cluster am Standort B gesammelt werden.

Andererseits nahmen die IOPS für den Standort Ein Storage-Cluster die zusätzlichen Workloads von Standort B nach dem automatisierten Failover ab. Der zusätzliche Workload kann im folgenden Screenshot auf der rechten Seite der IOPS- und Durchsatzdiagramme angezeigt werden. Darin wird das NAbox Grafana Performance-Dashboard für Standort A Storage-Cluster angezeigt.

Das oben aufgeführte Szenario für das Storage-Disaster-Test bestätigte, dass der Microsoft SQL Server Workload einen vollständigen Ausfall des Storage-Clusters an Standort B überleben kann, wo sich die Datenbank befindet. Die Applikation verwendete die von dem Standort Einem Storage-Cluster bereitgestellten Datenservices transparent, nachdem ein Ausfall erkannt und der Failover stattgefunden hat.

Wenn auf der Rechenebene die VMs, die an einem bestimmten Standort ausgeführt werden, ein Host-Ausfall auftreten, werden die VMs so konzipiert, dass sie automatisch durch die VMware HA-Funktion neu gestartet werden. Für einen vollständigen Ausfall des Standorts ermöglicht es die VM-/Host-Affinitätsregeln, VMs am noch intakten Standort neu zu starten. Damit eine geschäftskritische Applikation unterbrechungsfreie Services bereitstellen kann, ist jedoch ein applikationsbasiertes Clustering wie Microsoft Failover Cluster oder Container-basierte Applikationsarchitektur für Kubernetes erforderlich, um Ausfallzeiten bei Applikationen zu vermeiden. Bitte lesen Sie das entsprechende Dokument zur Implementierung des applikationsbasierten Clustering. Dieses Dokument übersteigt den Rahmen dieses technischen Berichts.

"Weiter: Fazit."

Schlussfolgerung

"Zurück: Lösungsvalidierung - validierte Szenarien."

Das FlexPod Datacenter mit SM-BC beruht auf einem aktiv/aktiv-Datacenter-Design, das Business Continuity und Disaster Recovery für geschäftskritische Workloads bietet. Mit der Lösung sind normalerweise zwei Datacenter verknüpft, die an separaten, geografisch verteilten Standorten in einem Großraumgebiet bereitgestellt werden. Die NetApp SM-BC Lösung verwendet synchrone Replizierung, um geschäftskritische Datenservices gegen einen Standortausfall zu schützen. Voraussetzung für die Lösung ist, dass die beiden FlexPod-Bereitstellungsstandorte eine Netzwerklatenz von weniger als 10 Millisekunden pro Jahr nutzen.

Der NetApp ONTAP Mediator, der an einem dritten Standort implementiert wird, überwacht die SM-BC-Lösung und ermöglicht ein automatisiertes Failover bei einem Standortausfall. VMware vCenter mit VMware HA und

Stretched VMware vSphere Metro Storage Cluster Konfiguration funktionieren nahtlos mit NetApp SM-BC, damit die Lösung die gewünschten RPO von null und RTO von fast null erfüllt.

Die FlexPod SM-BC Lösung kann auch in vorhandenen FlexPod Infrastrukturen implementiert werden, wenn sie die Anforderungen erfüllen, oder wenn eine zusätzliche FlexPod Lösung zu einem vorhandenen FlexPod hinzugefügt wird, um die Business Continuity-Ziele zu erreichen. Zusätzliche Management-, Monitoring- und Automatisierungs-Tools wie Cisco Intersight, Ansible und HashiCorp Terraform- basierte Automatisierung stehen von NetApp und Cisco zur Verfügung, damit Sie die Lösung einfach überwachen, Einblicke in ihren Betrieb erhalten und die Implementierung und den Betrieb automatisieren können.

Aus Sicht einer geschäftskritischen Applikation wie Microsoft SQL Server ist eine Datenbank, die sich auf einem VMware Datastore befindet und durch eine ONTAP SM-BC CG-Beziehung geschützt ist, trotz eines Standort-Storage-Ausfalls weiterhin verfügbar. Wie während der Validierungstests verifiziert, wird nach einem Stromausfall im Storage Cluster, in dem sich die Datenbank befindet, ein Failover der SM-BC CG-Beziehung durchgeführt und die Microsoft SQL Server Transaktionen ohne Applikationsunterbrechung fortgesetzt.

Dank der granularen Datensicherung für Applikationen können ONTAP SM-BC CG-Beziehungen für geschäftskritische Applikationen erstellt werden, um RPO-Anforderungen von null und RTO von nahezu null zu erfüllen. Damit das VMware Cluster, auf dem die Microsoft SQL Server Applikation ausgeführt wird, einen Storage-Ausfall vor Ort überleben kann, sind die Boot-LUNs der ESXi Hosts an jedem Standort ebenfalls durch eine SM-BC CG-Beziehung geschützt.

Dank der Flexibilität und Skalierbarkeit von FlexPod können Sie mit einer geeigneten Infrastruktur beginnen, die sich Ihren wachsenden Geschäftsanforderungen anpassen lässt. Dieses validierte Design ermöglicht es Ihnen, zuverlässig eine auf VMware vSphere basierende Private Cloud in einer verteilten und integrierten Infrastruktur zu implementieren. Dadurch erhalten Sie eine Lösung, die sich gegen viele Single-Point-of-Failure-Szenarien sowie einen Standortausfall schützen kann, sodass wichtige Business-Datenservices geschützt sind.

"Weiter: Wo finden Sie zusätzliche Informationen und Versionsverlauf."

Wo finden Sie weitere Informationen und Versionsverlauf

"Zurück: Schlussfolgerung."

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

FlexPod

- FlexPod Startseite

  "https://www.flexpod.com"

- Cisco Validated Design und Implementierungsleitfäden für FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Cisco Server – Unified Computing System (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- NetApp Produktdokumentation

"https://www.netapp.com/support-and-training/documentation/"

- FlexPod Datacenter with Cisco UCS 4.2(1) im UCS Managed Mode, VMware vSphere 7.0 U2 und NetApp ONTAP 9.9 Design Guide

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- FlexPod Datacenter with Cisco UCS 4.2(1) im UCS Managed Mode, VMware vSphere 7.0 U2 und NetApp ONTAP 9.9 Deployment Guide

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- FlexPod Datacenter mit Cisco UCS X-Serie, VMware 7.0 U2 und NetApp ONTAP 9.9 Design Guide

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- FlexPod Datacenter mit Cisco UCS X-Serie, VMware 7.0 U2 und NetApp ONTAP 9.9 Deployment Guide

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp All Flash FAS/FAS NVA Design-Leitfaden

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini and NetApp AFF/FAS NVA Deployment Guide

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP mit VXLAN-Frontend für mehrere Standorte

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox

  "https://nabox.org"

- NetApp Harvest

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4878: SnapMirror Business Continuity (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Wie eine SnapMirror Beziehung ONTAP 9 richtig gelöscht wird

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Grundlagen von SnapMirror Synchronous Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Grundlagen der asynchronen SnapMirror Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Datensicherung und Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Installieren oder aktualisieren Sie den ONTAP Mediator-Dienst

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere HA und vSphere Metro Storage Cluster

- Erstellen und Verwenden von vSphere HA-Clustern

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage-Cluster (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Empfohlene Practices für VMware vSphere Metro Storage-Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP mit NetApp SnapMirror Business Continuity (SM-BC) mit VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Schutz von Tier-1-Applikationen und -Datenbanken mit VMware vSphere Metro Storage-Cluster und ONTAP

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL und HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Architecting Microsoft SQL Server on VMware vSphere Best Practices Guide

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- HammerDB-Website

  "https://www.hammerdb.com"

Kompatibilitätsmatrix

- Cisco UCS Hardware Compatibility Matrix

  "https://ucshcltool.cloudapps.cisco.com/public/"

- NetApp Interoperabilitäts-Matrix-Tool

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- VMware Compatibility Guide

  "http://www.vmware.com/resources/compatibility/search.php"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2022	Erste Version.

FlexPod Datacenter with VMware vSphere 7.0, Cisco VXLAN Single-Site Fabric, and NetApp ONTAP 9.7 – Design

Ramesh Isaac, Cisco Abhinav Singh, NetApp

Cisco Validated Designs (CVDs) bestehen aus Systemen und Lösungen, die entwickelt, getestet und dokumentiert wurden, um Kundenimplementierungen zu vereinfachen und zu verbessern. Bei diesen Designs wird ein breites Spektrum an Technologien und Produkten in ein Portfolio von Lösungen integriert, das speziell für die Geschäftsanforderungen der Kunden entwickelt wurde. Gemeinsam entwickeln Cisco und NetApp FlexPod, eine Lösung, die als Grundlage für eine Vielzahl verschiedener Workloads dient, und liefern robuste, effiziente und skalierbare Architekturdesigns, die genau auf Kundenanforderungen zugeschnitten sind. Eine FlexPod Lösung ist ein validierter Ansatz für die Implementierung von Technologien und Produkten von Cisco und NetApp für den Aufbau von Shared Private und Public Cloud-Infrastrukturen.

"FlexPod Datacenter with VMware vSphere 7.0, Cisco VXLAN Single-Site Fabric, and NetApp ONTAP 9.7 – Design"

FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 – Bereitstellung

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt das Cisco und NetApp FlexPod-Datacenter mit NetApp ONTAP 9.7 auf NetApp AFF A400 All-Flash-Storage-System, die Unified Software-Version 4.1(2) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation und VMware vSphere 7.0. Cisco UCS Manager (UCSM) 4.1(2) bietet konsolidierten Support für Folgendes:

- Alle aktuellen Cisco UCS Fabric Interconnect-Modelle: 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- IOM der Serie 2200/2300/2400
- Cisco UCS B-Serie
- Cisco UCS C-Serie

Darüber hinaus sind die Cisco Intersight- und NetApp Active IQ-SaaS-Managementplattformen enthalten.

FlexPod-Datacenter mit NetApp ONTAP 9.7, Cisco UCS Unified Software Release 4.1(2) und VMware vSphere 7.0 umfassen eine vorab entwickelte Best-Practice Datacenter-Architektur auf Basis des Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switches, MDS 9000 Multilayer Fabric Switches, Und den NetApp Storage-Arrays der AFF A-Serie mit der Datenmanagement-Software ONTAP 9.7.

"FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 – Bereitstellung"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, einen validierten Ansatz zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere, der beliebtesten Virtualisierungsplattform der Enterprise-Klasse für Datacenter auf FlexPod.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 – Deployment

John George, Cisco Scott Kovacs, NetApp

Der aktuelle Trend in der Datacenter-Branche geht hin zu Shared IT Infrastructures. Durch die Virtualisierung und vorab validierte IT-Plattformen begeben sich Enterprise-Kunden auf den Weg zur Cloud. Sie verlassen sich dabei auf Applikationssilos und

nutzen eine schnell implementierbare Shared IT-Infrastruktur, wodurch sich die Flexibilität erhöht und die Kosten sinken. Cisco und NetApp haben gemeinsam FlexPod entwickelt. Diese Technologie verwendet branchenführende Storage-, Server- und Netzwerkkomponenten, um als Grundlage für eine Vielzahl von Workloads zu dienen. So können effiziente Architekturdesigns bereitgestellt werden, die schnell und sicher implementiert werden können.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 – Deployment"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt eine validierte Lösung zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere, der beliebtesten Virtualisierungsplattform der Enterprise-Klasse für Datacenter auf FlexPod.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und Anwendungsfällen unterstützt. Mit dieser Lösung können Kunden schnell und zuverlässig eine auf VMware vSphere basierende Private Cloud in einer integrierten Infrastruktur implementieren.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design"

FlexPod-Datacenter mit VMware vSphere 6.7 U2, Cisco UCS – Fabric-Infrastruktur der Forth-Generation und NetApp ONTAP 9.6

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt das FlexPod-Datacenter von Cisco und NetApp mit NetApp ONTAP 9.6, die Unified Software Release 4.0(4) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation und VMware vSphere 6.7 U2. Cisco UCS Manager (UCSM) 4.0(4) bietet konsolidierten Support für Folgendes:

- Alle aktuellen Cisco UCS Fabric Interconnect-Modelle: 6200, 6300, 6324 (Cisco UCS Mini)
- 6454
- IOM der Serie 2200/2300/2400
- Cisco UCS B-Serie
- Cisco UCS C-Serie:

FlexPod-Datacenter mit NetApp ONTAP 9.6, Cisco UCS Unified Software Release 4.0(4) und VMware vSphere 6.7 U2 ist eine vorab entwickelte Best-Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switch-Familie, MDS 9000 Multilayer Fabric Switches, NetApp AFF Storage-Arrays Der A-Serie mit ONTAP 9.

"FlexPod-Datacenter mit VMware vSphere 6.7 U2, Cisco UCS Fabric der vierten Generation und NetApp ONTAP 9.6"

FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series – Design

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, einen validierten Ansatz zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere, der beliebtesten Virtualisierungsplattform der Enterprise-Klasse von Datacentern auf FlexPod.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und Anwendungsfällen unterstützt. Mit dieser Lösung können Kunden eine auf VMware vSphere basierende Private Cloud schnell und zuverlässig in einer integrierten Infrastruktur implementieren.

Die empfohlene Lösungsarchitektur basiert auf Cisco Unified Computing System (Cisco UCS) und verwendet die einheitliche Softwareversion zur Unterstützung der Cisco UCS Hardware-Plattformen, einschließlich Cisco UCS B-Series Blade- und C-Series Rack-Servern, Cisco UCS 6454 Fabric Interconnects, Switches der Cisco Nexus 9000 Serie, Cisco MDS Fibre Channel Switches, NetApp All-Flash-Storage-Arrays vorgestellt. Darüber hinaus enthält es VMware vSphere 6.7 Update 1, das eine Reihe neuer Funktionen zur Optimierung der Storage-Auslastung und zur Einrichtung einer privaten Cloud bietet.

"FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series – Design"

FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt das FlexPod-Datacenter von Cisco und NetApp mit der einheitlichen Softwareversion 4.0(2) von Cisco UCS Manager und VMware vSphere 6.7 U1. Cisco UCS Manager (UCSM) 4.0(2) bietet konsolidierten Support für alle aktuellen Cisco UCS Fabric Interconnect Modelle (6200, 6300, 6324 (Cisco UCS Mini)), IOM der Serie 6454,2200/2300, Cisco UCS B-Serie und Cisco UCS C-Serie. FlexPod Datacenter mit Cisco UCS Unified Software Release 4.0(2) und VMware vSphere 6.7 U1 ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (UCS), der Cisco Nexus 9000 Switch-Familie und MDS 9000 Multilayer Fabric Switches basiert. Und NetApp Storage-Arrays der AFF A-Serie mit dem Storage-Betriebssystem ONTAP 9.

"FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series"

Design von FlexPod Datacenter mit Cisco ACI Multi-Pod, NetApp MetroCluster IP und VMware vSphere 6.7

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Dieses Dokument beschreibt die Integration der Cisco ACI Multi-Pod und NetApp MetroCluster IP Lösung in das FlexPod Datacenter, um eine hochverfügbare Multi-Datacenter-Lösung anzubieten. Die Multi-Datacenter-Architektur bietet die Möglichkeit, Workloads zwischen zwei Datacentern auszubalancieren, indem unterbrechungsfreie Workload-Mobilität genutzt wird. Auf diese Weise können Services ohne Unterbrechung eines Ausfalls zwischen den Standorten migriert werden.

Die FlexPod mit ACI Multi-Pod und NetApp MetroCluster IP Lösung bietet folgende Vorteile:

- Nahtlose Workload-Mobilität über mehrere Datacenter hinweg
- Einheitliche Richtlinien an allen Standorten
- Layer-2-Erweiterung über geografisch verteilte Datacenter hinweg
- Verbesserte Vermeidung von Ausfallzeiten während der Wartung
- Vermeidung von Ausfällen und Recovery

"Design von FlexPod Datacenter mit Cisco ACI Multi-Pod, NetApp MetroCluster IP und VMware vSphere 6.7"

FlexPod Datacenter mit Cisco ACI Multi-Pod mit NetApp MetroCluster IP und VMware vSphere 6.7 – Implementierung

Haseeb Niazi, Cisco Ramesh Issac, Cisco Arvind Ramakrishnan, NetApp

Cisco und NetApp haben gemeinsam eine Reihe von FlexPod Lösungen zur Unterstützung strategischer Datacenter-Plattformen entwickelt. Die FlexPod Lösung bietet eine integrierte Architektur, die Best Practices für das Design von Computing, Storage und Netzwerken umfasst. Dadurch werden IT-Risiken minimiert, indem die integrierte Architektur validiert wird, um die Kompatibilität verschiedener Komponenten sicherzustellen. Die Lösung löst auch IT-Problempunkte durch dokumentierte Designanleitungen, Implementierungsanleitungen und Support, die in verschiedenen Phasen (Planung, Entwurf und Implementierung) einer Bereitstellung verwendet werden können.

"FlexPod Datacenter mit Cisco ACI Multi-Pod mit NetApp MetroCluster IP und VMware vSphere 6.7 – Implementierung"